DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA PROYECTOS DE INVESTIGACIÓN EN EL ÁREA MEDIOAMBIENTAL

Segundo Ovidio Castro Umaña

Universidad Distrital Francisco José de caldas
Facultad Tecnológica
Maestría en Gestión y Seguridad de la Información
Bogotá D.C
Agosto 2025

DISEÑO DE UN MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA PROYECTOS DE INVESTIGACIÓN EN EL ÁREA MEDIOAMBIENTAL

Segundo Ovidio Castro Umaña

Trabajo de grado, Monografía para optar por el título de Magister en Gestión y Seguridad de la Información

Directora: MSc Rocio Rodríguez Guerrero

Universidad Distrital Francisco José de Caldas
Facultad tecnológica
Maestría en Gestión y Seguridad de la Información
Bogotá D.C
Agosto 2025

Agradecimientos

En primer lugar, agradezco a Dios por la fortaleza, la perseverancia y la claridad para avanzar que me brindó a lo largo de este exigente proceso. Su inspiración fue un soporte constante en los momentos de mayor desafío.

Deseo expresar mi más profundo agradecimiento a mi directora, la MSc. Rocio Rodríguez Guerrero. Más que una guía, fue una mentora cuya confianza, rigor metodológico y visión estratégica fueron indispensables para transformar este modelo. Su acompañamiento y exigencia me impulsaron a superar los desafíos de esta investigación.

A la Universidad Distrital Francisco José de Caldas y al cuerpo docente de la Maestría en Gestión y Seguridad de la Información, por brindarme la formación y las herramientas necesarias para emprender este desafío profesional y por ser el espacio académico que me permitió crecer.

Finalmente, a mi familia, por ser mi principal fuente de motivación y por su inagotable paciencia en las largas jornadas de trabajo. Su amor y apoyo incondicional han sido el cimiento sobre el cual se ha construido este logro. Este triunfo también les pertenece.

Resumen

Este documento presenta la propuesta de diseño conceptual para un modelo de seguridad de la información aplicado a proyectos de investigación en el ámbito medioambiental. La iniciativa surge a partir de la necesidad de responder a las particularidades operativas y normativas de estos entornos, en los que se gestionan datos sensibles, distribuidos y sujetos a riesgos específicos.

El modelo propuesto se estructura conforme al ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Integra lineamientos de normas internacionales como ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2022, MAGERIT v3 y NIST SP 800-53 Rev. 5. Esta base normativa permite establecer un enfoque sistemático para la identificación, análisis y tratamiento de riesgos, alineado con los objetivos de investigación y las condiciones técnicas del entorno.

El diseño contempla políticas, prácticas y controles organizados por función (preventivos, detectivos, correctivos y disuasivos), clasificados según el nivel de riesgo de los activos y su nivel de madurez tecnológica. Sumado a esto, incorpora mecanismos de segmentación, trazabilidad y documentación que favorecen su aplicación en contextos institucionales o programas de investigación científica. El resultado es un modelo conceptual integral que, al alinear marcos normativos con las particularidades del sector, constituye una guía estratégica para fortalecer la protección de activos críticos y mejorar la resiliencia operativa en proyectos de investigación medioambiental.

Palabras clave:

Seguridad de la información, proyectos ambientales, gestión de riesgos, activos digitales, controles de seguridad, ciclo PHVA, datos sensibles, normativas ISO, MAGERIT, ciberseguridad.

Abstract

This document presents a conceptual design proposal for an information security model applied to environmental research projects. The initiative arises from the need to address the operational and regulatory particularities of these environments, where sensitive, distributed data are managed and subject to specific risks.

The proposed model is structured according to the PDCA cycle (Plan, Do, Check, Act). It integrates guidelines from international standards such as ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 27005:2022, MAGERIT v3, and NIST SP 800-53 Rev. 5. This normative foundation enables a systematic approach to the identification, analysis, and treatment of risks, aligned with research objectives and the technical conditions of the environment.

The design includes policies, practices, and controls organized by function (preventive, detective, corrective, and deterrent), classified according to the risk level of the assets and their technological maturity. In addition, it incorporates segmentation, traceability, and documentation mechanisms that support its application in institutional contexts or scientific research programs. The result is a comprehensive conceptual model that, by aligning regulatory frameworks with sector-specific characteristics, serves as a strategic guide to strengthen the protection of critical assets and enhance operational resilience in environmental research projects.

Keywords:

Information security, environmental projects, risk management, digital assets, security controls, PDCA cycle, sensitive data, ISO standards, MAGERIT, cybersecurity.

TABLA DE CONTENIDO

Pag

Capítulo 1: Introducción 16

1.1 Planteamiento del Problema 18
1.2 Justificación 24
1.3 Alcances y Limitaciones del Modelo 26
1.3.1 Alcance del Diseño del Modelo 26
1.3.2 Limitaciones del Diseño Propuesto 28
1.4 Objetivos 29
1.4.1 Objetivo General 29
1.4.2 Objetivos Específicos 29

Capítulo 2: Fundamentos Teóricos Y Marcos De Referencia 30

2.1 Marco Teórico 31
2.1.1 Seguridad de la Información 31
2.1.2 Teoría de la Información y Seguridad 32
2.1.3 Principios de Seguridad 33
2.1.3.1 Confidencialidad. 33
2.1.3.2 Integridad. 34
2.1.3.3 Disponibilidad 34
2.1.3.4 Autenticidad. 34
2.1.3.5 No Repudio. 35
2.1.4 Modelos de Amenazas y Vulnerabilidades 35
2.1.4.1 Modelos de Amenazas. 35
2.1.4.2 Vulnerabilidades. 35
2.1.5 Activos de Información 36
2.1.6 Riesgos y Controles 36
2.2 Gestión del Riesgo y Seguridad de la Información. 36
2.2.1 Identificación de Riesgos 37
2.2.2 Evaluación y Tratamiento de Riesgos 37
2.2.3 Monitoreo Continuo y Gestión de Cambios 38
2.3 Investigación Medioambiental 38
2.3.1 Categorías en proyectos de investigación medioambiental 39
2.3.2 Datos Medioambientales 40
2.3.3 Infraestructura tecnológica en proyectos de investigación 41
2.3.3.1 Infraestructura de Captura y Adquisición de Datos. 43

2.3.3.2 Infraestructura de Transmisión y Comunicaciones. 45
2.3.3.3 Infraestructura de Almacenamiento y Procesamiento. 47
2.3.3.4 Infraestructura de Análisis y Visualización. 49
2.3.3.5 Infraestructura para Gestión de Proyectos y Datos. 51
2.3.3.6 Infraestructura de Seguridad y Cumplimiento. 54
2.3.3.7 Infraestructura de Respaldo, Continuidad y Energía. 56
2.3.3.8 Infraestructura de Desarrollo y Automatización. 57

2.4 Gobierno y Gestión Estratégica de la Información 60

2.4.1 Gobierno y Dirección Estratégica de TI 60
2.4.2 Gestión y Gobierno Integrado de TI 60
2.4.3 Arquitectura Empresarial Aplicada a Proyectos Medioambientales 61

Capítulo 3: Análisis de la Sensibilidad de Datos en el Contexto Medioambiental 62

3.1 Clasificación y Protección de Datos Medioambientales Sensibles 64
3.2 Licenciamiento para el Acceso y Uso de Datos Sensibles 65

3.2.1 Licencia de Acceso Confidencial o Clasificado 65
3.2.2 Licencia de Acceso Restringido Interno 66
3.2.3 Licencia de Acceso Controlado Externo 67
3.2.4 Licencia Temporal o Contextual 67
3.2.5 Licencia de Uso Académico o de Investigación 68
3.2.6 Licencia de Uso Comercial o con Fines Económicos 68
3.2.7 Licencia de Acceso Abierto con Condiciones 69

3.3 Características Particulares de los Proyectos Medioambientales 71
3.4 Contraste con Modelos Genéricos de Gestión de Proyectos 72

3.4.1 Enfoque Normativo y Consideraciones Sectoriales 73
3.4.2 Amenazas y Riesgos Diferenciales 74
3.4.3 Ejemplos y Estudios de Caso 76
3.4.4 Protocolos Específicos 78
3.4.5 Análisis Interpretativo de la Comparación 80
3.4.6 Comparativa Proyectos Medioambientales vs. Modelos Genéricos 83
3.4.7 Contraste Proyectos Medioambientales vs. Modelos Tradicionales de Gestión 85

Capítulo 4: Estructura Metodológica del Diseño 89

4.1.1 Fase Planear (Plan) 91
4.1.2 Fase Hacer 92
4.1.3 Fase Verificar 93
4.1.4 Fase Actuar 93

Capítulo 5: Fase de Planificación (Plan): Diagnóstico y Análisis de Riesgos 94

5.1 Diagnóstico del Contexto del Proyecto Medioambiental 96

5.1.1 Objetivo del Diagnóstico 98

5.1.2 Alcance del Diagnóstico 100
5.1.3 Proceso del Diagnóstico y Aspectos Clave 102
5.1.3.1 Técnicas de Recolección de Información. 103
5.1.3.2 Aspectos a Diagnosticar en el Contexto Ambiental. 106
5.1.3.3 Aplicación contextual al sector ambiental. 107
5.2 Identificación y Clasificación de Activos de Información en Entornos Distribuidos 109
5.2.1 Proceso de Gestión Conceptual de Activos 111
5.2.2 Tipología extendida de activos según contexto medioambiental 113
5.2.3 Clasificación Aplicada a Entornos Técnicos Distribuidos 124
5.2.4 Criticidad y Sensibilidad para Activos 125
5.2.4.1 Fórmula De Cálculo De Prioridad. 126
5.2.4.2 Activos de Información Documental. 128
5.2.4.3 Datos Ambientales. 129
5.2.4.4 Software y Herramientas Analíticas. 131
5.2.4.5 Equipamiento Tecnológico. 132
5.2.4.6 Servicios de Información. 133
5.2.4.7 Activos Humanos. 135
5.2.4.8 Normativos y Contractuales. 137
5.2.4.9 Soportes Físicos y Materiales. 139
5.2.5 Defensa en Profundidad 141
5.3 Análisis y Evaluación de Riesgos 147
5.3.1 Identificación de Amenazas y Vulnerabilidades. 150
5.3.2 Evaluación de Impacto y Sensibilidad. 160
5.3.3 Análisis de Riesgos. 166
5.3.3.1 Matriz de Evaluación de Riesgos. 168
5.3.4 Determinación de los Niveles de Riesgo. 169
5.3.5 Tratamiento del Riesgo y Selección de Controles 170
5.4 Análisis Avanzado de Amenazas 173
5.4.1 Caracterización de Fuentes de Amenazas 175
5.4.1.1 Perfilado de Motivaciones y Capacidades. 176
5.4.2 Análisis de Métodos de Explotación 178
5.4.3 Priorización de Amenazas Críticas 179
5.4.4 Generación de Perfiles de Amenaza 182
5.5 Planificar la formación y concienciación 185
5.5.1 Objetivo del Programa 185
5.5.2 Estructura del Programa de Formación y Concienciación 185
5.5.3 Relación con la Gestión de Riesgos 186
5.5.4 Ciclo de Mejora Continua 187
5.6 Planificación de Políticas y Procedimientos 188

5.7 Resultados Esperados (Fase Planear) 193

Capítulo 6: Fase de Diseño (Do): Estructuración del Modelo y Definición de Controles 195

6.1 Diseño de Políticas y Procedimientos de Seguridad 197

6.1.1 Diseño de Políticas de Alto Nivel 198
6.1.2 Diseño de Procedimientos Operativos 200
6.1.3 Integración de Partes Interesadas 202

6.2 Selección y Diseño Detallado de Controles de Seguridad 204

6.2.1 Criterios para la Selección de Controles 205
6.2.2 Diseño de Controles Técnicos Aplicables 207
6.2.3 Diseño de Controles Organizacionales y Administrativos 209
6.2.4 Diseño de Controles Físicos y Ambientales 211
6.2.5 Incorporación de Controles de Defensa en Profundidad 212
6.2.6 Trazabilidad de Requisitos a Controles Diseñados 215

6.3 Segmentación y Priorización de Controles Diseñados 217

6.3.1 Segmentación Lógica por Infraestructura, Uso o Funcionalidad 218
6.3.2 Metodología de Priorización para la Implementación Futura 220
6.3.3 Evaluación de Madurez Tecnológica 222

6.4 Estructuración y Documentación del Modelo de Seguridad 224

6.4.1 Arquitectura Lógica del Modelo de Seguridad 225
6.4.2 Formalización de la Documentación de Procesos y Procedimientos 231
6.4.3 Validación de la Estructura y Documentación Diseñadas 233

6.5 Mecanismos de Respuesta a Incidentes de Seguridad 235
6.6 Resultados Obtenidos 238

6.6.1 Sumario de los Principales Elementos Diseñados 240
6.6.2 Alineación con los Objetivos del Proyecto y el Contexto 242
6.6.3 Preparación para la Fase Verificar (Check) 244

Capítulo 7: Fase de Verificación (Check): Revisión y Validación Conceptual del Diseño 247

7.1 Revisión de la Conformidad y Coherencia del Diseño 248
7.2 Evaluación de la Eficacia del Diseño 250
7.3 Identificación de Gaps y Áreas de Mejora 252
7.4 Resultados de la Fase Verificar 253

Capítulo 8: Fase de Ajuste (Act): Mejora Continua del Diseño 255

8.1 Objetivo de la Fase Actuar en el Contexto del Diseño 257
8.2 Consolidación de Hallazgos y Lecciones Aprendidas 258
8.3 Definición y Priorización de Acciones para Mejorar el Diseño 260
8.4 Implementación de Ajustes en el Diseño del Modelo 261
8.5 Actualización de la Documentación del Modelo 262

8.6 Diseño de un Proceso para la Mejora Continua del Modelo 263
8.6.1 Incorporación de Nuevas Amenazas y Tecnologías 265
8.6.2 Adaptación a Cambios Normativos y del Contexto 265
8.6.3 Mecanismos de Retroalimentación para la Mejora 266
8.7 Resultados Esperados de la Fase Actuar 267

Capítulo 9: Plan de Implementación y Validación Empírica 268

9.1 Objetivos de la Planificación 269
9.2 Metodología y Alcance 270
9.3 Marco de Implementación Progresiva por Niveles de Madurez 271
9.4 Plan Detallado de Implementación Conceptual 273
9.5 Plan Detallado de Validación Empírica 274
9.6 Consideraciones de Riesgos y Desafíos 275
9.7 Resultados Esperados y Vinculación con la Mejora Continua Operacional 276

Capítulo 10: Gobernanza y Participación de Actores Interesados 278

10.1 Identificación y Análisis de las Partes Interesadas 279
10.2 Roles y Responsabilidades en la Gobernanza e Implementación 280
10.3 Estrategias de Comunicación y Capacitación Adaptadas 281
10.4 Mecanismos de Participación y Retroalimentación Continua 283

Capítulo 11: Análisis de Consideraciones Éticas, Legales y Sociales (CELS) 285

11.1 Fundamentos y Alcance de las Consideraciones CELS en el Proyecto 286
11.2 Implicaciones Éticas del Modelo de Seguridad 287
11.3 Marco Legal y Cumplimiento Normativo Ampliado 288
11.4 Impacto Social y Consideraciones Comunitarias 289
11.5 Integración y Gestión Continua de las Consideraciones CELS 289

Capítulo 12: Estrategia de Sostenibilidad del Modelo a Largo Plazo 291

12.1 Concepto de Sostenibilidad en Modelos de Seguridad Medioambiental 292
12.2 Sostenibilidad Tecnológica y Adaptación a la Obsolescencia 293
12.3 Sostenibilidad Económica y de Recursos a Largo Plazo 294
12.4 Sostenibilidad Organizacional y Gobernanza Continua 295
12.5 Resiliencia ante Cambios Físicos y Ambientales 296
12.6 Estrategia Integrada para la Sostenibilidad del Modelo 297

Capítulo 13: Contribuciones y Aportes del Modelo 299

13.1 Contribuciones Técnicas a la Seguridad de Datos Medioambientales 300
13.2 Innovaciones Operativas para la Colaboración Multi-Actor 301
13.3 Avances en la Responsabilidad Ética y Social 302
13.4 Perspectivas Estratégicas para la Sostenibilidad y Escalabilidad 302

Capítulo 14: Líneas de Investigación y Trabajos Futuros 304

14.1 Priorización de las Líneas Estratégicas Futuras 305
14.2 Línea Estratégica 1 (LE1): Consolidación y Optimización del Modelo Existente 307

14.2.1 Profundización de la Cobertura de Seguridad por Dominios Tecnológicos y Capas de Infraestructura 308

14.2.1.1 Controles para la Capa de Captura. 308
14.2.1.2 Controles para la Capa de Transmisión. 308
14.2.1.3 Controles para la Capa de Procesamiento 308
14.2.1.4 Validación y Métricas de Desempeño. 309

14.2.2 Refinamiento de la Arquitectura de Seguridad y Control Transversales 311

14.2.2.1 Políticas de Acceso Dinámico. 311
14.2.2.2 Monitoreo Continuo con SIEM. 311
14.2.2.3 Segmentación de Redes y Criptografía. 312
14.2.2.4 Respuesta a Incidentes. 312
14.2.2.5 Validación y Métricas. 312

14.2.3 Optimización Continua de la Gobernanza del Modelo, Gestión de Riesgos Integrada y Cumplimiento Dinámico (GRC) 314

14.2.3.1 Cuadro de Mando GRC. 314
14.2.3.2 Auditorías Automatizadas. 314
14.2.3.3 Gobernanza Multi-Actor. 314
14.2.3.4 Retroalimentación y Capacitación. 315

14.3 Línea Estratégica 2 (LE2): Especialización y Adaptación del Modelo a Contextos Dinámicos 316

14.3.1 Diseño y Desarrollo de Submodelos de Seguridad Especializados para Áreas de Alto Impacto o Requerimientos Particulares 316

14.3.1.1 Controles para la Seguridad de Datos de Investigación Medioambiental. 316
14.3.1.2 Cifrado Diferencial y Políticas de Retención. 317
14.3.1.3 Controles para Infraestructuras de Tecnología Operacional (OT). 317
14.3.1.4 Controles para Plataformas de Colaboración y Datos Abiertos 317
14.3.1.5 Validación y Guías de Implementación. 318

14.3.2 Adaptación Proactiva del Modelo a Nuevos Paradigmas Operativos, Tecnológicos y de Colaboración 319

14.3.2.1 Seguridad en Entornos Híbridos y Remotos. 319
14.3.2.2 Gestión de Identidades en Modelos Multi-Cloud. 320
14.3.2.3 Interoperabilidad y Federación de Identidades. 320
14.3.2.4 Validación y Guías de Configuración. 321

14.4 Línea Estratégica 3 (LE3): Innovación, Prospectiva y Resiliencia Estratégica 322

14.4.1 Investigación e Integración Piloto de Tecnologías de Seguridad Emergentes 322

14.4.1.1 Inteligencia Artificial y Aprendizaje Automático para Detección de Amenazas. 322

14.4.1.2 Criptografía Post-Cuántica para Protección a Largo Plazo. 323
14.4.1.3 Seguridad en Edge Computing para Entornos Remotos. 323
14.4.1.4 Blockchain para Integridad y Trazabilidad. 323
14.4.1.5 Validación mediante Pilotos. 324

14.4.2 Fortalecimiento de las Capacidades de Ciberinteligencia, Caza de Amenazas (Threat Hunting) y Ciberresiliencia Proactiva 325

14.4.2.1 Ciberinteligencia para Amenazas Específicas. 325
14.4.2.2 Búsqueda Proactiva de Amenazas. 326
14.4.2.3 Estrategias de Ciberresiliencia. 326
14.4.2.4 Validación y Guías Operativas. 326

14.5 Línea Estratégica 4 (LE4): Evolución del Marco de Gestión y Medición del Desempeño del Modelo 328

14.5.1 Perfeccionamiento Continuo del Ciclo PHVA Aplicado al Modelo: Métricas y Mecanismos de Retroalimentación 328

14.5.1.1 Diseño de KPIs y KRIs. 328
14.5.1.2 Mecanismos de Retroalimentación Automatizada. 328
14.5.1.3 Validación y Guías de Implementación. 329

14.5.2 Desarrollo de un Marco de Madurez y Hoja de Ruta para la Evolución Futura del Modelo de Seguridad (hacia V2.X, V3.X) 330

14.5.2.1 Marco Conceptual de Madurez. 330
14.5.2.2 Métricas de Evaluación. 331
14.5.2.3 Hoja de Ruta para V2.X y V3.X. 331
14.5.2.4 Validación y Guías de Evaluación. 332

Capítulo 15: Conclusiones y Recomendaciones Finales 334

15.1 Logros del Diseño y Planificación del Modelo de Seguridad 334
15.2 Respuesta a la Pregunta Central de Investigación 337
15.3 Análisis e Interpretación de Resultados en el Contexto Medioambiental 338

Referencias Bibliográficas 340

Anexos…….. 353

LISTA DE TABLAS

Pag.

Tabla 1 *Comparativa Proyectos Medioambientales vs. Modelos Genéricos* 83

Tabla 2 *Comparativa integral de seguridad de la información*..... 86

Tabla 3 *Diagnóstico del Contexto Organizacional*..... 104

Tabla 4 *Clasificación de Datos*..... 115

Tabla 5 *Evaluación de criticidad y sensibilidad de los datos*..... 120

Tabla 6 *Identificación y Clasificación de Activos por Capa de Defensa*..... 144

Tabla 7 *Identificación de Amenazas y Vulnerabilidades*..... 153

Tabla 8 *Análisis de Riesgos y Amenazas* 156

Tabla 9 *Evaluación Integridad, Confidencialidad y Disponibilidad*..... 162

Tabla 10 *Evaluación del Acceso y Disponibilidad* 163

Tabla 11 *Resumen de Políticas y Procedimientos Diseñados* 190

Tabla 12 *Implementación por Fases de Madurez*..... 271

Tabla 13 *Priorización para Trabajos Futuros*..... 306

LISTA DE FIGURAS

Figura 1 *Necesidad de un modelo de seguridad* 22

Figura 2 *Tecnología requerida identificada para proyectos MA*..... 41

Figura 3 *Infraestructura Básica Proyectos Medioambientales* 42

Figura 4 *Protección de Datos Ambientales*..... 62

Figura 5 *Diagrama de Ciclo del Proceso PDCA en la Metodología de Seguridad* 91

Figura 6 *Fundamentos Estratégicos del Modelo de Seguridad* 94

Figura 7 *Diagrama de Flujo del Proceso de Diagnóstico Organizacional*..... 98

Figura 8 *Diagrama de Flujo del Proceso de Gestión de Activos de Información* 111

Figura 9 *Defensa en profundidad investigación medioambiental*..... 143

Figura 10 *Matriz de Evaluación de Riesgos por Probabilidad e Impacto*..... 168

Figura 11 *Vinculación de activos con el marco legal y metodológico* 188

Figura 12 *Flujo General del Diseño y Definición de Controles de Seguridad*..... 197

Figura 13 *Estructura del Modelo de Seguridad*..... 226

Figura 14 *Modelo de Seguridad con Enfoque Ambiental* 238

Figura 15 *Verificación y Validación del Modelo Propuesto*..... 248

Figura 16 *Mejora Continua y Optimización del Diseño* 257

Figura 17 *Planificación y Validación Empírica del Modelo de Seguridad* 268

Figura 18 *Relaciones de partes interesadas, procesos y contexto*..... 278

Figura 19 *Componentes éticos, legales y sociales en la gobernanza de las CELS*..... 285

Figura 20 *Estrategia de Sostenibilidad del Modelo de Seguridad*..... 291

Figura 21 *Aportes Técnicos, Sociales y Estratégicos a la Investigación Ambiental* 299

Figura 22 *Marco Estratégico para la Evolución del Modelo de Seguridad*..... 304

Figura 23 *Impacto vs. Esfuerzo*..... 307

LISTA DE ANEXOS

Anexo A: Glosario Ampliado *353*

Anexo B: Plan de capacitación, sensibilización y comunicación de seguridad de la información 353

Anexo C: Guía de Referencia para Desarrollar un Diagnóstico de Madurez en Seguridad de la Información 353

Anexo D: Marcos Teórico y de Referencia Ampliado..... 353

Anexo E: Estructuración del Modelo de Seguridad..... 353

Capítulo 1: Introducción

La creciente complejidad de los entornos digitales, junto con la rápida evolución de las amenazas en seguridad de la información, plantea desafíos importantes para los proyectos de investigación en el ámbito medioambiental. Estos proyectos dependen cada vez más de infraestructuras tecnológicas especializadas, como nodos de sensores climáticos, sistemas de análisis remoto, y sistemas de información geográfica para datos georreferenciados. La gestión precisa de grandes volúmenes de información sensible, como registros de calidad del aire, parámetros hídricos, o datos de biodiversidad, expone estos esfuerzos a riesgos que comprometen la confidencialidad, la integridad de los resultados científicos, y la disponibilidad de los sistemas que los soportan.

Considerando este contexto, el presente documento propone el diseño conceptual de un modelo de seguridad de la información específicamente adaptado a los proyectos de investigación medioambiental. Este modelo define un conjunto integral de políticas, controles, y procesos para proteger activos críticos frente a amenazas como accesos no autorizados, intercepciones en redes de baja potencia, y manipulaciones de datos georreferenciados. Estructurado conforme al ciclo PHVA (Planificar, Hacer, Verificar, Actuar), el diseño aborda desafíos operativos, como la colaboración interinstitucional y las limitaciones de conectividad en entornos remotos, asegurando la confidencialidad, integridad, disponibilidad, y gestión adecuada de activos.

Este propósito se respalda en un marco normativo sistemático y un enfoque basado en riesgos, a través de la integración de estándares y marcos reconocidos internacionalmente. Se utilizan normas como ISO/IEC 27001:2022 (para la gestión de seguridad), ISO/IEC 27002:2022 (para controles técnicos), y ISO/IEC 27005:2022 (para gestión de riesgos). Se complementa con ISO 31000:2018 para principios de gestión de riesgos, ISO 55002:2018 para la gestión de activos físicos, ISO/IEC 38500:2024 y COBIT 2019 para la gobernanza estratégica, NIST SP 800-53 Rev. 5, MAGERIT v3, y CIS Controls v8 para controles específicos, e ITIL 4 y TOGAF Ver 10 para operaciones y arquitectura tecnológica. Este marco integral asegura la escalabilidad y resiliencia operativa, incorporando planificación, participación Multi-Actor, consideraciones éticas, legales, sociales, y estrategias de sostenibilidad.

La finalidad de esta propuesta es proporcionar una guía técnica precisa que permita a las organizaciones de investigación medioambiental proteger datos sensibles, garantizar la continuidad operativa, y cumplir con estándares globales, abordando las particularidades de entornos distribuidos mediante un enfoque sistemático y sostenible.

1.1 Planteamiento del Problema

La evolución de los proyectos de investigación en el ámbito medioambiental ha integrado intensivamente tecnologías de la información en ecosistemas tecnológicos dinámicos y heterogéneos, generando nuevos riesgos para la seguridad de datos sensibles, como registros de biodiversidad, mediciones climáticas en tiempo real y localizaciones exactas de especies protegidas (Cole et al., 2020). Estos datos se gestionan mediante arquitecturas tecnológicas que integran sensores IoT diseñados para operar en condiciones adversas, redes de transmisión como LoRaWAN que aseguran la conectividad en zonas remotas, plataformas de análisis en la nube y bases de datos geoespaciales que permiten gestionar grandes volúmenes de información distribuida (Luna-López et al., 2021). Aun así, cada componente tecnológico introduce riesgos específicos que comprometen la seguridad, integridad y disponibilidad de los datos, conforme a 7.2.1 ("Identificar y describir los riesgos de seguridad de la información") de ISO/IEC 27005:2022. A lo anterior se añade la interoperabilidad entre estos sistemas heterogéneos, que amplifica las vulnerabilidades y crea puntos importantes de exposición, afectando tanto la calidad de la investigación como la protección de los ecosistemas que buscan preservarse (Radanliev et al., 2020).

Con el fin de profundizar en esta problemática, es preciso destacar que la criticidad de la seguridad en este dominio no se deriva únicamente de la complejidad tecnológica, sino de la naturaleza intrínseca de la información gestionada. A diferencia de los activos de datos en otros sectores, la información medioambiental abarca un espectro de alta sensibilidad, cuyo compromiso puede tener consecuencias directas y, en ocasiones, irreversibles. El modelo debe, por tanto, estar preparado para proteger un conjunto heterogéneo de activos que incluye, entre otros: coordenadas geoespaciales precisas de áreas de anidación o hábitats de especies en peligro de extinción, cuya exposición facilitaría actividades de caza furtiva o la degradación de ecosistemas; datos genéticos de especies endémicas, susceptibles de biopiratería y explotación comercial no autorizada; series temporales de mediciones de contaminantes en fuentes hídricas, cuya manipulación podría afectar la salud pública y las decisiones regulatorias; así como información etnográfica sobre el uso de recursos por parte de comunidades locales, la cual está protegida por consideraciones éticas y de privacidad.

Esta sensibilidad inherente a los datos magnifica los riesgos asociados a cada componente tecnológico. Los sensores IoT, por ejemplo, desplegados en entornos remotos, son particularmente susceptibles a configuraciones inseguras que permiten accesos no autorizados a esta información delicada (Aghaei et al., 2023). La ausencia de cifrado desde la captura inicial facilita la intercepción de mediciones climáticas, comprometiendo así su confidencialidad, tal como lo ilustra el trabajo de (Shome et al., 2025), al proponer un índice de vulnerabilidad para especies que destaca cómo la pérdida de datos sobre su distribución puede facilitar actividades ilegales.

Junto con los riesgos relacionados con sensores IoT, las redes LoRaWAN enfrentan amenazas particulares debido a su función en áreas remotas. Estas redes, de gran importancia para conectar sensores en zonas sin infraestructura tradicional, enfrentan amenazas que afectan directamente la continuidad de la recolección de datos (Maurya et al., 2025). Los ataques de interferencia (jamming) interrumpen la transmisión en tiempo real, lo que puede comprometer estudios climáticos de alta sensibilidad. Sumado a esto, las debilidades en los esquemas de autenticación abren la puerta a nodos maliciosos, mientras que los ataques de repetición afectan la integridad de los registros de biodiversidad. Una interferencia prolongada en un proyecto de monitoreo forestal demostró cómo este tipo de fallas retrasó la detección de un incendio, agravando la pérdida de hábitats (Yasmin et al., 2020).

Por su parte, las plataformas en la nube introducen otros desafíos en términos de seguridad y gestión de la información. La flexibilidad que ofrecen para el análisis y almacenamiento de datos se ve contrarrestada por la posibilidad de errores en la configuración de los controles de acceso (IAM), que pueden exponer la información a actores no autorizados (BlackFog, 2025). La dependencia de terceros introduce también riesgos relacionados con la soberanía de los datos, mientras que los ataques de denegación de servicio (DDoS) interrumpen la disponibilidad de la información en momentos importantes, afectando las decisiones para la toma de decisiones (Khoda Parast et al., 2022). Una filtración en una plataforma de análisis climático permitió el acceso no autorizado a datos geoespaciales de alto valor, comprometiendo la planificación de áreas protegidas (Alouffi et al., 2021).

Complementariamente, las bases de datos geoespaciales requieren una atención especial por el carácter altamente sensible de la información que manejan. (Weekers et al., 2021) analizan cómo las áreas marinas protegidas enfrentan desafíos debido a la pesca ilegal, destacando la

importancia de gestionar adecuadamente los datos geoespaciales para prevenir actividades ilícitas. Este tipo de activos es vulnerable a técnicas de Re-Identificación, incluso cuando los datos han sido anonimizados. También, amenazas técnicas como las inyecciones SQL pueden alterar grandes volúmenes de información, y la falta de segmentación en controles de acceso expone datos importantes a actores malintencionados. Por ejemplo, el estudio de (ALI GUMA et al., 2025), destaca cómo los cazadores furtivos pueden explotar datos GPS de sistemas de seguimiento de vida silvestre para localizar especies en peligro, subrayando la necesidad de proteger la información geoespacial en proyectos de conservación. (Lopes et al., 2025) examina las consecuencias no intencionadas de las áreas marinas protegidas que excluyen a las comunidades locales, como en el caso de la Estación Ecológica de Tamoios en Brasil.

Aun así, más allá de estos riesgos particulares, la integración tecnológica configura un entorno aún más complejo. Las diferencias entre protocolos, formatos y estándares de seguridad generan brechas que pueden ser explotadas para manipular o comprometer la información. La falta de validaciones rigurosas durante la conversión de datos desde sensores hacia plataformas en la nube aumenta el riesgo de errores que afectan la integridad de las mediciones climáticas. Las divergencias entre los mecanismos de autenticación de LoRaWAN y de los sistemas en la nube permiten accesos no autorizados durante las transferencias de datos. Este panorama se agrava cuando se consideran las infraestructuras dispares de los múltiples actores involucrados, lo que genera un entorno donde los modelos de seguridad genéricos resultan claramente insuficientes. (Enemosah & Ifeanyi, 2024), exploran cómo la integración de dispositivos IoT y sistemas SCADA en entornos automatizados introduce desafíos importantes de ciberseguridad, especialmente al utilizar plataformas en la nube. Se discuten marcos de seguridad en la nube que emplean arquitecturas de confianza cero, sistemas de detección de intrusos y protocolos mejorados con aprendizaje automático para proteger la integridad de los datos y la resiliencia operativa.

Como resultado, estas vulnerabilidades integradas se traducen en impactos ambientales concretos y medibles. La exposición de localizaciones sensibles facilita la explotación ilegal de recursos, disminuyendo poblaciones importantes y alterando el equilibrio de los ecosistemas. Del mismo modo, la manipulación de datos climáticos clave puede provocar decisiones desacertadas en la gestión ambiental, afectando negativamente la asignación de recursos ante emergencias como incendios o inundaciones. El blog (Clinton Boyda & D4H, 2022) analiza cómo el cambio climático

está afectando la gestión de emergencias, destacando la importancia de datos precisos y actualizados para una respuesta efectiva ante desastres, en contraste el informe (CITES, 2021) destaca cómo la caza furtiva y el comercio ilegal están afectando a las poblaciones de jaguares en América Latina, y cómo la exposición de datos sensibles sobre la ubicación de estas especies puede facilitar actividades ilegales que amenazan su supervivencia.

Estos impactos ambientales no son hipotéticos; diversos incidentes reales documentados respaldan la magnitud del problema. En el artículo (World Bank Group, 2024) destaca cómo la tecnología, incluyendo trampas fotográficas con sensores de movimiento y drones, se utiliza para monitorear y proteger a los jaguares en la Amazonía. La recopilación y análisis de datos mediante inteligencia artificial permite identificar tendencias en el movimiento y uso del hábitat de los jaguares, facilitando la detección temprana de amenazas como la caza furtiva. Del mismo modo, el estudio (Abdullah Khan et al., 2024) presenta una estrategia para combatir la tala ilegal mediante el uso de dispositivos IoT equipados con inteligencia artificial. Los sensores monitorean continuamente los sonidos del entorno forestal, y el componente de IA utiliza métodos de aprendizaje automático para identificar actividades de tala ilegales, generando notificaciones en tiempo real que permiten a las agencias de aplicación de la ley intervenir rápidamente. En otro artículo (Ankit Dubey et al., s. f.) se aborda los desafíos de privacidad y seguridad asociados con los datos geoespaciales en la era digital. Destaca cómo la exposición de datos sensibles puede facilitar actividades ilegales, como la caza furtiva y la explotación de recursos naturales, afectando negativamente a la biodiversidad y al equilibrio de los ecosistemas.

La participación de múltiples actores, como universidades, entidades gubernamentales, organizaciones no gubernamentales y empresas privadas, introduce complejidades adicionales debido a sus diferentes expectativas y prioridades, conforme a la Cláusula 4.2 “Comprender las necesidades y expectativas de las partes interesadas” de ISO/IEC 27001:2022. Mientras los investigadores requieren acceso ágil y fiable a los datos para respaldar sus análisis científicos, las autoridades gubernamentales velan por el cumplimiento normativo y la protección de datos sensibles. Las organizaciones no gubernamentales priorizan la confidencialidad para proteger a las comunidades locales, mientras que las empresas privadas necesitan asegurar la resiliencia operativa que les permita integrar nuevas tecnologías sin aumentar su exposición al riesgo. Esta diversidad de intereses acentúa la dificultad de establecer controles coherentes que respondan

simultáneamente a todas estas exigencias. En el estudio (Valdez et al., 2023) se presenta un enfoque de Co-Diseño para mejorar el flujo de información sobre biodiversidad en los Andes Tropicales. Involucra a múltiples partes interesadas, incluyendo investigadores, gobiernos, ONG y comunidades locales, para desarrollar indicadores de biodiversidad que satisfagan las diversas necesidades y expectativas.

Como síntesis, la Figura 1 “Necesidad de un modelo de seguridad”, presenta las razones que justifican la necesidad de un enfoque específico, incluyendo la creciente sofisticación de las amenazas digitales, las deficiencias en capacitación, la evolución constante de las normativas y la transformación digital de los proyectos ambientales. La disparidad en los niveles de madurez en ciberseguridad entre los distintos actores, junto con la ausencia de marcos metodológicos adecuados, incrementa la vulnerabilidad de estos entornos. Los modelos genéricos de seguridad, pensados para infraestructuras homogéneas, no son capaces de responder a las particularidades que presentan la heterogeneidad tecnológica, la sensibilidad de los datos geoespaciales y las complejidades organizativas propias de este tipo de proyectos.

Figura 1

Necesidad de un modelo de seguridad



Fuente: Elaboración y Adaptación(Freepik, s. f.)

Nota: Las imágenes vectoriales utilizadas a lo largo del documento fueron obtenidas de Freepik.com. Todas ellas están sujetas a la licencia de uso estándar de dicha plataforma

Al final, para comprender la magnitud de estos desafíos, La Figura 1 presenta los factores determinantes que hacen necesario un enfoque específico de seguridad para los proyectos de investigación medioambiental. Se destacan la creciente sofisticación de las amenazas digitales sobre infraestructuras importantes (Cámara de Comercio Internacional España, 2024), las brechas en la capacitación que amplifican el riesgo humano, la constante evolución del entorno regulatorio, y la transición digital de proyectos tradicionales que requiere integrar tecnologías emergentes de forma segura (Triplett, 2022). También, se considera la complejidad de coordinar múltiples organismos e instituciones, junto con la actual ausencia de marcos metodológicos adaptados a estos entornos (Gordon et al., 2021). Considerando esta representación visual, se evidencia que los desafíos no solo justifican la necesidad de un enfoque especializado, sino que también introducen las condiciones estructurales que afectan directamente la gestión de la seguridad en estos proyectos. La gestión de datos sensibles y la participación de múltiples actores con distintos niveles de madurez en seguridad amplifican los riesgos y exigen soluciones adaptadas (Radanliev et al., 2020). Esta complejidad tecnológica y organizativa requiere un análisis detallado para garantizar la protección efectiva de la información.

En síntesis, el problema fundamental que esta investigación busca resolver radica en la incapacidad de los modelos de seguridad de la información convencionales para ofrecer una protección robusta y adaptada a las exigencias de los proyectos de investigación medioambiental. Dicha insuficiencia se manifiesta en tres dimensiones críticas:

- **La complejidad inherente al ecosistema operativo**, que se caracteriza por una marcada heterogeneidad tecnológica integrando desde redes de sensores IoT hasta infraestructuras en la nube, una amplia dispersión geográfica y la necesaria colaboración entre múltiples actores institucionales (universidades, ONGs, entidades gubernamentales) que presentan niveles dispares de madurez en ciberseguridad.
- **La naturaleza misma de los activos de información**, cuya alta sensibilidad como en el caso de datos geoespaciales sobre biodiversidad o series temporales de mediciones climáticas eleva significativamente el perfil de riesgo.
- **El impacto potencial de una brecha de seguridad**, el cual trasciende la esfera económica o reputacional, pudiendo ocasionar daños ecológicos y sociales directos e

irreversibles, una variable crítica que los marcos de seguridad tradicionales no están diseñados para gestionar con la profundidad y especificidad que se requiere.

¿Cómo estructurar conceptualmente el diseño de un modelo de seguridad de la información que permita proteger, clasificar y gestionar de forma efectiva activos sensibles en entornos de investigación medioambiental?

1.2 Justificación

La problemática planteada en la sección anterior pone de manifiesto una diferencia significativa entre la estructura normativa predominante en la gestión de la seguridad de la información y las condiciones reales de operación en proyectos de investigación científica con enfoque medioambiental. Esta diferencia no solo afecta la aplicabilidad de los controles técnicos, sino también la viabilidad de los procesos de gobernanza, la trazabilidad de los datos y el tratamiento de riesgos. Por esta razón, se considera técnicamente necesario desarrollar un modelo que complemente los marcos existentes y los adapte a un entorno distribuido, multiactor y tecnológicamente diverso.

No obstante, la justificación técnica de este modelo no se limita al cumplimiento normativo, sino que se fundamenta en la demostración de una brecha conceptual y operativa que los marcos de seguridad genéricos no logran cubrir. Para exponer esta brecha, se realiza un análisis comparativo que contrasta los requerimientos del sector medioambiental con los de entornos corporativos tradicionales. Esta diferenciación es un paso argumentativo necesario para demostrar el valor de este diseño conceptual y la pertinencia de una solución especializada. Los factores que se presentan a continuación de manera sintética, serán desarrollados y sustentados con mayor profundidad en la Sección 3.4 de este documento.

En primer término, la naturaleza de los activos de información es sustancialmente distinta. Mientras que en sectores corporativos tradicionales el valor principal de los datos radica en su confidencialidad y en el cumplimiento de regulaciones sobre sus procesos de negocio, en la investigación medioambiental los activos tales como registros de biodiversidad, coordenadas de ecosistemas frágiles o series temporales de variables climáticas son, con frecuencia, irremplazables. La pérdida o alteración de un dato de negocio puede derivar en consecuencias

económicas y reputacionales de importancia; no obstante, la exposición no controlada de la ubicación de una especie en peligro de extinción puede desencadenar un daño ecológico irreversible. Por consiguiente, el modelo de seguridad debe priorizar la integridad y la protección a largo plazo de los datos, con un enfoque que trasciende la simple confidencialidad.

En segundo término, el contexto operativo introduce un conjunto de riesgos que los modelos estándar no suelen contemplar. Las organizaciones en dichos sectores operan desde centros de datos con perímetros de seguridad definidos y una infraestructura centralizada y controlada. Por el contrario, los proyectos de investigación medioambiental dependen de una infraestructura tecnológica distribuida y expuesta a condiciones de campo adversas, que incluye sensores desplegados en áreas remotas, vehículos aéreos no tripulados (drones) y redes de comunicación de baja potencia. Este escenario, donde los supuestos de homogeneidad estructural de estándares como ISO/IEC 27001:2022 dejan de ser válidos, introduce una combinación de riesgos físicos, ambientales y de transmisión que exigen la implementación de controles de seguridad híbridos. A modo ilustrativo, el control 8.1 “Dispositivos finales de usuario” de la ISO/IEC 27002:2022, si bien establece la necesidad de proteger dichos dispositivos, no contempla los escenarios de operación en zonas remotas, con conectividad limitada y sin presencia técnica local, que son habituales en este campo.

Finalmente, la estructura de gobernanza constituye otro factor determinante. Un modelo de seguridad para sectores corporativos se diseña, por lo general, para una organización con una estructura jerárquica y líneas de autoridad definidas. El modelo propuesto en este trabajo, en cambio, debe ser capaz de gestionar una colaboración compleja y descentralizada entre múltiples actores universidades, ONGs, entidades gubernamentales y comunidades locales, cada uno con su propia cultura organizacional y distinto nivel de madurez en materia de seguridad. Por ello, y en línea con el principio de responsabilidad de la sección 5.6 "Rendición de Cuentas" de ISO/IEC 38500:2024, resulta relevante establecer responsabilidades claras en contextos donde los derechos de gestión están compartidos sin una autoridad central consolidada.

Desde la perspectiva de la gestión de riesgos, es pertinente considerar los lineamientos de ISO/IEC 27005:2022, cuya sección 7.3 “Análisis de los Riesgos de Seguridad de la Información” indica que la evaluación debe atender al entorno específico en el que los sistemas operan. Este nivel de análisis es indispensable en los entornos interinstitucionales distribuidos que nos ocupan.

Adicionalmente, y en concordancia con la sección 5.3 “Integración” de ISO 31000:2018, el marco de gestión del riesgo debe incorporarse dentro de todos los procesos relevantes del proyecto.

Por lo tanto, existe una justificación técnica clara y normativamente respaldada para diseñar un modelo de seguridad de la información adaptado a las condiciones específicas de los proyectos ambientales. En particular, este modelo debe responder a las siguientes condiciones estructurales:

- Diversidad tecnológica operativa: coexistencia de sensores, redes satelitales, dispositivos móviles, análisis en la nube y almacenamiento descentralizado.
- Asimetría institucional: participación de entidades con distintos niveles de madurez en gobernanza, infraestructura y políticas de seguridad.
- Falta de trazabilidad robusta: debilidades en mecanismos de control del ciclo de vida del dato, desde su origen hasta su consumo.
- Fragmentación normativa: coexistencia de marcos legales y normativos distintos, sin articulación funcional ni mecanismos de interoperabilidad operativa.

En conclusión, este modelo pretende enriquecer los marcos normativos internacionales al proporcionarles capacidad operativa en entornos no convencionales. Su enfoque se centra en desarrollar una arquitectura técnica coherente, escalable y funcional, diseñada para proteger la información crítica en condiciones operativas complejas, dinámicas y distribuidas.

1.3 Alcances y Limitaciones del Modelo

1.3.1 *Alcance del Diseño del Modelo*

Esta propuesta de modelo de seguridad de la información ha sido diseñada para responder a los requerimientos técnicos, organizativos, y normativos que enfrentan los proyectos de investigación medioambiental, especialmente aquellos que operan en entornos distribuidos, interinstitucionales, y con sistemas tecnológicos avanzados, como dispositivos de monitoreo climático y sistemas de procesamiento distribuido (Gamboa & Pulido, 2024). Su alcance se limita al plano conceptual y metodológico, sin implicar la ejecución directa de medidas operativas ni la validación práctica de sus componentes.

En términos generales, el modelo plantea una estructura referencial para el diseño de políticas, controles, y procesos de seguridad de la información que puedan integrarse en contextos académicos, públicos, o mixtos. Se basa en la armonización de lineamientos establecidos en normas como **ISO/IEC 27001:2022** (International Organization for Standardization & International Electrotechnical Commission, 2022), **ISO/IEC 27002:2022** (International Organization for Standardization; International Electrotechnical Commission, 2022a)**, ISO/IEC 27005:2022,** (International Organization for Standardization; International Electrotechnical Commission, 2022b)**, ISO/IEC 38500:2024-02** (International Organization for Standardization; International Electrotechnical Commission, 2024)**, ISO 55002:2018 ,** (International Organization for Standardization; International Electrotechnical Commission, 2018)**, COBIT 2019** (Information Systems Audit and Control Association (ISACA), 2018)**, NIST SP 800-53 Rev. 5** (National Institute of Standards and Technology, 2020)**, MAGERIT v3**(coordinación de contenidos et al., 20212; Ministerio de Hacienda y Administraciones Públicas, 2012a, 2012b) **, CIS Controls v8** (Center for Internet Security, 2021)**, ITIL 4** (AXELOS, 2019)**, y TOGAF Ver 10** (The Open Group, 2022), adaptándolos al contexto específico de la producción científica ambiental, caracterizado por alta dependencia tecnológica, baja estandarización institucional, y condiciones de conectividad variable.

Con este enfoque, el alcance de la propuesta se orienta a:

- Definir los elementos estructurales de un marco de seguridad adaptable, como políticas para autenticación multifactor, alineado con estándares internacionales.
- Establecer principios operativos para la gestión del riesgo, como controles para sensores remotos, y la protección de activos de información pertinentes.
- Ofrecer una arquitectura de referencia que pueda servir como base para futuras implementaciones por parte de organizaciones interesadas.

El modelo ha sido desarrollado como una herramienta flexible, que puede ser adoptada de manera progresiva, según los niveles de madurez institucional y tecnológica de cada entidad.

1.3.2 *Limitaciones del Diseño Propuesto*

Dado que este documento constituye una propuesta de diseño conceptual y no una implementación ejecutada, sus resultados carecen de evidencia empírica de efectividad operativa. Las recomendaciones formuladas se derivan de marcos teóricos y normativos, requiriendo pruebas de campo alineadas con el enfoque basado en riesgos, retroalimentación institucional, y ciclos iterativos de mejora para su validación.

Otro aspecto es que el modelo no abarca todas las posibles configuraciones organizativas o tecnológicas existentes, como sistemas propietarios cerrados o entornos sin infraestructura digital. Se asume una estructura general basada en proyectos de investigación ambiental distribuidos, lo que implica que condiciones específicas, como operaciones en entornos altamente centralizados o con requisitos regulatorios particulares, demandarían ajustes adicionales.

También, la aplicación práctica del modelo dependerá de la disponibilidad de recursos, como personal capacitado en ciberseguridad, infraestructura de red redundante, y presupuesto adecuado. Estas exigencias limitarían su adopción en contextos con restricciones severas de infraestructura o con experiencia limitada en gestión de seguridad de la información.

Es importante aclarar que esta propuesta no sustituye los sistemas de gestión, normativas internas, ni políticas institucionales existentes. Su propósito es ofrecer un marco complementario que fortalezca la alineación con estándares internacionales, como ISO/IEC 27001:2022, mejore la trazabilidad de los procesos, y facilite la gestión compartida de la seguridad en contextos de investigación científica colaborativa.

1.4 Objetivos

1.4.1 *Objetivo General*

Diseñar un modelo de seguridad de la información con el propósito de establecer un conjunto de prácticas, políticas y tecnologías que aseguren la protección y gestión adecuada de activos de información en proyectos de investigación medioambientales.

1.4.2 *Objetivos Específicos*

- Analizar las características específicas asociadas a la seguridad de la información en proyectos de investigación en el área medioambiental, en contraste con otros modelos definidos para la gestión de proyectos en general.
- Identificar requisitos específicos de Seguridad de la Información para la Investigación Medioambiental a través de la valoración de riesgo de los activos y la tecnología operativa usada por los investigadores.
- Clasificar los requisitos identificados desde la perspectiva de la criticidad del riesgo inherente de los activos y la madurez tecnológica.
- Definir controles preventivos, detectivos, correctivos o disuasivos para gestionar los riesgos catalogados como de criticidad medio, alto y crítico en el análisis de riesgos.
- Segmentar los controles definidos teniendo en cuenta características convergentes a nivel de infraestructura, uso y funcionalidad de los activos a salvaguardar.
- Documentar el modelo de seguridad de la información para proyectos de investigación medioambientales.

Capítulo 2: Fundamentos Teóricos y Marcos de Referencia

El marco de referencia para el Modelo de Seguridad de la Información en proyectos de investigación medioambiental se fundamenta en un conjunto de elementos conceptuales y metodológicos que, en conjunto, proporcionan una estructura sólida para entender y abordar la protección de datos sensibles en este ámbito. Cada componente del marco se centra en analizar aspectos específicos de la seguridad de la información, buscando asegurar que el modelo sea completo, actualizado y adaptado a las necesidades particulares de la investigación medioambiental (Peña-Casanova, 2020).

Dentro del marco teórico que sustenta el presente trabajo, resulta pertinente definir el concepto de Diseño y, de forma específica, el Diseño de un Modelo de Seguridad de la Información, dado que esta monografía aborda precisamente la conceptualización de dicho modelo. En un sentido amplio, el Diseño constituye el proceso de concepción, planificación y especificación para la construcción o realización de un objeto, sistema o proceso. Implica la definición de su forma, función y operación, sirviendo como la fase de especificación detallada que precede a la implementación práctica. Es una actividad que busca abordar problemáticas o satisfacer necesidades, considerando variables como el propósito, el contexto y las restricciones inherentes al proyecto o sistema a desarrollar.

El concepto de diseño se manifiesta de diversas maneras según el ámbito de aplicación. Se identifican, entre otros:

- Diseño Industrial: Orientado a la conceptualización de productos manufacturados.
- Diseño Gráfico: Enfocado en la comunicación a través de medios visuales.
- Diseño Arquitectónico: Relacionado con la planificación de estructuras y espacios.
- Diseño de Software: Dirigido a la conceptualización de la arquitectura y comportamiento de sistemas informáticos.
- Diseño de Procesos: Centrado en la definición de flujos de trabajo para alcanzar resultados.
- Diseño de Sistemas: Abocado a la conceptualización de la estructura y componentes de sistemas complejos, como los sistemas de gestión.

Aplicado al campo de la Gestión de Seguridad de la Información, el Diseño de un Modelo de Seguridad de la Información se define como el proceso de conceptualizar y especificar la estructura, componentes, políticas, procedimientos y controles necesarios para establecer y operar un marco de seguridad de la información en un contexto organizacional particular. En el contexto de esta monografía, este concepto se refiere a la especificación conceptual detallada de la estructura del modelo propuesto, fundamentada en:

- Los requisitos de seguridad establecidos.
- Los riesgos evaluados.
- Las directrices de marcos y normas de GSI reconocidos (ISO 27001, ISO 27002, Magerit, NIST, entre otros).
- Las características específicas del contexto organizacional y tecnológico de los proyectos de investigación medioambiental.

Este proceso de diseño no corresponde a la implementación práctica. En cambio, representa la definición conceptual de las medidas de protección (controles) y la organización de la gestión (políticas, roles, procesos) que, al ser llevadas a la práctica, permitirían alcanzar los objetivos de seguridad y manejar los riesgos identificados. Representa la etapa de planificación precisa antes de su puesta en marcha.

2.1 Marco Teórico

Se exploran las teorías y principios fundamentales que subyacen a la seguridad de la información. Esta sección sienta las bases conceptuales, proporcionando una visión clara de cómo se aplican estos principios en el contexto de la investigación medioambiental y por qué son importantes para la integridad y confidencialidad de los datos (Antonio et al., 2024).

2.1.1 *Seguridad de la Información*

De acuerdo con la norma ISO 27000, la Seguridad de la Información se define como la preservación de la confidencialidad, integridad y disponibilidad de la información. La confidencialidad garantiza que la información solo sea accesible por personas, entidades o procesos autorizados. La integridad asegura la exactitud y completitud de los datos, evitando

modificaciones no autorizadas. La disponibilidad permite que la información esté accesible y utilizable cuando sea requerida. Además, esta definición puede complementarse con otros atributos esenciales como la autenticidad, que certifica la identidad de los usuarios y la validez de los datos; la responsabilidad, que implica la asignación clara de funciones y obligaciones; el no repudio, que evita la negación de acciones realizadas; y la confiabilidad, que asegura la correcta operación de los sistemas de información. Estos principios son fundamentales para la protección de los activos de información y la gestión eficaz de los riesgos asociados a su uso.

2.1.2 *Teoría de la Información y Seguridad*

En la actualidad, donde la tecnología impregna cada aspecto de nuestras vidas, la protección de datos y sistemas se ha vuelto un pilar necesario en una sociedad interconectada. La constante interacción con tecnologías en el trabajo, el ocio y la vida cotidiana nos expone a numerosos riesgos de seguridad. La vulnerabilidad a ciberataques puede tener efectos devastadores, como pérdidas financieras o daños a la reputación. De acuerdo con la ISO/IEC, proteger nuestros sistemas informáticos y datos de accesos y usos no autorizados es una necesidad crítica, destacando la importancia de salvaguardar nuestros recursos tecnológicos ante amenazas en constante evolución (BRICEÑO, 2021).

Por esta razón, el énfasis en la seguridad de la información es innegable en la actualidad, especialmente para las organizaciones públicas que gestionan una cantidad significativa de datos sensibles. El constante aumento de las amenazas cibernéticas ha elevado la importancia de adoptar metodologías sólidas como MAGERIT, las cuales están diseñadas para fortalecer tanto la confidencialidad como la disponibilidad de la información. Este enfoque no solo protege los intereses y la integridad de las organizaciones públicas, sino que también desempeña un papel crítico en la salvaguardia de los datos personales de los ciudadanos, garantizando su privacidad y seguridad. Reflejando esta necesidad de adaptación, la versatilidad de MAGERIT se hace evidente al extender su aplicación a la industria del desarrollo de software, donde contribuye significativamente a validar y controlar los factores de seguridad de la información. En conjunto, estas acciones son esenciales para la construcción de un entorno digital más seguro y confiable en un mundo cada vez más interconectado (Terán Terranova, 2021).

Con el auge de la dependencia en aplicaciones web en la sociedad actual, se plantean desafíos significativos en términos de seguridad de la información. La rápida expansión de estas aplicaciones ha multiplicado los puntos de vulnerabilidad y ha hecho que la gestión de la seguridad sea más compleja que nunca. Dado que la información es un activo crítico tanto para las organizaciones como para los individuos, es fundamental reconocer la importancia de abordar estos riesgos de manera efectiva. La adopción de metodologías sólidas como MAGERIT se vuelve de gran importancia para proteger la confidencialidad, integridad y disponibilidad de los datos en un entorno cada vez más interconectado (Soto Pineda & Autor, 2021).

En el entorno de las Pequeñas y Medianas Empresas (PYMES), estas se desenvuelven en un entorno empresarial cada vez más digitalizado, donde la tecnología desempeña un papel necesario en sus operaciones diarias, abarcando desde la gestión de datos hasta la comunicación con clientes y proveedores. Sin embargo, esta creciente dependencia de la tecnología también conlleva riesgos sustanciales en lo que respecta a la seguridad cibernética. Para lograr este objetivo, se ha desarrollado un enfoque estratégico basado en la selección de estándares de seguridad ampliamente reconocidos, como ISO/IEC 27001 y 27002, además de los Controles Críticos de Seguridad (Controles CIS). Asimismo, se incorporan de manera coherente las directrices proporcionadas por el NIST CSF, un marco de trabajo de ciberseguridad que goza de amplia aceptación y uso (Cabezas Juárez, 2020).

2.1.3 *Principios de Seguridad*

La seguridad de la información es una disciplina que se centra en la protección de los datos y recursos de una organización. Para ello, se basa en una serie de principios fundamentales que garantizan la confidencialidad, integridad, y disponibilidad de la información, así como la autenticidad, no repudio y control de acceso. A continuación, se describen estos principios y su importancia en el ámbito de la seguridad de la información (Pira & Andrea, 2020).

2.1.3.1 Confidencialidad.

La confidencialidad asegura que la información solo sea accesible a las personas autorizadas y esté protegida contra el acceso no autorizado. Este principio es importante para prevenir la divulgación indebida de información sensible, ya sea intencional o accidental. Las

técnicas comunes para mantener la confidencialidad incluyen la criptografía, el uso de contraseñas seguras, y las políticas de control de acceso basadas en roles (RBAC). Según la norma ISO 27001, la confidencialidad es necesaria para la protección de datos personales, secretos comerciales y otra información sensible que, de ser divulgada, podría causar daños significativos a una organización (Poma Moya, 2020).

2.1.3.2 Integridad.

La integridad se refiere a la exactitud y completitud de la información y los métodos para procesarla. Este principio garantiza que los datos no sean alterados de manera no autorizada, manteniendo así su confiabilidad y precisión. La integridad se protege mediante controles como las sumas de verificación, las firmas digitales y los sistemas de detección de intrusiones. Además, la gestión adecuada de los cambios y auditorías regulares contribuyen a mantener la integridad de los datos (Escobar Quintana & Alarcón Pérez, 2023).

2.1.3.3 Disponibilidad.

La disponibilidad asegura que la información y los recursos estén accesibles a los usuarios autorizados cuando sea necesario. Este principio implica la implementación de medidas para mantener el funcionamiento continuo de los sistemas de información, incluso en situaciones de fallo o ataque. Las técnicas de respaldo, los sistemas de recuperación ante desastres y la redundancia son esenciales para garantizar la disponibilidad. La norma ISO 31000 destaca la importancia de la disponibilidad en la gestión de riesgos, asegurando que los recursos críticos estén operativos y accesibles en todo momento (De Originalidad & Primarias, 2024).

2.1.3.4 Autenticidad.

La autenticidad verifica que los usuarios, dispositivos o sistemas son quienes dicen ser. Este principio es necesario para evitar el acceso no autorizado y garantizar la veracidad de las transacciones electrónicas. Los mecanismos de autenticación incluyen contraseñas, tarjetas inteligentes, biometría y certificados digitales. La autenticidad se refuerza mediante políticas de autenticación robustas y la implementación de protocolos seguros, como SSL/TLS, que aseguran la identidad de las partes involucradas en la comunicación (Campos et al., 2020).

2.1.3.5 No Repudio.

El no repudio asegura que una transacción o comunicación no pueda ser negada por ninguna de las partes involucradas. Este principio es necesario en entornos donde la prueba de origen y la integridad de los datos son importantes, como en las transacciones financieras y los contratos electrónicos. Las firmas digitales y los registros de auditoría son herramientas clave para garantizar el no repudio, proporcionando evidenc(Alejandra & Useche, 2021)ones realizadas (Alejandra & Useche, 2021).

2.1.4 *Modelos de Amenazas y Vulnerabilidades*

La comprensión y gestión de las amenazas y vulnerabilidades es una parte integral de la seguridad de la información. Los modelos de amenazas y vulnerabilidades permiten a las organizaciones identificar, evaluar y mitigar los riesgos a los que están expuestas. A continuación, se describe en detalle estos conceptos y su importancia en el ámbito de la seguridad de la información(Alcibiadis & Cartagena, 2021) .

2.1.4.1 Modelos de Amenazas.

Un modelo de amenazas es una representación sistemática de las posibles amenazas que pueden afectar la seguridad de un sistema de información. Estos modelos ayudan a las organizaciones a anticipar posibles ataques y a diseñar estrategias de defensa adecuadas (Farias Estacio & Centeno Córdova, 2024).

2.1.4.2 Vulnerabilidades.

Las vulnerabilidades son debilidades o fallos en un sistema de información que pueden ser explotados por amenazas para comprometer la seguridad del sistema. Las vulnerabilidades pueden encontrarse en software, hardware, redes, procesos y en las personas que interactúan con el sistema. La gestión de vulnerabilidades es un proceso continuo que incluye la identificación, evaluación, tratamiento y monitoreo de las mismas(Mafla Flores, 2024).

2.1.5 *Activos de Información*

Los activos de información se definen como todos aquellos recursos que poseen valor para una organización y que son indispensables para el cumplimiento de sus objetivos. Estos activos pueden incluir tanto elementos tangibles, como bases de datos y sistemas informáticos, como intangibles, tales como el conocimiento y la propiedad intelectual. Por ejemplo, en un proyecto de investigación, los registros de cambios en la biodiversidad, los datos meteorológicos históricos y los estudios sobre la contaminación del agua constituyen activos clave que deben ser protegidos para garantizar la validez y continuidad de la investigación. Es importante destacar que la seguridad de estos activos no solo se refiere a su protección frente a accesos no autorizados, sino también a la preservación de su integridad y disponibilidad. Esto implica implementar controles que eviten su alteración o pérdida, asegurando que la información esté accesible cuando sea necesaria para la toma de decisiones críticas. En resumen, la correcta gestión y protección de los activos de información es un pilar necesario para mantener la confiabilidad y el éxito de cualquier proyecto de investigación (Landoll, 2005).

2.1.6 *Riesgos y Controles*

Los riesgos se refieren a la posibilidad de que una amenaza explote una vulnerabilidad en un activo de información, causando un impacto negativo en la organización. Estos riesgos pueden manifestarse de diversas maneras, como ataques cibernéticos, fallos técnicos, errores humanos o desastres naturales, y su impacto puede variar desde la interrupción temporal de un servicio hasta la pérdida irreversible de datos críticos. Para mitigar estos riesgos, se implementan controles, que son medidas diseñadas para prevenir, detectar, corregir o disuadir las amenazas (Duggineni, 2023).

2.2 Gestión del Riesgo y Seguridad de la Información.

La gestión del riesgo en seguridad de la información es un proceso estructurado y continuo que permite a las organizaciones identificar, evaluar y tratar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de sus activos de información. En este contexto, las normas ISO/IEC 27005:2022, ISO 31000:2018 y MAGERIT v3 proporcionan marcos

metodológicos complementarios para una administración efectiva de los riesgos asociados a la tecnología y los sistemas de información (Ortiz-Garcés et al., s. f.).

2.2.1 *Identificación de Riesgos*

La ISO/IEC 27005:2022 establece un enfoque detallado para la identificación de riesgos en la seguridad de la información, La Sección 7.2 cubre la aplicación de la evaluación de riesgos, y la Sección 6.4.2 establece los criterios de aceptación del riesgo, enfatizando la necesidad de comprender el contexto organizacional, los activos críticos y las posibles amenazas que podrían comprometer la seguridad. En complemento, ISO 31000:2018 introduce principios para la gestión del riesgo en un nivel estratégico, asegurando que la identificación de amenazas no solo se enfoque en el ámbito tecnológico, sino también en factores organizacionales y regulatorios. Por su parte, MAGERIT v3 proporciona una metodología específica para el análisis de riesgos en entornos tecnológicos, considerando dependencias entre activos, mapeo de amenazas y evaluación de vulnerabilidades dentro de los sistemas de información (Marín Velásquez et al., 2024) .

2.2.2 *Evaluación y Tratamiento de Riesgos*

El análisis de riesgos debe considerar la probabilidad de ocurrencia de los eventos identificados y su posible impacto en la organización. ISO/IEC 27005:2022 propone un enfoque estructurado basado en métricas cuantitativas y cualitativas para determinar el nivel de exposición al riesgo y las medidas de mitigación adecuadas. ISO 31000:2018 establece un enfoque estructurado para la gestión de riesgos. La Sección 6.4 Identificación de riesgos, describe el proceso de identificación, análisis y valoración de riesgos, mientras que la Sección 5.7.2 Mejora continua, enfatiza la mejora continua mediante la revisión periódica del entorno y las amenazas emergentes. En esta línea, MAGERIT v3 ofrece herramientas analíticas como la matriz de riesgos y el cálculo del riesgo residual, lo que facilita la priorización de acciones correctivas y preventivas (Beltrán Hernández et al., 2023).

2.2.3 *Monitoreo Continuo y Gestión de Cambios*

Un elemento importante de la gestión del riesgo es su naturaleza iterativa y su capacidad de adaptación a nuevas amenazas. ISO 31000:2018 destaca la importancia del monitoreo y revisión constantes para asegurar que las estrategias de gestión del riesgo sigan siendo efectivas ante cambios en el entorno. ISO/IEC 27005:2022 refuerza esta idea al sugerir la integración de auditorías periódicas y análisis forenses en la gestión de incidentes. Finalmente, MAGERIT v3 establece un marco metodológico en el que la revisión de riesgos se incorpora en el ciclo de vida de los sistemas de información, permitiendo una gestión proactiva que minimice el impacto de potenciales fallos de seguridad (Buitrago Díaz & Caho Rodríguez, 2024).

2.3 Investigación Medioambiental

La investigación medioambiental se centra en estudiar y encontrar soluciones a problemas relacionados con el medio ambiente. Este campo abarca diversas áreas como la conservación de la biodiversidad, el manejo sostenible de recursos, el desarrollo de energías renovables, el cambio climático, la restauración ecológica, y la evaluación del impacto ambiental, entre otros. Cada uno de estos enfoques tiene como objetivo comprender mejor los procesos naturales y desarrollar estrategias para mitigar los impactos negativos de la actividad humana (-Manabí -Ecuador, 2023).

En este tipo de proyectos, es necesario contar con un modelo de seguridad de la información que proteja los datos y recursos utilizados. Los datos de investigación pueden incluir información sobre biodiversidad, ubicaciones de especies protegidas, datos climáticos y geológicos, entre otros (dc et al., 2024). La protección de estos datos es de suma importancia no solo para el éxito científico de los proyectos, sino también para la preservación de la integridad de los ecosistemas estudiados y la protección de especies vulnerables (Ipiniza et al., 2021).

El cumplimiento de normativas y estándares internacionales de protección de datos es otra consideración importante. Los proyectos deben adherirse a regulaciones específicas que gobiernan la recolección, almacenamiento, procesamiento y difusión de información, asegurando que todas las prácticas estén alineadas con las mejores prácticas de seguridad (Ureña Agüero, 2020).

Finalmente, la naturaleza interdisciplinaria de la investigación medioambiental requiere una gestión coordinada de la seguridad de la información. La colaboración entre diferentes

instituciones y expertos necesita un enfoque coherente y bien estructurado para la protección de datos, asegurando que la información compartida sea precisa, segura y utilizable por todas las partes involucradas(Moresi et al., 2023).

2.3.1 *Categorías en proyectos de investigación medioambiental*

Las categorías en proyectos de investigación medioambiental incluyen una serie de áreas enfocadas en la protección y el manejo responsable del entorno natural. Primero, la conservación de la biodiversidad busca mantener la diversidad biológica y apoyar ecosistemas capaces de adaptarse a los cambios ambientales. (Karina Gutiérrez-Camacho & Magdalena Contreras-Mendoza, 2021).

Por otro lado, el manejo sostenible de recursos se dirige a optimizar el uso de los recursos naturales, garantizando su disponibilidad para las generaciones futuras. En cuanto a la energía, el desarrollo de energías renovables tiene como objetivo reducir la dependencia de los combustibles fósiles, contribuyendo a una reducción de la huella de carbono. Adicionalmente, la investigación sobre cambio climático es importante para crear estrategias de mitigación y adaptación efectivas. La restauración ecológica, por su parte, se enfoca en recuperar áreas degradadas, restaurando funciones esenciales para la estabilidad de los ecosistemas. También, la evaluación del impacto ambiental es importante para comprender y gestionar las consecuencias de las actividades humanas (Mieles-Giler et al., 2024).

En el ámbito educativo, la misión es aumentar la conciencia y comprensión pública sobre los desafíos ambientales, fomentando una participación activa en su solución. En el área tecnológica, la innovación en tecnología ambiental desarrolla herramientas para un monitoreo y protección más eficientes del entorno. El urbanismo sostenible se enfoca en planificar ciudades que minimicen su impacto ambiental, mientras que la gestión de residuos implementa sistemas eficaces para reducir, reutilizar y reciclar desechos. La conservación de aguas y cuencas hidrográficas es importante para garantizar la calidad y disponibilidad del agua, y el monitoreo ambiental ofrece datos constantes para decisiones informadas. La participación comunitaria es clave para asegurar el respaldo necesario a los proyectos ambientales, mejorando su efectividad y sostenibilidad a largo plazo (SUSTENTABLE, 2023).

2.3.2 *Datos Medioambientales*

Los datos medioambientales constituyen un insumo estratégico para la investigación científica, la gestión sostenible y la formulación de políticas públicas. Su análisis permite comprender con mayor precisión fenómenos complejos como el cambio climático, la pérdida de biodiversidad o la degradación de ecosistemas. Estos datos abarcan desde información geoespacial y meteorológica, hasta indicadores físico-químicos, registros biológicos e incluso variables socioeconómicas vinculadas a dinámicas ambientales (Lema Sánchez et al., 2023).

Debido a su naturaleza transversal, los datos ambientales son utilizados por múltiples actores: organismos internacionales, entidades gubernamentales, centros de investigación, organizaciones no gubernamentales y comunidades locales. Esta diversidad de usos y usuarios incrementa la exposición a riesgos de integridad, acceso no autorizado, manipulación o pérdida de disponibilidad (Dormido et al., 2022).

La sensibilidad de estos datos radica no solo en su contenido técnico, sino también en su capacidad para incidir en decisiones de alto impacto político, económico o territorial. Por tanto, su adecuada protección deja de ser una medida técnica opcional para convertirse en una necesidad estratégica. Implementar un modelo de seguridad de la información robusto en este contexto implica garantizar su autenticidad, trazabilidad, disponibilidad y confidencialidad, sin comprometer los principios de acceso abierto o reutilización científica que caracterizan a muchas iniciativas ambientales actuales (Lanegra, s. f.).

La comprensión profunda de los datos medioambientales y su sensibilidad nos conduce inevitablemente a considerar la infraestructura tecnológica que los soporta. Para garantizar la integridad, disponibilidad y confidencialidad de esta información, es indispensable contar con una arquitectura robusta que abarque desde la captura de datos en campo hasta su procesamiento y almacenamiento seguro. En la siguiente sección se detalla la infraestructura crítica necesaria para los proyectos de investigación ambiental, abarcando todos los niveles operativos y tecnológicos que hacen posible una gestión eficiente y segura de la información.

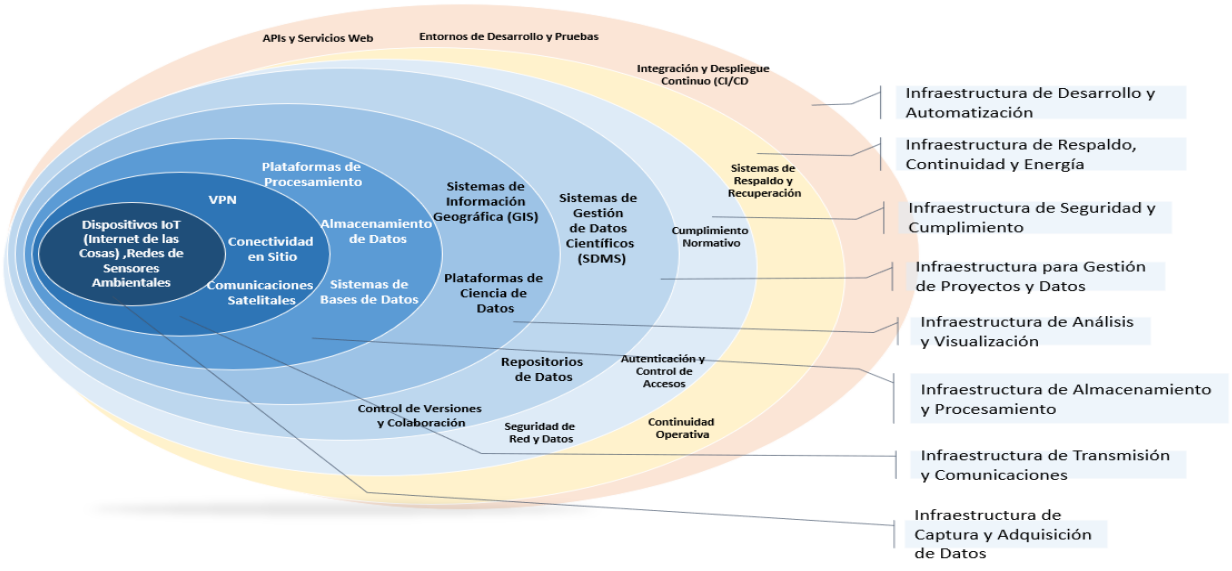
2.3.3 *Infraestructura tecnológica en proyectos de investigación*

La ejecución de proyectos de investigación, como se detalla en la sección 2.3.1, se apoya en una infraestructura tecnológica que debe responder a las necesidades prácticas de recolectar y gestionar datos en entornos muy variados. Como se vio en la sección 2.3.2, los datos ambientales son a menudo dispersos y su valor depende del momento en que se recogen. Por eso, se necesitan soluciones que permitan capturarlos, procesarlos y transmitirlos de manera eficiente.

Para organizar esta complejidad, la infraestructura tecnológica se puede estructurar en una serie de capas funcionales que van desde los dispositivos en campo hasta las plataformas de gestión. La Figura 2 presenta un modelo conceptual de esta estructura, donde los componentes tecnológicos se organizan en capas concéntricas que representan el flujo de la información. El núcleo corresponde a los elementos de captura, y las capas exteriores se expanden para abarcar el procesamiento, el análisis y la gobernanza. Los siguientes apartados explican cada uno de estos niveles en detalle.

Figura 2

Tecnología requerida identificada para proyectos MA



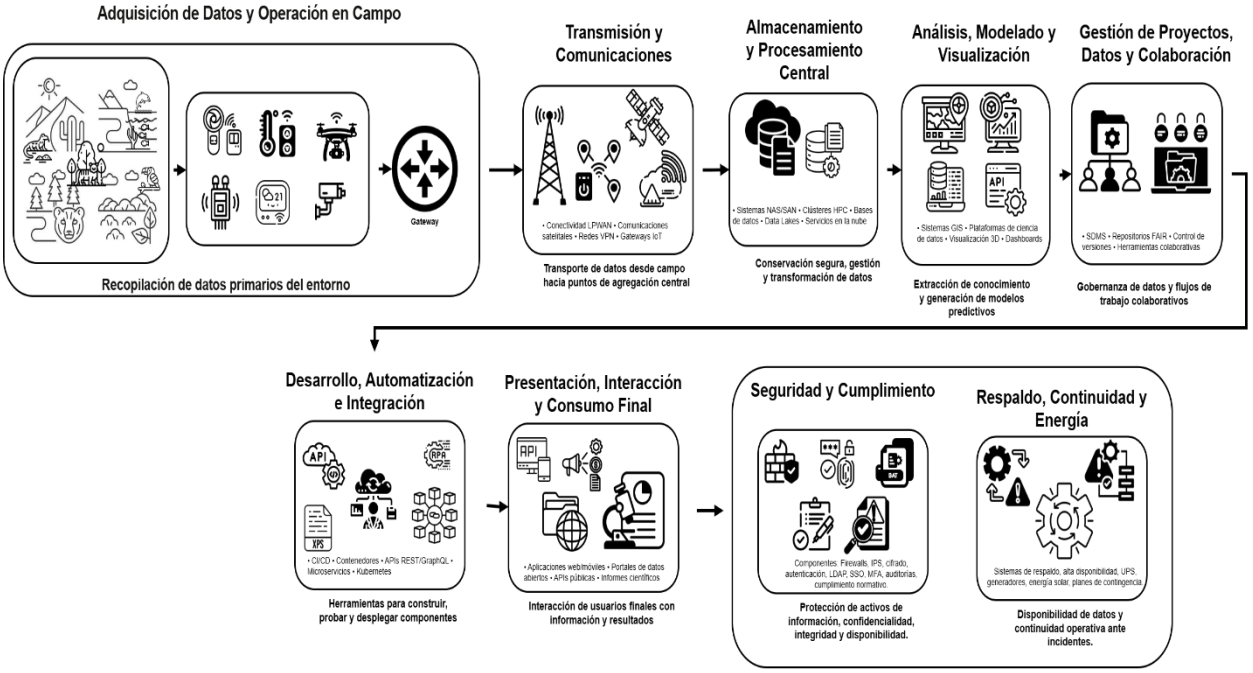
Fuente: Elaboración propia

En esta sección se describen los distintos niveles de infraestructura necesarios para estas actividades, desde los sensores en campo hasta las plataformas de procesamiento y visualización. También se incluyen los sistemas de transmisión, las arquitecturas de almacenamiento, las herramientas de análisis y las medidas de seguridad para mantener la integridad de la información.

Se presentan casos de uso específicos que permiten visualizar cómo estas tecnologías se aplican en proyectos reales, facilitando una referencia práctica para la selección y diseño de la infraestructura en iniciativas de monitoreo y análisis medioambiental. Este flujo de trabajo completo, desde la recolección en campo hasta la protección final de los datos, se representa en la Figura 3. Este diagrama sirve como una hoja de ruta visual para las subsecciones que se detallan a continuación, donde cada bloque del esquema corresponde a una etapa del proceso.

Figura 3

Infraestructura Básica Proyectos Medioambientales



Fuente: Elaboración propia

La Figura ilustra el flujo de trabajo completo y el ciclo de vida de los datos en un proyecto medioambiental típico, desde su origen en campo hasta su consumo final y protección. Este diagrama de flujo sirve como hoja de ruta para las siguientes subsecciones, donde cada bloque principal de la figura se desarrollará en detalle. El proceso inicia con la Adquisición de Datos y

Operación en Campo (Sección 2.3.3.1), seguido por la Transmisión y Comunicaciones (Sección 2.3.3.2), y así sucesivamente, cubriendo todas las etapas hasta la seguridad y el respaldo.

2.3.3.1 Infraestructura de Captura y Adquisición de Datos.

La captura y adquisición de datos marcan el inicio operativo de los proyectos de investigación medioambiental, proporcionando la información base que sustenta análisis posteriores, desde mediciones de calidad del aire hasta registros de dinámica hídrica. Retomando las categorías descritas en 2.3.1 y la sensibilidad de los datos ambientales señalada en 2.3.2, esta infraestructura tecnológica se enfoca en recolectar datos de manera precisa y confiable, incluso en entornos remotos o bajo condiciones adversas como alta humedad o terrenos accidentados. Más allá de la simple recolección, estas soluciones deben operar dentro de un marco que proteja la información desde su generación, alineándose con estándares como ISO/IEC 27001:2022 para mitigar riesgos como la alteración o el robo de datos en campo.

En la práctica, esto implica el uso de herramientas como sensores de bajo consumo, estaciones automatizadas y sistemas móviles que respondan a las demandas reales de los proyectos, donde retrasos o fallos en la captura pueden comprometer plazos y resultados. Por ejemplo, la creciente dependencia de redes IoT para monitoreo en tiempo real según un informe de la IEEE de 2023, adoptadas en un 68% de proyectos ambientales en regiones rurales exige no solo precisión técnica, sino también integración con medidas de seguridad básicas, como cifrado en el punto de captura. Este apartado detalla los elementos principales de esta infraestructura, acompañado de casos prácticos que reflejan su uso en escenarios reales, ofreciendo una visión concreta y profesional de cómo se inicia el flujo de datos en la investigación medioambiental.

Redes de Sensores Ambientales

- Sensores para medir temperatura, humedad, radiación solar, pH, salinidad, calidad del agua y aire: Estos dispositivos permiten la recopilación continua de datos ambientales necesarios para el análisis de ecosistemas.
- Sensores piezoeléctricos para monitoreo sísmico o vibraciones: Utilizados para detectar movimientos tectónicos o vibraciones en estructuras naturales y artificiales.

- Sensores acústicos para monitoreo de fauna o aplicaciones submarinas: Empleados en la detección y estudio de especies marinas mediante la captura de sonidos subacuáticos.
- Cámaras multiespectrales, térmicas e infrarrojas: Utilizadas en teledetección para evaluar la salud de la vegetación, detectar cambios en el uso del suelo y monitorear la temperatura superficial.
- Estaciones meteorológicas automáticas (AWS): Proporcionan datos en tiempo real sobre condiciones climáticas, facilitando estudios de patrones meteorológicos y cambios climáticos.
- Boyas oceanográficas con telemetría para datos marinos: Equipadas con sensores para medir variables como temperatura, salinidad y corrientes marinas, transmitiendo información en tiempo real.
- Drones equipados con sensores LIDAR, RGB, multiespectrales e infrarrojos para mapeo y monitoreo, incluyendo UAV tipo VTOL para misiones de largo alcance: Permiten la generación de modelos digitales del terreno y la evaluación de la cobertura vegetal en áreas extensas.

Caso de uso: En el Golfo de Corcovado, Chile, se implementó el proyecto "The Blue BOAT Initiative", que utiliza boyas inteligentes equipadas con sensores acústicos para monitorear en tiempo real la presencia de ballenas y prevenir colisiones con embarcaciones, contribuyendo a la conservación de cetáceos en la región (Ministerio de Desarrollo Social y Familia. (s.f.)., 2020).

Dispositivos IoT (Internet de las Cosas)

- Controladores programables de campo (PLC) para automatización: Permiten la gestión eficiente de procesos y sistemas en entornos remotos.
- Gateways IoT para integración de datos desde sensores heterogéneos: Facilitan la comunicación y centralización de información proveniente de diversos dispositivos.
- Módulos con conectividad LoRaWAN, Zigbee, NB-IoT o LTE-M para transmisión eficiente en áreas remotas: Aseguran la transferencia de datos en lugares con infraestructura de comunicación limitada.

Caso de uso: Un estudio titulado "River Water Quality Monitoring Using LoRa-Based IoT" propone una solución práctica y de bajo costo basada en la tecnología LoRa para obtener observaciones en tiempo real de parámetros como temperatura, pH, conductividad y turbidez. Los datos recopilados en un nodo sensor se transmiten mediante modulación LoRa a una pasarela para su procesamiento y almacenamiento local en un servidor MQTT, visualización en una interfaz Node-RED o transmisión a la nube (Pires & Gomes, 2024).

2.3.3.2 Infraestructura de Transmisión y Comunicaciones.

Conectividad en Sitio

- Redes inalámbricas de área extensa (LPWAN) para cobertura en terrenos amplios. Estas redes permiten la comunicación eficiente de dispositivos IoT en áreas extensas con bajo consumo energético.
- Redes mesh para zonas forestales o ecosistemas densos con conectividad limitada. Estas redes permiten la interconexión de múltiples nodos, asegurando una comunicación robusta y flexible en entornos difíciles.
- Radioenlaces y antenas direccionales para comunicación punto a punto. Proporcionan enlaces de alta capacidad entre estaciones base y puntos remotos, facilitando la transmisión de datos en áreas donde otras formas de conectividad son inviables.
- Estaciones repetidoras móviles para flexibilidad en campo. Estas estaciones amplían la cobertura de la red en operaciones temporales o móviles, facilitando la comunicación en proyectos de investigación que requieren movilidad.

El estudio de caso “Case study: LoRa/LoRaWAN as a suitable LPWAN choice for pressure and flow monitoring in Bulgarian water utility sector” realizado en 2024 en Bulgaria evaluó la aplicabilidad de LoRa/LoRaWAN como una opción adecuada de LPWAN para el monitoreo de presión y flujo en el sector de servicios de agua. La investigación concluyó que LoRaWAN es una solución viable para la transmisión de datos en tiempo real en sistemas de gestión del agua (Milovanov, 2024).

Comunicaciones Satelitales

- Terminales VSAT para conectividad de alta capacidad y transmisión continua de grandes volúmenes de datos. Estos terminales ofrecen acceso a internet en ubicaciones sin infraestructura terrestre, permitiendo la transmisión de datos en tiempo real desde áreas remotas.
- Equipos BGAN, Iridium o Globalstar para envío en tiempo real de paquetes de datos pequeños en zonas sin infraestructura terrestre. Proporcionan comunicación satelital portátil para voz y datos en cualquier lugar, siendo ideales para operaciones en áreas aisladas.

Caso de uso: Iridium Installation Case Study, En 2023, la empresa Adroit colaboró con Waka Kotahi NZ Transport Agency (NZTA) en Nueva Zelanda para monitorear un deslizamiento de tierra de movimiento lento que amenazaba la State Highway 8 en la Isla Sur. Se instalaron cinco inclinómetros equipados con conectividad satelital Iridium para transmitir datos precisos sobre la rotación del terreno, detectando movimientos o deslizamientos a medida que ocurrían o proporcionando alertas tempranas sobre posibles inestabilidades. Debido a la escasa cobertura de redes IoT en la ubicación remota, se utilizaron inclinómetros capaces de comunicarse vía satélite, con datos cargados a la plataforma Adroit a través de la red satelital Iridium (Adroit., 2023).

Redes Privadas Virtuales (VPN)

- Acceso seguro a plataformas remotas con segmentación de tráfico científico. Las VPNs garantizan la integridad y confidencialidad de los datos transmitidos entre sitios, permitiendo a los investigadores acceder de forma segura a recursos y datos desde ubicaciones remotas.

Caso de uso: En 2018, la empresa Eco-Vision, dedicada a servicios ambientales, enfrentaba dificultades operativas por utilizar más de 20 herramientas VPN distintas. Para resolverlo, adoptaron una solución VPN estandarizada y centralizada que permitió asegurar las comunicaciones remotas, mejorar la eficiencia operativa y reducir costos. Esta implementación fortaleció el acceso seguro a datos ambientales desde múltiples ubicaciones remotas (IXON, 2018).

2.3.3.3 Infraestructura de Almacenamiento y Procesamiento.

Almacenamiento de Datos

- Sistemas NAS y SAN para almacenamiento local de alta capacidad: Proporcionan soluciones eficientes para el almacenamiento y acceso rápido a grandes volúmenes de datos ambientales en instalaciones locales.
- Soluciones distribuidas como Ceph o GlusterFS para escalabilidad: Permiten expandir el almacenamiento de manera flexible y gestionar datos de investigación ambiental de forma eficiente.
- Servicios en la nube como Amazon S3, Azure Blob o Google Cloud Storage: Ofrecen almacenamiento remoto seguro y accesible, facilitando la colaboración y el acceso a datos desde diversas ubicaciones.
- Librerías de cintas para archivo de largo plazo: Brindan una solución económica y duradera para la conservación de datos históricos de investigaciones ambientales.

Caso de uso*:* Investigadores desarrollaron una estrategia de almacenamiento utilizando Ceph para manejar grandes volúmenes de datos de teledetección en malla. Esta solución mejoró la estabilidad y redujo el tiempo de consulta en un 38% en comparación con estrategias anteriores, optimizando el almacenamiento y la eficiencia en la consulta de imágenes en malla (Tang et al., 2022).

Plataformas de Procesamiento

- Clústeres de cómputo de alto rendimiento (HPC) para simulaciones complejas: Permiten realizar modelados detallados y precisos de fenómenos ambientales, facilitando la comprensión de sistemas complejos y la predicción de cambios en el ecosistema.
- Servidores con GPUs para procesamiento paralelo: Ideales para tareas que requieren alta capacidad de cálculo, como el análisis de imágenes satelitales y modelado climático, acelerando significativamente el procesamiento de datos voluminosos.

- Nodos de edge computing con equipos como Jetson o Raspberry industrial para preprocesamiento en sitio: Facilitan el procesamiento de datos directamente en el lugar de recolección, reduciendo la latencia y la necesidad de transmitir grandes volúmenes de datos a centros de datos centrales.
- Plataformas serverless (FaaS) como AWS Lambda o Google Cloud Functions para tareas específicas en la nube: Permiten ejecutar funciones específicas en respuesta a eventos, optimizando recursos y costos en tareas como el procesamiento de datos ambientales en tiempo real.

Caso de estudio: Implementación de un clúster HPC para modelado ambiental en la Universidad de Hong Kong. En 2019, el Dr. Jed O. Kaplan y su equipo en el Grupo de Investigación TERRACES del Departamento de Ciencias de la Tierra de la Universidad de Hong Kong, implementaron un clúster de cómputo de alto rendimiento (HPC) para realizar simulaciones complejas sobre el impacto del uso del suelo en el cambio climático. Este clúster permitió ejecutar modelos de simulación, análisis estadísticos y visualización de resultados, apoyando a un equipo de hasta 12 investigadores en sus estudios sobre interacciones entre el cambio climático y la cobertura terrestre (XENON Systems, 2019).

Sistemas de Bases de Datos

- Relacionales: PostgreSQL con PostGIS para datos geoespaciales, MySQL Permiten el almacenamiento estructurado y la ejecución de consultas complejas sobre datos ambientales, con soporte para análisis espacial en el caso de PostGIS, útil para mapas temáticos, modelos de ocupación del suelo y análisis de cobertura vegetal.
- NoSQL: MongoDB, Cassandra, InfluxDB para series temporales Ideales para almacenar y consultar grandes volúmenes de datos no estructurados o semiestructurados, como mediciones continuas de sensores climáticos o calidad del aire, permitiendo consultas rápidas y escalables sobre series temporales.
- Data lakes y data warehouses: Snowflake, BigQuery, Redshift para análisis masivo Permiten integrar, almacenar y procesar grandes volúmenes de datos ambientales

heterogéneos, incluyendo sensores remotos, datos meteorológicos, imágenes satelitales y registros históricos para su análisis conjunto.

Caso de estudio: Uso de PostgreSQL/PostGIS para análisis de deforestación en el bioma amazónico. En 2022, investigadores brasileños utilizaron software libre como PostgreSQL y PostGIS para construir una base de datos geoespacial destinada a analizar la relación entre la deforestación y el Registro Ambiental Rural (CAR) en el bioma amazónico. El sistema permitió la organización y análisis de información espacial y temporal, facilitando estudios sobre el impacto del uso del suelo, la expansión agrícola y las políticas de conservación en la región. Esta infraestructura fortaleció el manejo de grandes volúmenes de datos ambientales y mejoró la trazabilidad de los análisis geográficos realizados (Brasco, 2022).

2.3.3.4 Infraestructura de Análisis y Visualización.

Sistemas de Información Geográfica (GIS)

- Software como ArcGIS, QGIS, GRASS GIS para análisis espacial: Estas herramientas permiten realizar análisis espaciales detallados, facilitando la visualización y comprensión de datos geográficos en estudios ambientales.
- Servidores de mapas como GeoServer o MapServer: Proporcionan la capacidad de publicar y compartir datos geoespaciales en la web, permitiendo el acceso y la colaboración en proyectos de monitoreo ambiental.
- Infraestructura compatible con estándares OGC (WMS, WFS, WCS): Garantiza la interoperabilidad entre diferentes sistemas y aplicaciones GIS, facilitando el intercambio y uso eficiente de datos geoespaciales en estudios ambientales.

Caso de estudio: En 2024, investigadores italianos desarrollaron una plataforma Web-GIS en el Valle Cervo (noroeste de Italia) como parte de una estrategia de gestión de riesgos hidrogeológicos. El sistema se diseñó utilizando herramientas de software libre como QGIS para la preparación cartográfica, GRASS GIS para cálculos hidrológicos avanzados, e infraestructura basada en estándares OGC para garantizar interoperabilidad.

El equipo integró datos geoespaciales estáticos (como modelos digitales de terreno y mapas de uso del suelo) con datos dinámicos de sensores hidrometeorológicos, permitiendo identificar áreas vulnerables a inundaciones y flujos de detritos. El resultado fue una aplicación web interactiva que permite explorar escenarios de riesgo en tiempo real, facilitando la toma de decisiones en planes de mitigación y respuesta ante desastres (Graña et al., 2024).

Plataformas de Ciencia de Datos

- Entornos como JupyterHub, RStudio Server o Google Colab para análisis colaborativo: Estas plataformas permiten a equipos de investigadores trabajar de manera conjunta en proyectos de ciencia de datos, facilitando el acceso compartido a notebooks y recursos computacionales desde cualquier ubicación.
- Librerías científicas: NumPy, SciPy, GDAL, Pandas: Estas herramientas proporcionan funcionalidades esenciales para el análisis y manipulación de datos numéricos y geoespaciales, permitiendo realizar operaciones complejas de manera eficiente en estudios ambientales y científicos.

Caso de estudio: Implementación de JupyterHub y RStudio Server para la enseñanza de ciencia de datos en la Universidad de Washington. En 2020, la Universidad de Washington implementó JupyterHub y RStudio Server en un entorno de computación en la nube para facilitar la enseñanza de ciencia de datos. Esta infraestructura permitió a estudiantes y profesores acceder a entornos de programación consistentes y preconfigurados desde cualquier ubicación, mejorando la eficiencia en la enseñanza y el aprendizaje. El uso de estas plataformas también facilitó la colaboración en proyectos y la gestión centralizada de recursos computacionales (B. Kim & Henke, 2021).

Visualización 3D y SIG Web

- Herramientas como CesiumJS, Leaflet, OpenLayers para mapas interactivos con capas en tiempo real: Estas bibliotecas permiten la creación de mapas web interactivos en 2D y 3D, facilitando la visualización y análisis de datos geoespaciales en tiempo real.
- Dashboards: Grafana, Power BI, Tableau, Kibana para presentación de datos integrados con APIs dinámicas: Estas plataformas ofrecen interfaces dinámicas

para la visualización y monitoreo de datos, permitiendo la integración con diversas fuentes y la actualización en tiempo real de la información presentada.

Caso de estudio: Sistema Web-GIS para monitoreo de cultivos en la isla de Lemnos, Grecia. Se desarrolló un sistema interactivo Web-GIS para monitorear sistemas agrícolas en la isla de Lemnos, Grecia en 2023. Este sistema Multiescala integra datos de sensores, imágenes satelitales y modelos predictivos, permitiendo a los agricultores y responsables de políticas visualizar y analizar información en tiempo real sobre el estado de los cultivos. La implementación de este sistema ha mejorado la toma de decisiones en la gestión agrícola y ha optimizado el uso de recursos (Avanidou et al., 2023).

2.3.3.5 Infraestructura para Gestión de Proyectos y Datos.

La gestión efectiva de proyectos de investigación medioambiental y de los datos que estos producen requiere un marco estructurado que integre y coordine las actividades investigativas, asegurando su correcta ejecución y protección. Tras haber explorado las infraestructuras de captura, transmisión, almacenamiento, procesamiento, análisis y visualización de datos en las secciones previas, se hace necesario unificar estos elementos tecnológicos en un sistema que facilite la planificación, el seguimiento y la administración de los procesos. Esta infraestructura para la gestión de proyectos y datos busca consolidar los flujos de información generados durante el ciclo de vida del proyecto, alineándolos con principios de seguridad de la información como la confidencialidad, integridad y disponibilidad, además con normativas reconocidas, tales como ISO/IEC 27001:2022 y COBIT 2019.

Por lo tanto, este apartado abarca herramientas y sistemas diseñados para optimizar la organización y supervisión de los proyectos, al mismo tiempo que proporciona un entorno sólido para la gobernanza de los datos ambientales. Desde plataformas que permiten asignar recursos y monitorear avances hasta sistemas de metadatos y repositorios que aseguran la trazabilidad y el uso adecuado de la información, esta capa tecnológica conecta las capacidades operativas descritas en puntos anteriores con los objetivos estratégicos de la investigación. Además, la inclusión de controles de seguridad específicos protege los activos de información frente a riesgos derivados de la colaboración interdisciplinaria y del manejo de datos sensibles, como los vinculados a la

biodiversidad o al cambio climático. A continuación, se presentan los elementos principales de esta infraestructura, acompañados de ejemplos prácticos que ilustran su aplicación en proyectos medioambientales reales, ofreciendo así un enfoque integrado y profesional para la gestión segura y eficiente en este ámbito.

Sistemas de Gestión de Datos Científicos (SDMS)

- Plataformas como LabKey o OpenBIS para metadatos, flujos de trabajo y trazabilidad experimental. Estas herramientas permiten una gestión integral de datos científicos, facilitando la organización, análisis y compartición de información en entornos de investigación colaborativa.

Caso de estudio: Integración de openBIS, qPortal y OMERO para la gestión de datos multimodales en investigación en ciencias de la vida. Investigadores implementaron una infraestructura de gestión de datos que integra las plataformas openBIS, qPortal y OMERO para manejar datos multimodales en ciencias de la vida en 2022. Esta solución permitió la gestión y análisis conjunto de datos ómicos (como secuenciación genética y espectrometría de masas) junto con datos de microscopía e imágenes médicas. La integración de estas plataformas facilitó la armonización de metadatos y mejoró la eficiencia en la gestión de datos complejos, apoyando prácticas de ciencia abierta y cumpliendo con los principios FAIR (Findable, Accessible, Interoperable, Reusable). Este enfoque también permitió la generación de conjuntos de datos multidimensionales, facilitando análisis basados en datos y el entrenamiento de modelos de aprendizaje automático para aplicaciones predictivas futuras (Kuhn Cuellar et al., 2022).

Repositorios de Datos

- Infraestructura conforme a principios FAIR (Findable, Accessible, Interoperable, Reusable): Garantiza que los datos sean fácilmente localizables, accesibles, interoperables y reutilizables, facilitando su uso eficiente en la comunidad científica.
- Repositorios como DataVerse, CKAN o Zenodo: Plataformas diseñadas para almacenar, compartir y gestionar datos de investigación, promoviendo la colaboración y el acceso abierto a la información científica.

Caso de estudio: Implementación de un repositorio de datos de energía fotovoltaica en Malta utilizando CKAN. En 2025, investigadores en Malta desarrollaron el primer repositorio público de datos de energía fotovoltaica del país, empleando sensores de alta precisión conformes con la norma IEC y metodologías estandarizadas. Este repositorio, basado en la plataforma CKAN, permite la recopilación, almacenamiento y acceso abierto a datos de rendimiento de sistemas fotovoltaicos, facilitando la investigación y el desarrollo en el sector energético. La implementación de este sistema ha mejorado la transparencia y disponibilidad de datos energéticos en Malta, apoyando iniciativas de energía renovable y políticas basadas en evidencia (Bartolo et al., 2025).

Control de Versiones y Colaboración

- Git (GitHub, GitLab, Bitbucket) para código, datos y workflows reproducibles (ej. DVC): Estas plataformas permiten el control de versiones de código fuente y, mediante herramientas como DVC (Data Version Control), facilitan la gestión y reproducción de flujos de trabajo en proyectos de ciencia de datos y aprendizaje automático.
- Herramientas como Confluence, Redmine o JIRA para documentación y seguimiento técnico: Estas aplicaciones proporcionan espacios colaborativos para la documentación, gestión de proyectos y seguimiento de incidencias, mejorando la comunicación y organización dentro de los equipos de trabajo.

Caso de estudio: Gestión de la complejidad en proyectos de aprendizaje automático con DVC, MLflow y W&B. Para enfrentar los desafíos de manejar múltiples versiones de datos y modelos en un sistema de recomendación basado en aprendizaje automático, un equipo de desarrollo adoptó una integración de herramientas avanzadas de control de versiones y colaboración. Se utilizó DVC para gestionar de forma estructurada las versiones de datos y modelos, MLflow para el registro detallado de los experimentos y Weights & Biases (W&B) para la visualización de métricas y el trabajo colaborativo en tiempo real (Venkatesan, 2025).

2.3.3.6 Infraestructura de Seguridad y Cumplimiento.

Seguridad de Red y Datos

- Firewalls físicos/virtuales y sistemas de prevención de intrusos (IPS): Estos dispositivos controlan y monitorean el tráfico de red para prevenir accesos no autorizados y detectar actividades sospechosas, protegiendo la integridad de los sistemas.
- Cifrado en tránsito y reposo para datos sensibles: La encriptación asegura que los datos, tanto en movimiento como almacenados, sean inaccesibles para usuarios no autorizados, garantizando su confidencialidad y cumpliendo con normativas de protección de datos.

Caso de estudio: Implementación de medidas de ciberseguridad en sistemas de monitoreo ambiental. Un estudio reciente del 2024, destaca la importancia de implementar medidas de ciberseguridad, como firewalls, sistemas de detección y prevención de intrusos (IDPS) y cifrado de datos, en sistemas de monitoreo ambiental. Estas medidas son esenciales para proteger la integridad y confidencialidad de los datos ambientales recopilados, especialmente en infraestructuras críticas que dependen de tecnologías digitales para su funcionamiento (Scholar Chinenye Obasi et al., 2024).

Autenticación y Control de Accesos

- **LDAP, Active Directory, SSO, autenticación multifactor (MFA) y políticas RBAC***:* Estas tecnologías y políticas permiten gestionar de manera centralizada las identidades y accesos de usuarios en sistemas de monitoreo ambiental, garantizando que solo personal autorizado pueda interactuar con datos sensibles y dispositivos críticos.

Caso de estudio: Implementación de un sistema de autenticación y monitoreo en áreas críticas utilizando inteligencia artificial. Investigadores desarrollaron un sistema que integra autenticación basada en reconocimiento facial y control de accesos mediante políticas RBAC en un centro de datos dedicado al monitoreo ambiental. Utilizando técnicas de inteligencia artificial,

el sistema autentica a los usuarios y monitorea en tiempo real las áreas críticas, asegurando que solo el personal autorizado pueda acceder a zonas sensibles. Esta solución mejora la seguridad física y lógica del centro, protegiendo tanto la infraestructura como los datos ambientales recopilados (Villegas-Ch & García-Ortiz, 2023).

Cumplimiento Normativo

- Trazabilidad mediante logs, auditorías y herramientas como ELK Stack. El uso de herramientas como ELK Stack (Elasticsearch, Logstash y Kibana) facilita la recopilación, análisis y visualización de logs, permitiendo una trazabilidad efectiva y auditorías detalladas de las operaciones del sistema.
- Soporte para estándares como ISO 27001 o GDPR. Implementar prácticas y tecnologías que respalden el cumplimiento de normativas internacionales, como ISO 27001 para la gestión de seguridad de la información y GDPR para la protección de datos personales, es esencial para garantizar la conformidad legal y la confianza de los usuarios.

Caso de estudio: Implementación de ISO 27001 en EarthSoft para la gestión segura de datos ambientales. EarthSoft, una empresa especializada en software para la gestión de datos ambientales y geotécnicos, reconoció la necesidad de fortalecer la seguridad de su información para proteger datos sensibles y cumplir con regulaciones internacionales. Para ello, implementaron un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022, lo que les permitió identificar y mitigar riesgos, establecer controles adecuados y garantizar la confidencialidad, integridad y disponibilidad de los datos que manejan. Esta certificación no solo mejoró la postura de seguridad de EarthSoft, sino que también reforzó la confianza de sus clientes y socios en su capacidad para manejar información crítica de manera segura (EarthSoft, s. f.).

Este caso de estudio demuestra cómo la implementación de la norma ISO 27001 puede mejorar la seguridad y el cumplimiento normativo en organizaciones que gestionan datos ambientales, asegurando la protección de la información y el cumplimiento de estándares internacionales.

2.3.3.7 Infraestructura de Respaldo, Continuidad y Energía.

Sistemas de Respaldo y Recuperación

- Copias automatizadas locales y en la nube con versionado. Implementar soluciones de respaldo que realicen copias de seguridad automáticas tanto en infraestructuras locales como en la nube, incorporando control de versiones, garantiza la protección de datos críticos y facilita la recuperación ante desastres. Este enfoque híbrido asegura redundancia y disponibilidad, permitiendo restaurar información a estados específicos en caso de pérdida o corrupción de datos.

Caso de estudio: Implementación de estrategias de respaldo de datos en la recuperación ante desastres para minimizar el tiempo de inactividad. Un estudio publicado en 2023 exploró diversas estrategias de respaldo de datos empleadas en la recuperación ante desastres para minimizar el tiempo de inactividad y proteger información valiosa. Se analizó la importancia de la redundancia de datos, el papel de las soluciones de respaldo basadas en la nube y los beneficios de enfoques híbridos que combinan almacenamiento local y en la nube. El estudio destacó las mejores prácticas para determinar la frecuencia de los respaldos, seleccionar medios de almacenamiento apropiados e implementar procesos de respaldo automatizados para mejorar la confiabilidad y acelerar los esfuerzos de recuperación. Además, se abordaron los desafíos relacionados con la integridad, seguridad y cumplimiento de los datos, proporcionando información sobre cómo las organizaciones pueden enfrentar estas preocupaciones mientras optimizan sus estrategias de respaldo. Al comprender e implementar estrategias de respaldo de datos sólidas, las empresas pueden reducir significativamente el riesgo de pérdida de datos y asegurar una rápida restauración de las operaciones, salvaguardando en última instancia su éxito a largo plazo (Stephen, 2023) .

Continuidad Operativa

- Planes de contingencia y sistemas de alta disponibilidad (HA). La implementación de planes de contingencia y sistemas de alta disponibilidad es esencial para garantizar la continuidad operativa en organizaciones que manejan datos críticos. Estos planes permiten una respuesta eficaz ante interrupciones imprevistas,

minimizando el tiempo de inactividad y asegurando la disponibilidad continua de servicios esenciales.

Caso de estudio: Implementación de un sistema de monitoreo ambiental con alta disponibilidad en la Universidad de Aarhus. La Universidad de Aarhus, a través de su Departamento de Ciencias Ambientales, enfrentaba desafíos en la recopilación de datos precisos y continuos para el monitoreo de glaciares. Para abordar esta necesidad, colaboraron con Ignitec en el desarrollo de una solución tecnológica robusta y escalable. La implementación resultante permitió la recopilación de datos en tiempo real, mejorando la precisión y eficiencia en la investigación ambiental. Este sistema de monitoreo ambiental con alta disponibilidad aseguró la continuidad operativa y la integridad de los datos, incluso en condiciones extremas (Ignitec, 2025).

Energía Autónoma

- Sistemas UPS, generadores y paneles solares para estaciones remotas.
- Aislamiento eléctrico, tierra física y gabinetes resistentes ante condiciones climáticas extremas.

2.3.3.8 Infraestructura de Desarrollo y Automatización.

Entornos de Desarrollo y Pruebas

- Máquinas virtuales y contenedores (Docker). El uso de máquinas virtuales y contenedores permite crear entornos de desarrollo y pruebas consistentes y aislados. Docker facilita la creación de contenedores ligeros que incluyen aplicaciones y sus dependencias, asegurando uniformidad en diferentes etapas del ciclo de vida del desarrollo.
- Orquestadores como Kubernetes o OpenShift. Estas herramientas gestionan la implementación, escalado y operación de aplicaciones en contenedores. Kubernetes y OpenShift automatizan la orquestación de contenedores, mejorando la eficiencia y confiabilidad en entornos de desarrollo y producción.

Caso de estudio: Implementación de Kubernetes y Docker en la investigación medioambiental. Un estudio publicado en 2020 exploró la aplicación de Docker y Kubernetes en entornos de nube a gran escala, destacando su impacto en la gestión de aplicaciones en investigaciones científicas, incluyendo el ámbito medioambiental. La integración de estas tecnologías permitió a las organizaciones aprovechar sus fortalezas combinadas, creando un marco robusto para desplegar y gestionar aplicaciones en la nube. El estudio discutió modelos de implementación que utilizan ambas herramientas, enfatizando beneficios como mayor escalabilidad, flexibilidad y facilidad de gestión. Además, se identificaron desafíos comunes en la implementación de Docker y Kubernetes, como problemas de escalabilidad, complejidad en la gestión y preocupaciones de seguridad, y se exploraron estrategias para superarlos (Krishnamurthy, 2020).

Integración y Despliegue Continuo (CI/CD)

- Jenkins, GitLab CI o TravisCI para scripts y APIs científicas, incluyendo validación de modelos. Estas herramientas automatizan la integración y despliegue de código, facilitando la validación y pruebas continuas de modelos científicos y APIs, lo que mejora la eficiencia y confiabilidad en proyectos de investigación.

Caso de estudio: Implementación de CI/CD en la ingeniería de datos para optimizar pipelines de datos. Un estudio publicado en enero de 2025 exploró la aplicación de prácticas de Integración y Despliegue Continuo (CI/CD) en la ingeniería de datos, enfocándose en la automatización de pipelines de datos para mejorar su confiabilidad y escalabilidad. La investigación destacó cómo la automatización de procesos de construcción, prueba y despliegue contribuye a la consistencia y eficiencia en el desarrollo de pipelines de datos. Se abordaron metodologías, mejores prácticas y desafíos asociados con la implementación de CI/CD en este contexto, incluyendo el control de versiones, diseño modular de pipelines, pruebas automatizadas, gestión de artefactos, infraestructura como código y monitoreo efectivo. El estudio concluyó que la adopción de CI/CD en la ingeniería de datos es fundamental para construir soluciones confiables, escalables y eficientes, impulsando la innovación y productividad en prácticas modernas de ingeniería de datos (Parmar, 2025).

APIs y Servicios Web

- APIs REST/GraphQL y microservicios para procesamiento modular. Las APIs REST y GraphQL permiten la comunicación eficiente entre componentes de software, facilitando arquitecturas de microservicios que promueven el procesamiento modular y escalable.
- Gateways de API para control de acceso, escalabilidad y gestión centralizada de servicios. Los gateways de API actúan como puntos de entrada unificados para las solicitudes de los clientes, gestionando la autenticación, autorización, enrutamiento y limitación de tasas, lo que mejora la seguridad y el rendimiento del sistema.

Caso de estudio: Implementación de una arquitectura basada en microservicios para la simulación de procesos ambientales. En un estudio publicado en 2021, se propuso un enfoque basado en microservicios para organizar la modelización de simulaciones en entornos de computación distribuida heterogéneos. Este enfoque permitió la integración de datos meteorológicos en modelos de gemelos digitales de infraestructuras, facilitando la investigación de componentes críticos de dichos objetos. La arquitectura propuesta mejoró la flexibilidad y escalabilidad en la simulación de procesos ambientales, demostrando la eficacia de los microservicios en la gestión de tareas complejas en sistemas distribuidos (Kostromin et al., 2021).

La infraestructura tecnológica propuesta para proyectos de investigación medioambiental representa una aproximación estructurada que busca responder a las necesidades técnicas identificadas, aunque reconoce que su viabilidad efectiva dependerá de múltiples factores operativos y estratégicos que trascienden el diseño conceptual. La diversidad de tecnologías involucradas como sensores especializados, redes de comunicación híbridas, capacidades de procesamiento distribuido y soluciones de almacenamiento seguro, plantea desafíos concretos de integración, compatibilidad y mantenimiento que deberán gestionarse de forma rigurosa a lo largo del ciclo de vida del proyecto. Asimismo, la solidez del modelo estará condicionada por la evolución de los riesgos tecnológicos, la disponibilidad de recursos para garantizar actualizaciones permanentes, y la capacidad organizativa para sostener mecanismos de control y verificación que respalden la confiabilidad de los datos. En este contexto, la infraestructura no debe interpretarse como una solución concluyente, sino como una base inicial que exige validaciones técnicas

progresivas y un proceso continuo de revisión para asegurar que las expectativas del proyecto se correspondan con resultados verificables y ajustados a los estándares de cumplimiento aplicables.

2.4 Gobierno y Gestión Estratégica de la Información

La gestión estratégica de la información y su gobernanza son elementos para garantizar que las tecnologías de la información (TI) contribuyan de manera efectiva a los objetivos organizacionales. Para ello, ISO/IEC 38500:2024, COBIT 2019 y TOGAF 10 proporcionan principios y marcos metodológicos que permiten estructurar, supervisar y mejorar la gestión de TI, asegurando alineación con los objetivos estratégicos, mitigación de riesgos y optimización de recursos.

2.4.1 *Gobierno y Dirección Estratégica de TI*

La norma ISO/IEC 38500:2024 establece principios para la gobernanza de TI, asegurando que la toma de decisiones en tecnología se alinee con la estrategia de la organización. Define un modelo de gobernanza basado en los principios de evaluar, dirigir y monitorear el uso de TI, fomentando la creación de valor, el uso responsable de los recursos y la gestión efectiva de riesgos. Además, introduce la importancia de la participación de las partes interesadas, asegurando que los directivos y responsables de TI comprendan los impactos de la tecnología en el negocio.

2.4.2 *Gestión y Gobierno Integrado de TI*

COBIT 2019 complementa la gobernanza establecida en ISO/IEC 38500 al proporcionar un marco operativo para la gestión de TI en las organizaciones. Define un sistema de gobernanza y gestión que integra componentes clave, como estructuras organizacionales, procesos, políticas y principios, garantizando que las TI sea gestionada de manera efectiva. COBIT estructura su modelo en objetivos de gobierno y gestión, asegurando que las TI soporten las necesidades del negocio y generen valor de manera sostenible.

2.4.3 *Arquitectura Empresarial Aplicada a Proyectos Medioambientales*

El estándar TOGAF 10 establece un marco de arquitectura empresarial que permite diseñar y gestionar entornos tecnológicos alineados con los objetivos estratégicos de la organización. En el contexto de proyectos medioambientales, TOGAF facilita la integración de TI con la infraestructura organizacional, optimizando el uso de datos y asegurando la interoperabilidad entre sistemas. Mediante su método ADM (Architecture Development Method), proporciona una hoja de ruta estructurada para desarrollar arquitecturas tecnológicas sostenibles y escalables.

En conjunto, ISO/IEC 38500:2024, COBIT 2019 y TOGAF 10 proporcionan una base sólida para la gobernanza y gestión estratégica de la información, asegurando que la TI sea utilizada de manera efectiva, alineada con la estrategia del negocio y adaptada a los requerimientos del entorno operativo.

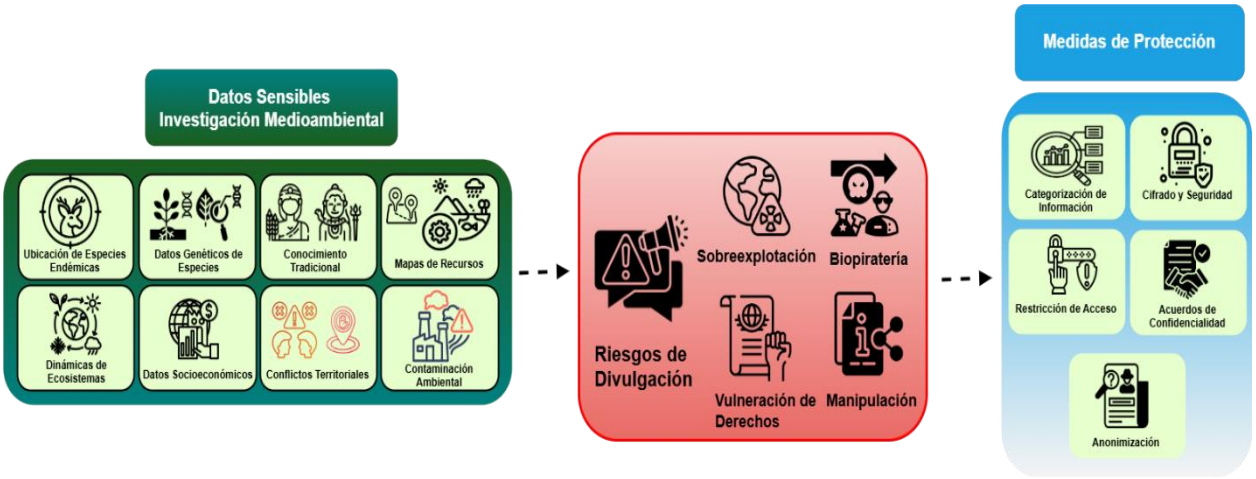
La investigación y el análisis detallado de los componentes tecnológicos, desde los dispositivos de captura en campo (Sección 2.3.3.1) hasta los sistemas de respaldo y automatización (Secciones 2.3.3.7 y 2.3.3.8), han permitido evidenciar el ecosistema de hardware y software que sustenta los proyectos de investigación medioambiental. Esta caracterización exhaustiva, que abarca desde el tipo de sensores y redes de comunicación hasta las plataformas de análisis y el software especializado, culmina en la consolidación de un modelo de infraestructura integral. Dicho modelo se representa visualmente en las Figuras 2 y 3, que no solo resumen los elementos descritos, sino que también concluyen la investigación sobre las tecnologías requeridas, presentando una arquitectura de referencia para este tipo de proyectos.

Capítulo 3: Análisis de la Sensibilidad de Datos en el Contexto Medioambiental

Los proyectos de investigación medioambiental manejan una gran variedad de registros que, por sus implicaciones ecológicas, sociales o culturales, deben considerarse sensibles. Abordar esta realidad es el primer paso para construir cualquier estrategia de seguridad que sea verdaderamente efectiva. Sin un entendimiento claro de qué información es valiosa o delicada, los controles aplicados serían genéricos y, muy probablemente, insuficientes. La Figura 4 resume visualmente este proceso de análisis: parte de la identificación de Datos Sensibles comunes en este campo, los conecta con los Riesgos de Divulgación que suponen, y finalmente, esboza las Medidas de Protección generales que se pueden aplicar. Este diagrama, en esencia, es una conclusión del análisis sobre los tipos de datos que se deben resguardar, los peligros que enfrentan y las estrategias para su protección.

Figura 4

Protección de Datos Ambientales



Fuente*: Elaboración Propia*

Un dato se considera sensible no necesariamente por ser secreto, sino por el potencial de daño que su divulgación o mal uso podría causar. En este contexto, un dato es sensible cuando, sin las debidas precauciones, su exposición puede tener consecuencias negativas para los ecosistemas, las comunidades locales o las instituciones involucradas. Este tipo de información suele detallar aspectos muy específicos del entorno natural, de la fauna y flora protegidas, o de la compleja relación de las personas con su medio. Su carácter reservado se justifica, por tanto, en la

prevención: si se expone sin control, existe un riesgo claro y tangible de causar daños ecológicos, económicos o de vulnerar derechos fundamentales.

A continuación, se presentan algunos ejemplos que ilustran por qué estos datos requieren un alto nivel de cuidado:

- **Posibilidad de sobreexplotación de recursos naturales:** La información sobre la ubicación exacta de especies en peligro, si cae en las manos equivocadas, podría disparar la caza o la extracción ilegal, amenazando su supervivencia.
- **Protección de la privacidad y los derechos de las comunidades:** Los datos sobre usos tradicionales de recursos, prácticas agrícolas o condiciones socioeconómicas pueden vulnerar la privacidad de las poblaciones locales o facilitar el aprovechamiento indebido de sus conocimientos ancestrales.
- **Riesgos de encubrimiento o manipulación:** Los informes sobre contaminación o degradación de hábitats podrían ser silenciados o alterados por actores con intereses económicos, evitando que se tomen medidas de protección a tiempo.
- **Componentes genéticos y patentes (Biopiratería):** La investigación sobre el ADN de especies puede llevar a la explotación comercial no autorizada si los resultados se publican sin supervisión, perjudicando a las comunidades que han conservado ese patrimonio genético.
- **Compromiso ético y responsabilidades institucionales:** Los equipos de investigación tienen la responsabilidad de proteger la integridad del entorno y el bienestar de las personas que dependen de él.

Definir un conjunto de datos como “sensibles” implica reconocer que su manejo inadecuado puede causar daños ambientales, sociales y económicos. Por ello, la implementación de medidas de protección es una consecuencia directa de este análisis. La categorización de la información permite aplicar recursos de seguridad de manera eficiente, enfocándolos donde más se necesitan. El cifrado de registros críticos asegura que, incluso si los dispositivos son vulnerados, la información permanezca inaccesible. La restricción de accesos garantiza que solo el personal autorizado pueda consultar o modificar los datos. Finalmente, los acuerdos de confidencialidad establecen un marco legal y ético que obliga a todas las partes a un manejo responsable. Estas

acciones no solo protegen a los ecosistemas y a las comunidades, sino que también refuerzan la validez y la credibilidad de los resultados científicos.

3.1 Clasificación y Protección de Datos Medioambientales Sensibles

Una vez determinada la sensibilidad de la información, su clasificación se convierte en un mecanismo para la aplicación de medidas de protección diferenciadas. ISO/IEC 27001:2022 en su Anexo A – Control 5.12 Clasificación de la Información, establece que las organizaciones deben definir un esquema formal de categorización, alineado con sus requisitos operacionales y regulatorios, garantizando la correcta gestión del acceso, almacenamiento y transmisión de datos.

Desde un enfoque práctico, CIS Controls v8 – Control 3 Protección de los Datos, enfatiza la necesidad de documentar y etiquetar la información conforme a su clasificación, asegurando una gestión eficiente a lo largo de su ciclo de vida. Para ello, recomienda la implementación de herramientas de Data Loss Prevention (DLP) y el monitoreo activo de datos en reposo y en tránsito, evitando accesos indebidos y filtraciones no autorizadas.

Para garantizar la seguridad de los datos clasificados, ISO/IEC 27002:2022 establece controles específicos que refuerzan la protección de la información como 8.2 Gestión de Privilegios de Acceso, define la asignación de privilegios mínimos (principio de menor privilegio) para limitar el acceso a datos críticos, Control 8.3 Restricción del Acceso a la Información, establece políticas que restringen el acceso a la información según su nivel de confidencialidad, evitando accesos indebidos y Control 8.10 Eliminación de la Información, regula la eliminación segura de datos clasificados, asegurando que no puedan ser recuperados sin autorización.

Complementando este marco, CIS Controls v8 introduce medidas adicionales de seguridad que refuerzan la protección de la información, Control 3.12 Segmentar el procesamiento y almacenamiento de datos en función de la sensibilidad, asegura que los datos con distintos niveles de sensibilidad no sean almacenados ni procesados en los mismos sistemas, reduciendo el riesgo de exposición y Control 3.7 Establecer y mantener un esquema de clasificación de datos, exige la revisión periódica del esquema de clasificación, asegurando que se mantenga actualizado ante cambios organizacionales o regulatorios.

La clasificación y protección de los datos no debe considerarse un proceso estático. ISO/IEC 27001 establece la necesidad de una revisión regular de los controles aplicados, permitiendo su ajuste conforme evolucionen los riesgos, la infraestructura tecnológica y los requerimientos regulatorios.

3.2 Licenciamiento para el Acceso y Uso de Datos Sensibles

La gestión de activos sensibles requiere un esquema de licenciamiento que regule su acceso y uso, protegiendo los datos frente a riesgos identificados (Tabla 8 "Análisis de Riesgos y Amenazas"). Este esquema define condiciones, responsabilidades y niveles de restricción, alineándose con la Cláusula 5.3 "Funciones, responsabilidades y autoridades de la organización" de ISO/IEC 27001:2022. Organizado de mayor a menor restricción según la sensibilidad y criticidad operativa (Tabla 6 "Identificación y Clasificación de Activos"), el esquema incluye categorías de licencias que abarcan desde accesos altamente controlados hasta licencias abiertas, adaptándose a las necesidades de los proyectos medioambientales, como la protección de datos en entornos distribuidos (Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación), la colaboración Multi-Actor (Sección 10 "Análisis de las Partes Interesadas y Estrategia de Participación"), y la promoción de la transparencia científica (Sección 2.3.2 "Datos Medioambientales"). La elección de la licencia adecuada depende de factores como el uso comercial, la posibilidad de crear obras derivadas, la necesidad de atribución, la reutilización en otros proyectos, y las restricciones específicas (por ejemplo, no modificación)(CEPAL, s. f.) , asegurando un equilibrio entre accesibilidad y seguridad.

3.2.1 *Licencia de Acceso Confidencial o Clasificado*

La Licencia de Acceso Confidencial o Clasificado restringe el acceso a entidades autorizadas, asegurando trazabilidad completa, cifrado obligatorio mediante AES-256 (Sección 6.2.2 "Diseño de Controles Técnicos Aplicables"), monitoreo continuo con SIEM (Sección 6.2.2 "Diseño de Controles Técnicos Aplicables"), y control de copias, conforme a la Sección 8.24 "Uso de la criptografía" de ISO/IEC 27002:2022. Esta licencia protege datos altamente sensibles, como las ubicaciones exactas de especies protegidas (Sección 2.3.2 "Datos Medioambientales"), evitando su uso en actividades ilegales, como la caza furtiva (Tabla 8 "Análisis de Riesgos y

Amenazas"). Se aplica mediante autenticación multifactor (Sección 6.2.5 "Incorporación de Controles de Defensa en Profundidad") y auditorías periódicas (Sección 8.6.3 "Mecanismos de Retroalimentación para la Mejora"), garantizando que solo usuarios autorizados puedan utilizar la información, con registros de auditoría para asegurar su trazabilidad. En este nivel de máxima restricción, las licencias propietarias de software, como Microsoft Volume Licensing que regula el uso comercial y la distribución del software y sus datos pueden aplicarse a herramientas utilizadas para procesar esta información, limitando su uso a configuraciones aprobadas.

3.2.2 *Licencia de Acceso Restringido Interno*

La Licencia de Acceso Restringido Interno limita el acceso exclusivamente al personal autorizado dentro del proyecto, implementando controles basados en roles (RBAC), en conformidad con la Sección 5.15 "Control de Acceso" de ISO/IEC 27002:2022. En el contexto de investigaciones, esta licencia protege datos como resultados preliminares, información de identificación personal (Sección 11.2 "Implicaciones Éticas del Modelo de Seguridad") y localizaciones de sensores (Sección 2.3.3.1 "Infraestructura de Captura y Adquisición de Datos"), garantizando que permanezcan bajo control exclusivo del equipo técnico, especialmente en entornos distribuidos (Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación").

Su aplicación exige autenticación multifactor (Sección 6.2.5 "Incorporación de Controles de Defensa en Profundidad"), monitoreo mediante registros de uso (Sección 6.5 "Mecanismos de Respuesta a Incidentes de Seguridad") y segmentación de permisos según funciones asignadas (Sección 6.2.3 "Diseño de Controles Organizacionales y Administrativos"). De este modo, se reducen significativamente los riesgos de accesos no autorizados internos (Tabla 8 "Análisis de Riesgos y Amenazas").

Asimismo, esta licencia puede extenderse al uso de software restringido, aplicando condiciones específicas para herramientas internas bajo licenciamiento propietario, cuyo uso queda reservado a miembros previamente habilitados del proyecto.

3.2.3 *Licencia de Acceso Controlado Externo*

La Licencia de Acceso Controlado Externo permite extender el acceso a terceros mediante acuerdos formales como memorandos de entendimiento (MOUs) o contratos específicos bajo condiciones de uso claramente definidas, trazabilidad operativa y límites de redistribución. Este tipo de acceso controlado se fundamenta en el control AC-2 “Gestión de Cuentas” de NIST SP 800-53 Rev. 5, y es particularmente relevante en proyectos medioambientales que requieren colaboración con entidades externas, como ministerios, universidades o ONGs (Sección 10 "Análisis de las Partes Interesadas y Estrategia de Participación").

El objetivo es garantizar que la información compartida sea utilizada de forma controlada y verificable, reduciendo el riesgo de filtraciones o usos no autorizados por parte de actores externos (Tabla 8 "Análisis de Riesgos y Amenazas"). La validez y cumplimiento de esta licencia se sustentan mediante la firma de acuerdos contractuales y la ejecución de auditorías periódicas.

En proyectos que operan sobre entornos distribuidos (Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación"), esta licencia puede complementarse con esquemas técnicos como licencias de acceso de cliente (CAL) y licencias de administración (ML) de Microsoft, que permiten la gestión segura y segmentada de dispositivos y usuarios dentro de redes colaborativas interinstitucionales.

3.2.4 *Licencia Temporal o Contextual*

La Licencia Temporal o Contextual habilita el acceso a datos por un periodo limitado o en función de una actividad específica, estableciendo su revocación automática una vez alcanzado el objetivo previsto. Se fundamenta en el proceso DSS05 “Gestionar los Servicios de Seguridad” de COBIT 2019, y resulta especialmente adecuada para proyectos piloto, actividades de prueba o ejercicios de interoperabilidad en entornos de investigación (Sección 9.3 "Plan Detallado de Implementación Conceptual").

Esta modalidad de acceso se caracteriza por definir un intervalo de vigencia (por ejemplo, seis meses), establecer condiciones explícitas de caducidad, y exigir auditorías de cierre para verificar la finalización segura del acceso (Sección 9.4 "Plan Detallado de Validación Empírica"). De esta manera, se previene la permanencia indebida de privilegios o credenciales una vez

concluido el uso legítimo, mitigando así riesgos relacionados con accesos residuales o reutilización no autorizada (Tabla 8 "Análisis de Riesgos y Amenazas").

Este tipo de licencia resulta especialmente útil en escenarios donde los datos no requieren ser reutilizados en fases posteriores, pero donde su protección durante el periodo activo es crítica para garantizar la seguridad operativa del proyecto.

3.2.5 *Licencia de Uso Académico o de Investigación*

La Licencia de Uso Académico o de Investigación restringe el acceso exclusivamente a fines científicos no comerciales, bajo condiciones de atribución obligatoria. Su fundamento se encuentra en el Apartado 5.6 “Responsabilidad” de la norma ISO/IEC 38500:2024, que promueve el uso ético y transparente de la información en contextos de gobernanza digital.

En el marco de proyectos medioambientales, esta licencia facilita la colaboración con investigadores externos al autorizar el acceso a bases de datos especializadas, como registros de biodiversidad o mediciones de cambio climático (Sección 2.3.2 "Datos Medioambientales"). Su aplicación refuerza la replicabilidad científica y la transparencia del conocimiento generado, siempre que se garantice la citación formal al proyecto fuente (Sección 11.4 "Impacto Social y Consideraciones Comunitarias").

Además, esta licencia contribuye a mitigar el riesgo de uso indebido de los datos con fines comerciales no autorizados, alineándose con los mecanismos de protección definidos en la Tabla 8 "Análisis de Riesgos y Amenazas".

3.2.6 *Licencia de Uso Comercial o con Fines Económicos*

La Licencia de Uso Comercial o con Fines Económicos permite el aprovechamiento de datos sensibles en desarrollos tecnológicos o servicios de carácter lucrativo, bajo condiciones contractuales específicas. Esta modalidad se basa en el Proceso DSS05 "Gestionar los Servicios de Seguridad" de COBIT 2019, que establece lineamientos para controlar el acceso externo a servicios y recursos gestionados.

En proyectos de investigación, esta licencia habilita la integración de conjuntos de datos, por ejemplo, geoespaciales, meteorológicos o de calidad ambiental en aplicaciones, plataformas o herramientas comerciales (Sección 2.3.2 "Datos Medioambientales"). De este modo, se posibilita la generación de valor económico sin comprometer la protección y trazabilidad de los datos compartidos.

Su implementación requiere la formalización de contratos específicos, el establecimiento de restricciones claras de uso, y la ejecución de auditorías financieras periódicas que garanticen la conformidad con las condiciones acordadas (Sección 6.2.3 "Diseño de Controles Organizacionales y Administrativos"). Esta estructura contractual contribuye a prevenir el uso no autorizado con fines lucrativos, mitigando riesgos de explotación económica indebida (Tabla 8 "Análisis de Riesgos y Amenazas").

3.2.7 *Licencia de Acceso Abierto con Condiciones*

La Licencia de Acceso Abierto con Condiciones permite el acceso público a conjuntos de datos medioambientales bajo términos específicos que exigen atribución obligatoria y, en algunos casos, la prohibición de modificaciones. Esta categoría se fundamenta en la Sección 5.10 "Uso aceptable de la información y otros activos asociados" de ISO/IEC 27002:2022, la cual establece directrices para garantizar que el uso abierto de activos de información no comprometa su integridad, confidencialidad ni trazabilidad.

En investigaciones medioambientales, esta licencia resulta especialmente útil para fomentar la transparencia científica y promover la replicación de resultados, al facilitar el acceso a datos anonimizados, como mediciones de calidad del aire o registros de sensores distribuidos (Sección 2.3.2 "Datos Medioambientales"). Estos datos se publican en repositorios abiertos, donde pueden ser utilizados con fines científicos o educativos sin restricciones comerciales, mitigando riesgos de tergiversación, modificación no autorizada o mal uso (Tabla 8 "Análisis de Riesgos y Amenazas").

Complementariamente, esta modalidad puede aplicarse a datos generados por software libre o sistemas de captura en campo (Sección 2.3.3.1 "Infraestructura de Captura y Adquisición de Datos"), integrando condiciones específicas mediante licencias de contenido abierto.

Entre las licencias aplicables se encuentran:

Creative Commons (CC), según lo documentado por la CEPAL:

- CC BY (Reconocimiento): Permite uso, modificación y distribución con atribución al autor original. Adecuada para datos que buscan máxima difusión y visibilidad.
- CC BY-SA (Reconocimiento-CompartirIgual): Requiere mantener la misma licencia en obras derivadas, útil para preservar condiciones de apertura.
- CC BY-ND (Reconocimiento-SinObraDerivada): Permite redistribución, pero no permite modificaciones, asegurando la integridad del contenido.
- CC BY-NC (Reconocimiento-NoComercial): Restringe el uso a fines no comerciales, aunque permite adaptación del contenido con atribución.

Open Data Commons (ODC):

- ODC-By (Open Data Commons Attribution License): Requiere atribución, permitiendo copiar, modificar y distribuir bases de datos.
- ODbL (Open Database License): Exige atribución, mantiene la licencia en derivados y prohíbe el uso de DRM, asegurando la apertura continua.
  (CEPAL, s. f.)

Estas licencias son aplicables, por ejemplo, a bases de datos geoespaciales anonimizadas, cuando el objetivo es permitir su libre reutilización sin comprometer su autenticidad ni la autoría original (Sección 6.2.2 "Diseño de Controles Técnicos Aplicables").

La aplicación de esta licencia se alinea con los controles definidos en: Cláusula 8.2 " Evaluación de riesgos de seguridad de la información " de ISO/IEC 27001:2022, Sección 5.15 "Control de acceso" de ISO/IEC 27002:2022, Control AC-2 " Gestión de cuentas" de NIST SP 800-53 Rev. 5. Y se complementa con: Políticas de acceso adaptativo (Sección 6.2.3 "Diseño de Controles Organizacionales y Administrativos"), Mecanismos de defensa en profundidad (Sección 5.2.5 "Defensa en Profundidad"), Controles técnicos especializados (Sección 6.2.2 "Diseño de Controles Técnicos Aplicables").

Esta integración permite regular cada flujo de datos abiertos conforme a su sensibilidad, el uso autorizado y los riesgos asociados, fortaleciendo la protección de los activos de información clasificados (Tabla 6 "Identificación y Clasificación de Activos") frente a las amenazas identificadas (Tabla 8 "Análisis de Riesgos y Amenazas").

3.3 Características Particulares de los Proyectos Medioambientales

Los proyectos medioambientales presentan particularidades que condicionan de manera primordial la forma en que deben gestionarse los riesgos asociados a la seguridad de la información. A diferencia de los proyectos corporativos convencionales, donde la información suele estar delimitada a entornos organizacionales con canales controlados, en los proyectos de investigación intervienen múltiples factores externos que desdibujan los perímetros de seguridad tradicionales. Actores tan diversos como comunidades locales, entidades gubernamentales, organizaciones no gubernamentales y centros de investigación internacionales colaboran en un ecosistema donde la información fluye constantemente. Esta dinámica, sumada a la naturaleza misma de los datos tratados, introduce una complejidad que exige un enfoque de seguridad adaptado, flexible y sumamente específico.

Uno de los aspectos más relevantes es precisamente, la naturaleza de los datos. En un entorno empresarial, la pérdida de datos suele tener consecuencias financieras o reputacionales. En la investigación medioambiental, las consecuencias trascienden. Los datos geoespaciales sobre el uso del suelo, los registros meteorológicos para modelos climáticos, los inventarios de biodiversidad o las series de monitoreo de la calidad del agua en tiempo real son, en muchos casos, irremplazables. Su valor no es solo científico, son la base para la toma de decisiones críticas en política pública, ordenamiento territorial y gestión de recursos estratégicos. Por ello, se requiere un manejo mucho más riguroso en términos de confidencialidad, integridad y disponibilidad, que debe atender no solo a la normativa legal, sino también a los marcos de ética científica y a los principios de ciencia abierta que rigen la colaboración en este campo (Parra, 2023).

En primer lugar, la información recolectada en estos estudios es decisiva para la formulación de políticas y estrategias de conservación efectivas. Por ejemplo, los datos sobre especies en peligro son indispensables para desarrollar planes de protección específicos, mientras que la información climática permite modelar y predecir cambios ambientales, facilitando la

creación de políticas de mitigación y adaptación al cambio climático. Asimismo, el monitoreo de la contaminación proporciona datos para identificar fuentes de polución y evaluar sus efectos en la salud de los ecosistemas y las comunidades humanas. Además, la investigación sobre recursos naturales asegura que su uso sea sostenible, evitando la sobreexplotación que podría comprometer la capacidad de las futuras generaciones para satisfacer sus necesidades (Tapi, 2023).

En relación con lo anterior, el artículo "Environmental Sustainability in the Age of Big Data: Opportunities and Challenges for Business and Industry", escrito por Z. Li, X. Zhou, y S. Huang, examina cómo la revolución del big data está redefiniendo la investigación ambiental y su impacto en la industria y los negocios. Con el auge del Big Data, las organizaciones tienen acceso a volúmenes masivos de información ambiental que pueden utilizar para tomar decisiones más informadas y sostenibles. Sin embargo, este acceso también conlleva una serie de desafíos, como la necesidad de gestionar adecuadamente la privacidad y la sensibilidad de los datos recopilados. El artículo destaca cómo la correcta implementación de estrategias de Big Data puede mejorar significativamente la eficiencia en la gestión de recursos naturales, optimizar el uso de energía y reducir el impacto ambiental de las actividades industriales. No obstante, los autores también advierten sobre los riesgos asociados, como la sobrecarga de información y la posibilidad de malinterpretaciones de los datos que pueden conducir a decisiones erróneas. Además, se enfatiza la importancia de desarrollar métodos innovadores para proteger la privacidad de los datos y garantizar que la información se utilice de manera ética y responsable. Por lo tanto, la capacidad de integrar Big Data en las prácticas empresariales y de investigación ofrece un enorme potencial para promover la sostenibilidad ambiental, pero requiere un enfoque equilibrado que aborde tanto las oportunidades como los desafíos inherentes a este campo en evolución (Li & Huang, 2023).

Adicionalmente, existe una creciente presión por la transparencia y el acceso abierto, lo que implica un equilibrio complejo entre asegurar la protección de la información crítica y permitir su difusión en formatos reutilizables y bajo licencias abiertas.

3.4 Contraste con Modelos Genéricos de Gestión de Proyectos

Modelos ampliamente utilizados como PMBOK (Fundamentos para la Dirección de Proyectos) o ISO 21500 (Guía para la gestión de proyectos), abordan la gestión de riesgos desde una perspectiva transversal, pero no desarrollan de forma específica los elementos propios de la

seguridad de la información en contextos abiertos, colaborativos o con alta exposición pública. En estos modelos, la seguridad suele considerarse como un subconjunto del área de gestión de riesgos o calidad, y se focaliza en asegurar la continuidad operativa del proyecto o la protección de activos organizacionales internos.

Por el contrario, en proyectos medioambientales, los riesgos de seguridad no se limitan a interrupciones operativas, sino que abarcan escenarios como:

- Filtración anticipada de resultados preliminares, con implicaciones políticas o sociales.
- Manipulación intencionada de sensores o fuentes de recolección de datos en campo.
- Acceso indebido a datos por actores con intereses particulares o conflictos de interés.

Estas situaciones rara vez están contempladas de forma explícita en modelos genéricos, lo cual demanda una adaptación metodológica y técnica más fina.

3.4.1 *Enfoque Normativo y Consideraciones Sectoriales*

La necesidad de adecuar los marcos de análisis de riesgos al sector medioambiental encuentra sustento normativo en marcos especializados como ISO/IEC 27005:2022 y MAGERIT.

- En ISO/IEC 27005:2022, particularmente en su sección 6. Establecimiento del contexto, se plantea que la gestión de riesgos debe partir de una comprensión clara del entorno organizacional y de los interesados involucrados. Esta orientación es útil para integrar factores como la exposición pública del proyecto, la interoperabilidad de plataformas abiertas y las exigencias legales del sector ambiental.
- Por su parte, MAGERIT versión 3.0, Libro I, sección 1.6 (El análisis y el tratamiento de los riesgos en su contexto), destaca que el tratamiento de los riesgos debe contextualizarse sectorialmente, identificando actores, entornos y tipologías de amenazas específicas. Este enfoque permite ajustar los análisis y las salvaguardas a situaciones particulares como las que se presentan en proyectos de

campo, investigación participativa o vinculación con entidades regulatorias ambientales.

3.4.2 *Amenazas y Riesgos Diferenciales*

La gestión de la seguridad de la información en proyectos de investigación medioambiental requiere un enfoque adaptativo que supere las premisas tradicionales de los modelos genéricos. En estos proyectos, los riesgos no sólo afectan activos tecnológicos o financieros, sino que pueden comprometer directamente la conservación de ecosistemas, la integridad de procesos científicos y los derechos de comunidades que interactúan con el entorno natural.

Entre las amenazas más relevantes se identifican la divulgación anticipada o no autorizada de resultados, que puede alterar procesos de licenciamiento ambiental, decisiones jurisdiccionales o consultas previas. Asimismo, el activismo digital representa un riesgo creciente, la manipulación de plataformas de recolección o visualización de datos por parte de grupos con intereses ideológicos o políticos puede distorsionar la evidencia científica o erosionar la confianza pública. A esto se suma la dependencia frecuente de sistemas abiertos o de bajo costo, sin controles adecuados de autenticación, auditoría o cifrado, especialmente en proyectos ejecutados con presupuestos limitados o en regiones con infraestructura restringida.

Estas condiciones, ausentes o marginalmente abordadas en modelos como PMBOK, PRINCE2 o ISO 21500, hacen necesaria la adopción de marcos normativos que permitan una gestión de riesgos basada en el contexto. En este sentido, la norma ISO/IEC 27005:2022, en su sección 6 (Establecimiento del Contexto), establece la importancia de considerar el entorno específico, las partes interesadas y los requisitos regulatorios para una evaluación precisa del riesgo. Este principio es reforzado por ISO 31000:2018, que subraya en su cláusula 5.4.1 (Comprensión de las organizaciones y su contexto), la necesidad de comprender el entorno organizacional y externo como paso inicial para diseñar un sistema de gestión eficaz del riesgo.

Desde una perspectiva más sectorial, MAGERIT v3, particularmente en el Libro I, sección 1.6 (Análisis y tratamiento de riesgos en su contexto), propone una caracterización detallada de amenazas, activos y escenarios aplicables a sistemas de información públicos, muchos de los

cuales se alinean con los esquemas de proyectos ambientales en territorios abiertos, descentralizados o interinstitucionales.

A diferencia de sectores donde los datos son considerados activos estratégicos organizacionales, en el campo medioambiental la información tiene un carácter público, dinámico y muchas veces sujeto a requerimientos de interoperabilidad y acceso abierto. Este escenario demanda medidas que armonicen los principios de transparencia científica con la protección frente a amenazas internas o externas. ISO/IEC 27001:2022, en su anexo A, promueve la implementación de controles de seguridad de la información ajustados al nivel de riesgo y a la sensibilidad del activo, lo cual se operacionaliza mediante las directrices técnicas descritas en ISO/IEC 27002:2022.

La fragmentación de actores, desde investigadores hasta agencias reguladoras y comunidades locales, eleva la necesidad de establecer políticas claras de clasificación, almacenamiento, transmisión y destrucción de información. El control de accesos, la trazabilidad documental y el cifrado de datos, recomendados tanto en los Controles CIS v8 (Control 3: Protección de los Datos, Control 6: Gestión de Control de Accesos), como en el catálogo de controles de NIST SP 800-53 Rev. 5. AC – Access Control: Esta familia proporciona directrices específicas para limitar y monitorear el acceso a sistemas de información. Controles como AC-2 (Gestión de Cuentas) y AC-6 (Privilegio Mínimo) son aplicables en entornos donde múltiples actores (investigadores, colaboradores externos, organismos estatales) requieren niveles diferenciados de acceso a los datos. Implementar políticas de acceso mínimamente necesario es esencial para proteger información sensible, especialmente cuando los resultados tienen implicaciones regulatorias o territoriales.

AU – Auditoría y Rendición de Cuentas: Establece los mecanismos para registrar y revisar eventos de seguridad relevantes. Controles como AU-2 (Registro de Eventos) y AU-6 (Revisión, Análisis y Elaboración de Informes de Auditoría) permiten generar evidencias sobre el uso de los sistemas, facilitando la detección de accesos indebidos o manipulaciones no autorizadas de la información. Esto es particularmente relevante cuando los datos sustentan decisiones de política pública o de conservación ambiental, donde la trazabilidad es un factor crítico de legitimidad y confianza.

SC – Protección de sistemas y comunicaciones: Esta familia abarca controles relacionados con la protección de la información en tránsito y en reposo. Por ejemplo, SC-12 (Establecimiento y Gestión de Claves Criptográficas) y SC-28 (Protección de la información en reposo) resultan fundamentales cuando se manejan bases de datos con información de ecosistemas, registros comunitarios o coordenadas sensibles de biodiversidad, que podrían ser objeto de explotación, sabotaje o mal uso si no se resguardan adecuadamente.

A nivel de gobierno de TI, COBIT 2019 y ISO/IEC 38500:2024 ofrecen marcos orientados a la toma de decisiones responsable, que permiten alinear la gestión de la seguridad con los objetivos institucionales del proyecto, garantizando el cumplimiento normativo y la rendición de cuentas. Por su parte, ISO 55002:2018, aunque centrada en la gestión de activos, enfatiza en su sección 6.1 (Acciones para abordar los riesgos y oportunidades para el sistema de gestión de activos) la importancia de identificar riesgos y oportunidades que puedan afectar el logro de los objetivos del sistema de gestión, lo cual aplica directamente a los datos considerados activos estratégicos en investigaciones medioambientales.

Desde el punto de vista operativo, marcos como ITIL 4 y TOGAF 10 pueden aportar valor en la estructuración de procesos de soporte, arquitectura de sistemas y diseño de capacidades organizacionales asociadas a la seguridad, integrando dimensiones como continuidad, respuesta a incidentes y mejora continua.

En conjunto, el panorama de amenazas en proyectos de investigación medioambiental exige modelos de protección que combinen controles técnicos con principios éticos y consideraciones legales. La construcción de un esquema de seguridad robusto en este contexto no sólo protege la información, sino que garantiza la legitimidad del conocimiento generado y su utilidad para la toma de decisiones en escenarios de alta sensibilidad ambiental y social.

3.4.3 *Ejemplos y Estudios de Caso*

La investigación ambiental moderna se basa cada vez más en grandes volúmenes de datos, desde mediciones de sensores hasta información proporcionada por comunidades locales. Esta abundancia de datos impulsa descubrimientos científicos, pero también conlleva la gestión de información sensible que puede incluir detalles personales o confidenciales. Estudios en el campo

del *big data* destacan que al manejar conjuntos masivos de información surgen desafíos de complejidad técnica, escalabilidad, posibles filtraciones de privacidad y problemas de confianza en el proceso analítico (Nmesoma Okorie et al., 2024). En el ámbito ambiental esto significa que la protección de datos se ha convertido en un elemento central para salvaguardar la privacidad de individuos y comunidades sin frenar el avance del conocimiento (Layode et al., 2024).

Frente a esta realidad, se han fortalecido marcos legales que regulan el uso de datos en la investigación. En Europa, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) establece pautas estrictas para el tratamiento de información personal, afectando también a proyectos ambientales que manejan datos de individuos. Recientemente, han surgido iniciativas legales específicas orientadas a facilitar la reutilización de datos con fines científicos y de sostenibilidad manteniendo la privacidad: la Ley de Gobernanza de Datos de la Unión Europea es un ejemplo de ello, aunque su implementación plantea interrogantes sobre la compatibilidad con las normas de protección de datos vigentes (Finck & Mueller, 2023). En consecuencia, los investigadores ambientales deben navegar un entorno normativo cada vez más complejo, equilibrando el cumplimiento legal con la necesidad de compartir información para el bien público.

Para cumplir con estas exigencias sin comprometer la utilidad de los datos, la comunidad científica recurre a soluciones técnicas innovadoras que protegen la información desde su origen. Técnicas de encriptación avanzadas y procedimientos de anonimización permiten que los datos ambientales se compartan y analicen minimizando el riesgo de reidentificar a las personas detrás de ellos (Layode et al., 2024). Por ejemplo, un estudio de caso en el ámbito sanitario demostró que es factible divulgar datos sensibles de manera segura, (Antunes et al., 2021) emplearon métodos avanzados de preservación de privacidad al publicar información sobre pacientes de COVID-19 de un hospital en Portugal, logrando que esos datos fueran útiles para la investigación epidemiológica sin exponer la identidad de los individuos. Este enfoque evidencia que la apertura de datos y la protección de la privacidad pueden coexistir cuando se aplican las herramientas adecuadas.

Además de estas medidas tradicionales, están emergiendo enfoques novedosos para el intercambio seguro de información ambiental. (Yang et al., 2021) describen un esquema de compartición de datos basado en tecnología blockchain que garantiza la trazabilidad y seguridad en redes de sensores, ilustrando una vía práctica para compartir datos de monitoreo sin

comprometer la confidencialidad de las fuentes. Soluciones de este tipo, junto con la adopción de métodos como el aprendizaje federado en el cual los modelos se entrenan de forma colaborativa sin centralizar los datos crudos, reflejan cómo la comunidad científica busca conciliar la colaboración abierta con el resguardo de la privacidad. Estas innovaciones amplían las posibilidades para realizar análisis integrados de información ambiental proveniente de múltiples fuentes, a la vez que mantienen el control sobre los datos sensibles.

No obstante, la tecnología por sí sola no basta, proteger la privacidad en la investigación ambiental exige también una gobernanza de datos sólida y cooperación multidisciplinaria. Los proyectos más avanzados integran consideraciones éticas y legales desde el diseño mismo del estudio, involucrando a expertos en protección de datos, juristas, científicos ambientales y representantes de las comunidades afectadas. Este enfoque colaborativo ayuda a anticipar riesgos y a establecer salvaguardas conforme a las expectativas sociales y las normativas vigentes, fomentando una cultura de manejo responsable de la información (Layode et al., 2024). Por ejemplo, en iniciativas de ciencia ciudadana sobre calidad del aire o del agua, definir desde el inicio protocolos claros de consentimiento informado, anonimización y acceso a la información fortalece la confianza de los participantes y legitima el uso de sus datos en beneficio del conocimiento colectivo.

En conjunto, la convergencia de medidas técnicas, legales y organizativas indica que la protección de datos es ya parte inherente del quehacer científico ambiental. Diversos autores coinciden en que el futuro de la investigación en este campo dependerá de integrar estratégicamente salvaguardas de privacidad sin frenar la innovación ni la apertura de información (Layode et al., 2024b; Finck & Mueller, 2023). De este modo, el aprovechamiento de los datos para comprender y resolver problemas ambientales podrá realizarse con rigor ético y respeto a los derechos de las personas, manteniendo la confianza del público en la ciencia.

3.4.4 *Protocolos Específicos*

El manejo riguroso de la información en proyectos de investigación ambiental requiere establecer protocolos bien definidos que aseguren tanto la calidad de los datos como su protección. En esta línea, los lineamientos de la Agencia de Protección Ambiental de los Estados Unidos (EPA)

han sido clave para establecer prácticas que garanticen la fiabilidad de los datos utilizados en decisiones regulatorias y científicas.

El documento “Guidance on Environmental Data Verification and Data Validation”, plantea una estructura clara para revisar y validar la información antes de su uso. La verificación se centra en identificar errores e inconsistencias, mientras que la validación busca confirmar que los datos se ajustan a los requisitos definidos para su uso específico. Este enfoque metódico incorpora planes de gestión de calidad que permiten asegurar que la información empleada en análisis ambientales, evaluaciones de impacto o políticas públicas, sea consistente, trazable y confiable (Epa & Quality Management Division, 2002).

De forma complementaria, la publicación “Environmental Information Policy, Procedures and Standards” refuerza este esquema al establecer políticas y procedimientos para la gestión integral del dato ambiental. Se abarcan aspectos que van desde la recolección hasta el análisis y uso final, todo bajo un mismo marco de control. Esta estandarización permite mantener la integridad de los datos a lo largo de su ciclo de vida, promoviendo una gestión más transparente y fortaleciendo la rendición de cuentas de las organizaciones responsables (U.S. Environmental Protection Agency, 2024).

Más allá del aseguramiento de la calidad, el tratamiento eficaz de datos se traduce también en una ventaja estratégica para la conservación ambiental. El estudio “Enhancing Biodiversity Conservation and Monitoring in Protected Areas through Efficient Data Management” destaca cómo la implementación de protocolos estandarizados y el uso de bases de datos espaciales permiten mejorar significativamente la toma de decisiones. Gracias a herramientas como los sistemas de información geográfica (GIS), es posible monitorear cambios en los ecosistemas con precisión, anticipar amenazas como la pérdida de hábitat o especies invasoras, y generar respuestas coordinadas. Además, se subraya el valor de la colaboración interinstitucional como medio para consolidar un enfoque más amplio y sostenible de gestión de la biodiversidad (Urbano et al., 2024).

El avance tecnológico ha traído consigo nuevos mecanismos de recolección y procesamiento de información. Los sistemas aéreos no tripulados (UAS), comúnmente conocidos como drones, han adquirido un papel cada vez más relevante en el monitoreo ambiental. En “Current Practices in UAS-based Environmental Monitoring”, se analizan tanto las ventajas operativas de estas tecnologías como los desafíos que conllevan. Si bien los UAS permiten capturar

información detallada incluso en zonas remotas o de difícil acceso, su implementación exige protocolos que regulen aspectos como la calibración de sensores, la frecuencia de captura, la resolución de los datos y la protección de la privacidad. Una correcta estandarización en su uso, junto con la capacitación de los operadores, resulta clave para asegurar la calidad de la información recolectada (Tmuši et al., 2020).

Sin embargo, asegurar la calidad técnica no es suficiente si no se protege adecuadamente la información. El estudio "The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth", introduce un modelo de evaluación orientado a identificar y mitigar riesgos asociados a la fuga de información en proyectos ambientales. El modelo contempla amenazas tanto internas como externas, e incorpora 26 controles validados por especialistas en seguridad. Estos controles cubren desde aspectos organizacionales y tecnológicos, hasta factores humanos, permitiendo a las organizaciones evaluar su nivel de exposición y definir medidas preventivas. Así, se fortalece no solo la protección del dato, sino también la continuidad y sostenibilidad de los proyectos ambientales (J. Kim et al., 2020).

En conjunto, estos enfoques ofrecen una visión integrada sobre la necesidad de establecer protocolos específicos que combinen calidad, trazabilidad, eficiencia operativa y seguridad de la información. La articulación entre prácticas de gestión de datos, tecnologías emergentes y modelos de protección permite a las organizaciones enfrentar los desafíos actuales con mayor solidez y confianza, reforzando la base sobre la cual se sustentan las decisiones en materia ambiental.

3.4.5 *Análisis Interpretativo de la Comparación*

La comparación estructurada entre los proyectos de investigación medioambientales y los modelos genéricos de gestión de proyectos evidencia con claridad que la seguridad de la información en el ámbito ambiental presenta un conjunto de características particulares que exigen una atención diferenciada, tanto en el diseño de controles como en la formulación de políticas y estrategias.

Uno de los elementos más relevantes identificados en la matriz es la singularidad de los datos medioambientales. A diferencia de los datos operacionales típicos en entornos corporativos,

los registros generados en contextos ecológicos suelen ser no replicables, de alta sensibilidad, y vinculados directamente a fenómenos físicos y biológicos. Esta condición impone un estándar superior de integridad, exactitud y protección, pues cualquier alteración o pérdida no solo compromete la calidad científica, sino que puede incidir negativamente sobre decisiones de impacto social, legal o ecológico.

Asimismo, las condiciones en las que se producen, transmiten y almacenan la información ambiental introducen un conjunto de vulnerabilidades que no son comunes en modelos genéricos. La necesidad de operar en terrenos remotos, con conectividad limitada y equipos expuestos a condiciones climáticas adversas, hace que la seguridad no pueda depender exclusivamente de herramientas digitales convencionales. La combinación de riesgos físicos, ambientales y tecnológicos demanda una aproximación híbrida y contextualizada, en la que converjan mecanismos de ciberseguridad con prácticas logísticas y operativas adaptadas al terreno.

Otro aspecto diferenciador es el marco regulatorio que regula estos proyectos. Mientras que los modelos genéricos suelen guiarse por normativas amplias como el RGPD o estándares ISO aplicables a datos personales o corporativos, los proyectos ambientales están sujetos a un entramado regulatorio internacional altamente especializado, que abarca desde convenios de biodiversidad hasta tratados sobre acceso a recursos genéticos. Esto obliga a una formulación precisa de protocolos de manejo de datos, que no solo garanticen la confidencialidad y disponibilidad, sino también el cumplimiento ético, ecológico y legal del tratamiento de la información.

El impacto potencial ante fallas en la seguridad también difiere notablemente. En el ámbito medioambiental, las consecuencias pueden extenderse más allá de sanciones económicas o daños reputacionales, afectando ecosistemas enteros, poblaciones vulnerables o políticas públicas. Esto resalta la necesidad de adoptar enfoques de gestión del riesgo más rigurosos y multidimensionales, como los propuestos en marcos como MAGERIT v3 o ISO/IEC 27005:2022, que permiten mapear amenazas no convencionales y establecer controles dinámicos y adaptables.

La comparación también pone de relieve la importancia de la interoperabilidad y la gobernanza colaborativa. Los proyectos medioambientales, por su naturaleza transnacional y multidisciplinaria, requieren compartir datos sensibles entre múltiples actores bajo diferentes

marcos legales y culturales. Este contexto demanda protocolos que aseguren trazabilidad, integridad y control de acceso granular sin obstaculizar la circulación legítima del conocimiento.

Por último, la sostenibilidad y adaptabilidad de las políticas de seguridad emergen como un punto crítico. Dada la duración prolongada de muchos proyectos ecológicos y la constante evolución de amenazas tecnológicas, las políticas no pueden ser estáticas. Se requiere una estructura de gobernanza capaz de revisar, ajustar y escalar los controles según la evolución del entorno, tanto natural como digital.

Este análisis establece que los proyectos de investigación medioambiental no solo se enfrentan a riesgos diferentes, sino que operan bajo una lógica de valor, exposición y consecuencia que trasciende las capacidades de los modelos genéricos de seguridad de la información. Por tanto, se hace imprescindible una arquitectura de seguridad diseñada a medida, con una integración profunda entre los objetivos científicos, la regulación ambiental y la tecnología utilizada.

3.4.6 *Comparativa Proyectos Medioambientales vs. Modelos Genéricos*

Tabla 1

Comparativa Proyectos Medioambientales vs. Modelos Genéricos

ASPECTOS EVALUADOS	PROYECTOS DE INVESTIGACIÓN MEDIOAMBIENTAL	MODELOS DE GESTIÓN DE PROYECTOS EN GENERAL	ANÁLISIS Y JUSTIFICACIÓN PROFESIONAL
NATURALEZA Y SENSIBILIDAD DE LOS DATOS	Manejo de datos altamente especializados, sensibles e irrepetibles: biodiversidad, variables climáticas, calidad de agua/suelo, entre otros. Su alteración afecta decisiones científicas, normativas y de conservación a escala local y global.	Información predominantemente administrativa, financiera u operativa, con alcance y consecuencias principalmente internas.	Los datos medioambientales poseen un valor científico y estratégico irremplazable. Un error, pérdida o filtración puede desencadenar consecuencias irreversibles sobre ecosistemas, poblaciones vulnerables y políticas públicas. Requieren un enfoque de seguridad más estricto, que va más allá de los criterios convencionales de confidencialidad.
VULNERABILIDADES Y AMENAZAS	Riesgos extendidos a condiciones de campo: pérdida por condiciones climáticas, errores en la recolección, interceptación de datos en zonas remotas sin cifrado. Riesgos físicos y cibernéticos combinados.	Riesgos predominantemente cibernéticos (phishing, malware, intrusión lógica), con bajo nivel de exposición física o ambiental.	La combinación de recolección en entornos no controlados y transmisión desde ubicaciones remotas expone los proyectos a vectores de ataque poco comunes en ambientes corporativos. Esto exige una gestión híbrida de seguridad, que contemple amenazas físicas, lógicas y de infraestructura.
REGULACIONES Y CUMPLIMIENTO	Sujetos a marcos regulatorios nacionales e internacionales complejos y específicos: CITES, convenios de biodiversidad, normas de ética ambiental, propiedad genética, etc.	Cumplimiento mayormente centrado en marcos generales de protección de datos (ej. GDPR, LGPD) sin especificidad sectorial.	Las regulaciones aplicables a investigaciones ambientales incluyen no solo aspectos de privacidad, sino también restricciones éticas, ecológicas y de uso de datos geoespaciales o genéticos. La seguridad debe articularse para garantizar cumplimiento legal, científico y operativo.
IMPLICACIONES DEL INCUMPLIMIENTO	Consecuencias multidimensionales: sanciones legales, destrucción de hábitats, pérdida de biodiversidad, afectación a comunidades, debilitamiento de políticas públicas.	Repercusiones centradas en pérdidas económicas, sanciones administrativas y deterioro reputacional.	La seguridad de los datos medioambientales está directamente vinculada a la protección del entorno y a la gobernanza ambiental. El incumplimiento compromete no solo los resultados científicos, sino también procesos políticos, sociales y ecológicos, lo que eleva su criticidad.

ASPECTOS EVALUADOS	PROYECTOS DE INVESTIGACIÓN MEDIOAMBIENTAL	MODELOS DE GESTIÓN DE PROYECTOS EN GENERAL	ANÁLISIS Y JUSTIFICACIÓN PROFESIONAL
COLABORACIÓN Y COMPARTICIÓN DE DATOS	Alta colaboración multilateral (académica, institucional, comunitaria, internacional). Exige interoperabilidad, trazabilidad y seguridad transfronteriza de datos.	Compartición generalmente limitada al entorno organizacional, con mecanismos más simples de control de acceso.	Los proyectos ambientales requieren estándares robustos de intercambio seguro de datos, capaces de adaptarse a marcos legales disímiles, a la vez que aseguran la integridad y autenticidad de la información compartida.
GESTIÓN DE RIESGOS	Riesgos asociados a la pérdida de datos clave para decisiones territoriales, conservación o salud pública. Abarca factores ambientales, tecnológicos, humanos y regulatorios.	Foco en continuidad operativa, eficiencia, y protección financiera. Menor impacto social o ambiental.	La gestión de riesgos en entornos ambientales requiere una aproximación contextualizada y multidisciplinaria. MAGERIT v3 e ISO/IEC 27005:2022 ofrecen enfoques más adecuados para mapear amenazas no convencionales presentes en este tipo de proyectos.
SOSTENIBILIDAD Y ADAPTABILIDAD DE POLÍTICAS	Políticas diseñadas para mantenerse vigentes en ciclos largos de investigación. Deben evolucionar frente a cambios regulatorios, tecnológicos y científicos.	Políticas de seguridad con ciclos más cortos, orientadas a proyectos de duración limitada y cambios menos disruptivos.	Las investigaciones medioambientales suelen extenderse por años, incluso décadas. Las políticas deben ser adaptables, resilientes y revisables para responder a amenazas emergentes, sin comprometer la trazabilidad y validez de los datos históricos.
ESTRATEGIAS DE SEGURIDAD	Uso de cifrado avanzado, autenticación fuerte, almacenamiento redundante, medidas anti-interferencia en campo. Integración de políticas físicas, lógicas y operativas.	Seguridad basada en medidas estándar: firewalls, antivirus, controles de acceso básicos. Foco en infraestructura corporativa.	El contexto de recolección en campo, conectividad limitada y datos sensibles requiere estrategias sofisticadas. El uso de UAS, sensores IoT y transmisión satelital introduce riesgos adicionales que deben ser abordados desde el diseño de las estrategias de seguridad.

Fuente*: Elaboración Propia*

Los modelos de gestión de proyectos tradicionales presentan enfoques estructurados y eficientes para contextos empresariales o industriales, pero resultan limitados al abordar entornos con altas exigencias éticas, colaborativas y científicas como los proyectos medioambientales. Esta diferencia estructural genera la necesidad de explorar, en mayor profundidad, los elementos críticos de seguridad de la información que deben ser considerados al diseñar un modelo adaptado a este tipo de iniciativas.

La Tabla 1 presenta una comparación entre proyectos de investigación medioambientales y modelos de gestión genéricos, destacando diferencias sustanciales en cuanto a naturaleza de los datos, perfil de riesgos, exigencias normativas, consecuencias del incumplimiento y complejidad operativa.

Mientras que los modelos genéricos se orientan a estructuras administrativas o financieras con un riesgo predominantemente lógico, los proyectos ambientales operan con datos altamente sensibles, frecuentemente irrepetibles, y sujetos a regulaciones más diversas. Además, enfrentan amenazas combinadas, tanto físicas como digitales, derivadas de su funcionamiento en entornos distribuidos y expuestos.

Esta diferencia justifica la necesidad de un modelo de seguridad adaptado, que responda al valor estratégico y al riesgo inherente de los activos involucrados, y que pueda integrar medidas normativas, técnicas y operativas de forma coordinada.

3.4.7 *Contraste Proyectos Medioambientales vs. Modelos Tradicionales de Gestión*

A partir del análisis anterior, resulta pertinente profundizar en aquellas dimensiones específicas que definen la seguridad de la información en proyectos de investigación medioambiental. Este enfoque no solo permite comprender las particularidades de su tratamiento, sino también contrasta sus requerimientos con los marcos más habituales de gestión de proyectos. A continuación, se presentan comparaciones estructuradas que permiten visualizar los elementos diferenciadores desde una perspectiva técnica de seguridad, alineada con marcos internacionales y buenas prácticas.

La gestión de la seguridad de la información en proyectos de investigación medioambiental presenta exigencias diferenciadas frente a los enfoques tradicionales de gestión de proyectos

utilizados en sectores industriales, financieros o tecnológicos. Este contraste se hace evidente cuando se analizan marcos generalistas como PMBOK, PRINCE2 o las directrices de ISO 21500, en comparación con los requisitos propios del ámbito científico-ambiental, donde confluyen datos altamente sensibles, cooperación internacional, exigencias éticas y sostenibilidad.

Las siguientes tablas presentan una comparación estructurada en dimensiones clave de la seguridad de la información, con un enfoque en aspectos críticos como la integridad, confidencialidad, disponibilidad, trazabilidad, interoperabilidad y gobernanza de los datos.

Tabla 2

Comparativa integral de seguridad de la información

Dimensión / Aspecto comparado	Proyectos de Investigación Medioambiental	Modelos Tradicionales de Gestión
Tipo de información tratada	Datos científicos, ambientales, climáticos, geo-espaciales, de biodiversidad; generados por sensores, satélites, campo o laboratorios.	Información técnico-financiera, contractual, operativa o comercial, centrada en cumplimiento y resultados de negocio.
Sensibilidad	Muy alta. Posibles implicaciones sobre biodiversidad, poblaciones locales, geopolítica y políticas públicas.	Variable. Generalmente vinculada a confidencialidad empresarial o cumplimiento normativo.
Normativas aplicables	Protocolos FAIR, principios CARE, licencias abiertas (Creative Commons), acuerdos multilaterales y políticas de ciencia abierta.	Marcos regulatorios internos o sectoriales como ISO 27001, GDPR, PCI-DSS, entre otros.
Requisitos de trazabilidad	Exigencia elevada de trazabilidad técnica, científica y ética. Registros detallados del ciclo de vida de los datos, desde captura hasta publicación.	Trazabilidad orientada a control de versiones de entregables, hitos y seguimiento presupuestario.
Aproximación al riesgo	Visión holística y multidimensional: considera riesgos éticos, reputacionales, ambientales, sociales y científicos.	Visión centrada en riesgos técnicos, financieros y de cumplimiento de objetivos operativos.
Gestión de amenazas	Involucra múltiples actores (comunidades, ONGs, gobiernos, entes internacionales). Se requieren mecanismos participativos y sensibles al contexto.	Gestión enfocada en proveedores, socios comerciales, equipos internos y actores contratuales.
Amenazas emergentes	Exposición a manipulación de datos, accesos no autorizados, interferencia	Riesgos comunes: malware, errores de configuración, fallas

Dimensión / Aspecto comparado	Proyectos de Investigación Medioambiental	Modelos Tradicionales de Gestión
	política, vigilancia geoespacial y divulgación indebida.	de infraestructura, ataques dirigidos.
Ecosistema de colaboración	Redes abiertas entre universidades, centros de investigación, gobiernos, ONGs y organismos multilaterales.	Estructuras cerradas de colaboración interna, proveedores y socios bajo contrato.
Modelo de gobernanza de la información	Enfoque distribuido, ético y abierto. Gobernanza compartida entre actores con reglas consensuadas y adaptativas.	Modelo jerárquico y corporativo. Reglas impuestas por la organización que lidera el proyecto.
Requisitos de interoperabilidad	Alto nivel de interoperabilidad semántica, sintáctica y técnica. Uso de estándares abiertos, ontologías, metadatos estructurados y APIs.	Requisitos limitados a herramientas internas y formatos propietarios. Poca integración externa.
Enfoque temporal	Largo plazo. Los datos deben conservarse, mantenerse accesibles y actualizados durante décadas, según su relevancia ecológica o científica.	Enfocado en los plazos del proyecto. Interés en conservación puntual hasta la entrega de resultados.
Persistencia de la información	Se requieren mecanismos de preservación digital, respaldo redundante, formatos sostenibles y repositorios institucionales.	Archivo documental convencional, sin garantía de mantenimiento ni acceso a largo plazo.
Gestión del conocimiento	Clave para la innovación, políticas públicas, educación científica y análisis longitudinal. Implica curaduría activa y actualización continua.	Centrada en la documentación de lecciones aprendidas para mejora operativa o administrativa futura.

Fuente*: Elaboración Propia*

La Tabla 2 establece una clasificación de la información utilizada en proyectos de investigación ambiental, basada en dos dimensiones complementarias: el impacto ambiental potencial y el nivel de confidencialidad requerido. Esta combinación permite establecer prioridades de protección en función del valor estratégico y la sensibilidad operativa de los activos de información, facilitando la aplicación de controles proporcionales al riesgo asociado.

El criterio de impacto ambiental contempla un rango que va desde datos de libre acceso hasta información crítica, como registros sobre zonas protegidas o especies en riesgo. En paralelo, el eje de confidencialidad clasifica los datos según el daño potencial derivado de una divulgación no autorizada, con niveles que oscilan entre nulo, moderado y grave. Esta estructura permite

segmentar los activos de manera más precisa y aplicar mecanismos de protección diferenciados según su función y contexto.

La clasificación propuesta sirve como base técnica para definir controles específicos, organizar capas de seguridad y priorizar recursos, en línea con los principios de normas como ISO/IEC 27002:2022 y metodologías de análisis de riesgos como MAGERIT v3. Al integrarse en el diseño del modelo, facilita una gestión más efectiva de la información en entornos con alta exposición y responsabilidad operativa.

Esta necesidad de segmentación y priorización confirma que los proyectos medioambientales requieren un enfoque de seguridad diferenciado, capaz de responder a exigencias éticas, técnicas y colaborativas propias de contextos científicos complejos. La adopción de marcos especializados como ISO/IEC 27005:2022, MAGERIT v3 y controles seleccionados del NIST SP 800-53 Rev. 5 resulta clave para desarrollar modelos de protección sólidos, adaptables y alineados con principios de ciencia abierta y conservación del entorno.

A diferencia de los modelos tradicionales de gestión de proyectos, diseñados para contextos empresariales o industriales, los proyectos ambientales operan bajo condiciones normativas y operativas más exigentes. Esta diferencia estructural obliga a revisar y adaptar los criterios de seguridad de la información, incorporando elementos críticos que garanticen la protección de datos con valor científico, ecológico y social.

Capítulo 4: Estructura Metodológica del Diseño

La metodología propuesta para el diseño del modelo de seguridad de la información se estructura a partir del ciclo PHVA (Planificar, Hacer, Verificar, Actuar). Es importante precisar que, si bien la norma ISO/IEC 27001:2022 aplica este ciclo a la gestión de un SGSI (Sistema de Gestión de Seguridad de la Información), en este trabajo se realiza una adaptación conceptual para utilizarlo como un marco lógico que organiza el proceso de diseño. Este enfoque permite construir una estructura coherente, adaptable y alineada con estándares reconocidos, abordando las particularidades de los proyectos de investigación medioambiental.

Resulta pertinente señalar que esta metodología no solo orienta la construcción del modelo, sino que, además, proporciona el marco para la medición y verificación del cumplimiento de cada uno de los objetivos específicos del proyecto. Si bien los objetivos están formulados para describir las fases de un proceso de diseño (analizar, identificar, definir), su consecución se materializa en entregables concretos y verificables, los cuales son el resultado directo de la aplicación de este ciclo

En este contexto adaptado:

La fase Planificar (Plan) (Sección 5) responde a los objetivos de análisis, identificación y clasificación. El resultado medible de esta etapa es el conjunto de diagnósticos, inventarios de activos (Tabla 6), matrices de riesgo (Tabla 8) y la clasificación de requisitos que conforman la base estratégica del modelo.

La fase Hacer (Do) (Sección 6) materializa los objetivos de definición y segmentación. Su cumplimiento se constata a través del diseño del catálogo de controles (Tabla 11), la arquitectura lógica del modelo (Anexo E) y la formalización de las políticas y procedimientos correspondientes.

La fase Verificar (Check) (Sección 7) se aborda de manera conceptual en este diseño, establece el marco para la validación y la evaluación de la eficacia del modelo.

La fase Actuar (Act) (Sección 8) define los mecanismos para la mejora continua, garantizando así que el modelo no sea una estructura estática.

Esta estructura metodológica responde a la necesidad de construir una estructura adaptable, técnicamente fundamentada y alineada con estándares reconocidos, considerando las

particularidades operativas y normativas de los proyectos de investigación en el ámbito medioambiental.

En este tipo de entornos, la información suele generarse a partir de tecnologías desplegadas en campo, operadas por distintos actores, bajo condiciones de conectividad variable y con diferentes niveles de madurez técnica. Además, se gestionan datos con implicaciones científicas, regulatorias y éticas, que exigen criterios diferenciados de protección. Por estas razones, el modelo se define desde su origen como una propuesta orientada a responder a estos desafíos, sin asumir una implementación operativa, pero anticipando su viabilidad y capacidad de integración futura.

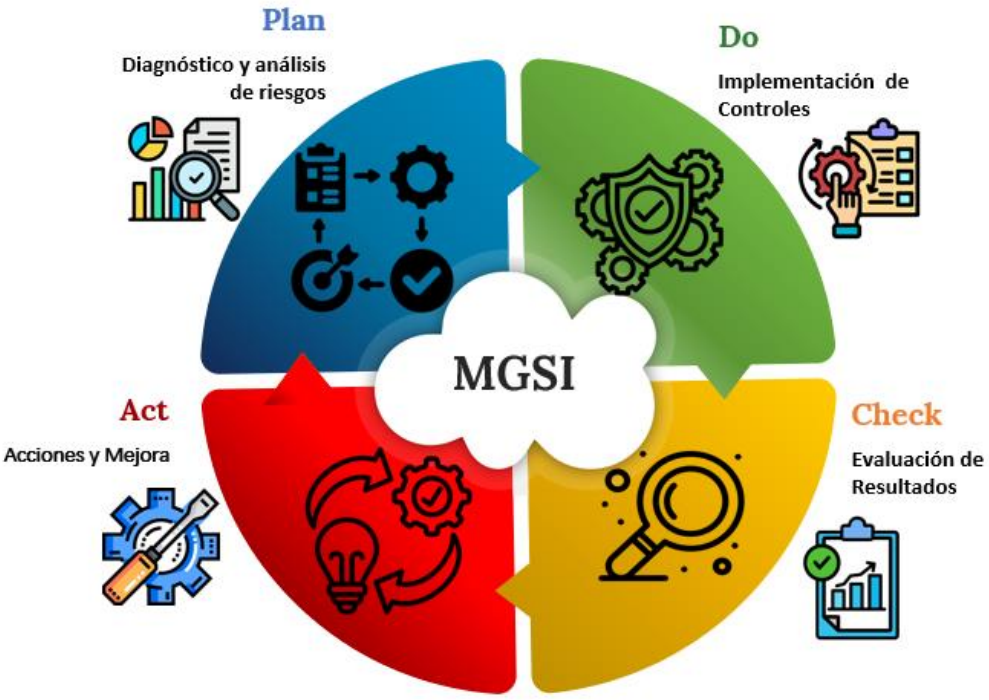
Cada fase del ciclo PHVA aporta una función específica en la construcción del modelo. Planificar permite identificar los activos informacionales, analizar los riesgos asociados y establecer prioridades de protección en función del contexto. En Hacer, se definen los controles conceptuales, se organiza la segmentación de activos y se establece la lógica funcional del sistema. Verificar introduce mecanismos de revisión interna, orientados a validar la consistencia del diseño frente a sus propios objetivos. Actuar contempla los ajustes necesarios para adaptar el modelo a cambios normativos, tecnológicos o institucionales, integrando un enfoque de mejora continua.

La estructura resultante se apoya en marcos como ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO 31000:2018, MAGERIT v3 y NIST SP 800-53 Rev. 5, sin reproducirlos de forma literal, sino adaptándolos a un entorno específico que combina exigencias de seguridad con responsabilidades de investigación y sostenibilidad.

En última instancia, el objetivo de documentar el modelo de seguridad se ve cumplido a través de la presente monografía. Este trabajo constituye la evidencia formal que integra y sistematiza los resultados obtenidos en cada una de las fases del ciclo PHVA. Queda demostrado, por tanto, que la aplicación de la metodología descrita es el instrumento que permite convertir los objetivos de proceso en resultados concretos, verificables y auditables.

Figura 5

Diagrama de Ciclo del Proceso PDCA en la Metodología de Seguridad



Fuente: Elaboración propia

El diagrama representa la aplicación del ciclo PHVA como marco metodológico para el diseño del modelo de seguridad de la información. Cada fase integra componentes específicos adaptados a entornos de investigación medioambiental, incluyendo acciones de diagnóstico, estructuración, validación y mejora. La propuesta articula principios establecidos en marcos internacionales como ISO/IEC 27001:2022, ISO/IEC 27005:2022, ISO 31000:2018, MAGERIT v3 y NIST SP 800-53 Rev. 5.

4.1.1 *Fase Planear (Plan)*

La fase de planificación establece la base estratégica del modelo, estructurando la identificación de activos de información, la evaluación de riesgos y la definición de prioridades de protección. En proyectos de investigación medioambientales, este proceso considera la sensibilidad, volumen y heterogeneidad de los datos, así como la exposición geográfica y la dispersión tecnológica de los entornos operativos.

Se incorpora la participación de las partes interesadas conforme a lo dispuesto en la ISO/IEC 27001:2022, sección 4.2 “Comprender las necesidades y expectativas de las partes interesadas”, donde se requiere identificar sus requisitos y determinar cuáles serán abordados por el SGSI. Esto se complementa con prácticas de gobernanza como las definidas en COBIT 2019 – APO12: Gestión del Riesgo, que orientan la alineación del diseño con objetivos de negocio, contexto institucional y marcos regulatorios.

El análisis de riesgos se fundamenta en las directrices técnicas descritas en ISO/IEC 27005:2022, sección 5.1 “Proceso de gestión de riesgos de seguridad de la información” y sección 6 “Establecimiento del contexto”, las cuales definen el proceso de identificación, valoración y tratamiento del riesgo adaptado al entorno específico de los activos. Además, se aplican criterios de evaluación basados en MAGERIT v3 Libro 2 – Catálogo de Elementos, Libro 3 – Guía de Técnicas, integrando catálogos estructurados de activos, amenazas y salvaguardas.

4.1.2 *Fase Hacer*

La fase Hacer (Do) formula el diseño técnico del modelo de seguridad y ejecuta operativamente los controles definidos para proteger los activos de información en proyectos de investigación, integrándolos de manera efectiva en los procesos tecnológicos y organizativos. Este proceso diseña y aplica controles asociados a los activos, priorizando su criticidad, madurez tecnológica y exposición al entorno, estructurándolos por propósito: preventivos, detectivos, correctivos o disuasivos conforme a la Sección 5 "Organización", la Sección 6 " Controles de personas", y la Sección 8 "Controles tecnológicos" de ISO/IEC 27002:2022. La segmentación funcional y la asignación de responsabilidades se diseñan y aplican considerando la estructura institucional, siguiendo el principio de proporcionalidad descrito en la Sección 5.2 "Liderazgo y compromiso" de ISO 31000:2018, que enfatiza la integración de la gestión del riesgo en todas las actividades organizativas, La estructura de gobernanza se refuerza con el objetivo APO01 "Administrar el marco de gestión de TI " de COBIT 2019, que alinea los procesos con las metas estratégicas. Este enfoque se complementa con controles técnicos seleccionados de las familias AC "Control de acceso", IA "Identificación y autenticación", AU "Auditoría y responsabilidad", y SI "Supervisión del sistema" del NIST SP 800-53 Rev. 5, aplicados según el tipo de activo y su nivel de exposición.

4.1.3 *Fase Verificar*

La verificación permite evaluar la consistencia interna del modelo sin requerir su ejecución. Se revisa la coherencia entre los riesgos identificados y los controles propuestos, así como la asignación de funciones y el grado de cobertura frente a amenazas plausibles.

Esta revisión se sustenta en las recomendaciones de ISO/IEC 27005:2022, sección 7 "Proceso de evaluación de riesgos de seguridad de la información", que establece un ciclo iterativo de revisión de riesgos y controles previo al tratamiento definitivo. Además, se contemplan elementos de evaluación documental exigidos por ISO/IEC 27001:2022, cláusulas 6.1.2 y 6.1.3, que obligan a documentar el proceso de evaluación y tratamiento de riesgos.

4.1.4 *Fase Actuar*

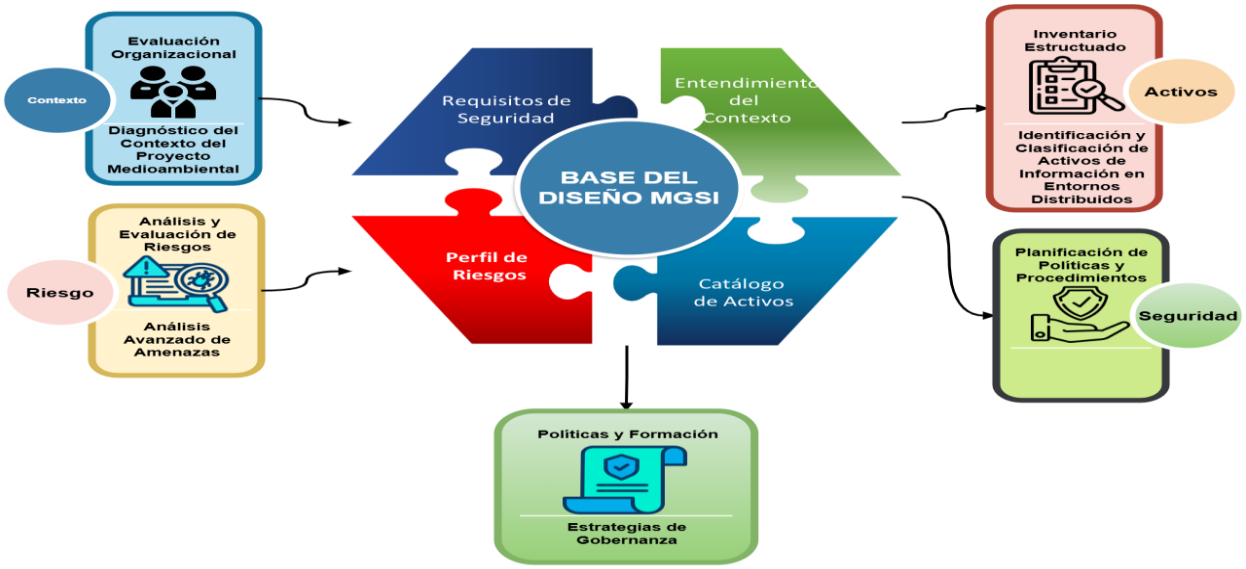
Esta fase consolida los mecanismos de ajuste y mejora continua del modelo. Se prevé su adaptación frente a cambios tecnológicos, regulatorios o estructurales, garantizando su vigencia y aplicabilidad futura. Esta lógica responde a las buenas prácticas definidas en ISO 31000:2018, donde se plantea la necesidad de retroalimentación para fortalecer la gestión del riesgo en ciclos repetitivos y adaptativos.

La capacidad de revisión periódica y ajuste se alinea con las exigencias de gobernanza dinámica en proyectos con múltiples actores y tecnologías emergentes. No se propone una reestructuración del modelo, sino un mecanismo formalizado para actualizar su contenido sin comprometer su integridad metodológica.

Capítulo 5: Fase de Planificación (Plan): Diagnóstico y Análisis de Riesgos

Figura 6

Fundamentos Estratégicos del Modelo de Seguridad



Fuente: Elaboración propia

Nota: La Figura presenta la estructura conceptual de esta fase, anticipando los elementos importantes que serán desarrollados en los apartados siguientes. Esta visión integradora facilita la lectura progresiva de los procesos de diagnóstico, valoración de activos, análisis de riesgos y planificación del diseño.

La fase Planear (Plan) del ciclo PHVA establece las bases metodológicas y estratégicas del modelo de gestión de seguridad de la información (MGSI) para proyectos de investigación medioambiental. Su propósito es garantizar la protección de datos sensibles, como registros de biodiversidad, y la continuidad operativa en entornos colaborativos, objetivos definidos en (Sección 1.4 "Objetivos"), abordando desafíos operativos y normativos de (Sección 1.1 "Planteamiento del Problema", Sección 2.3 "Investigación Medioambiental", Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles", Sección 3.2 "Características Particulares de los Proyectos Medioambientales"). Esta etapa define el alcance y contexto del MGSI, identifica activos, analiza riesgos y planifica acciones, asegurando un enfoque sistemático.

El proceso metodológico se estructura en cinco etapas, fundamentadas en (Cláusula 4.1 "Entender la organización y su contexto" de ISO/IEC 27001:2022, Cláusula 6.1 "Acciones para

abordar riesgos y oportunidades" de ISO/IEC 27001:2022, Sección 6 "Proceso" de ISO 31000:2018, Capítulo 3 "Método de análisis de riesgos" del Libro I de MAGERIT v3). Cada etapa contribuye a los objetivos de (Sección 1.4):

- **Diagnóstico del Contexto (Sección 5.1)**: Caracteriza el entorno operativo, identificando factores como la fragmentación institucional (diferencias en capacidades tecnológicas entre universidades, ONGs y gobiernos) y limitaciones de conectividad en áreas remotas, descritas en (Sección 2.3 "Investigación Medioambiental"). Por ejemplo, evalúa redes de sensores IoT en entornos remotos, apoyando la continuidad operativa.
- **Identificación y Clasificación de Activos (Sección 5.2)**: Inventaría activos como datos geoespaciales, sistemas SIG y dispositivos IoT, clasificándolos según su criticidad en entornos distribuidos. Esto protege datos sensibles de (Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles").
- **Análisis y Evaluación de Riesgos (Sección 5.3)**: Identifica amenazas, como accesos no autorizados a datos de biodiversidad, y evalúa su impacto, priorizando riesgos para cumplir con (Sección 1.4 "Objetivos").
- **Análisis Avanzado de Amenazas (Sección 5.4)**: Examina amenazas específicas, como ciberataques a sensores IoT, para diseñar defensas proactivas, contribuyendo a la resiliencia operativa.
- **Planificación de Formación y Políticas (Secciones 5.5 y 5.6)**: Define acciones de concienciación para mitigar riesgos humanos y establece políticas, como la política de seguridad del MGSI, conforme a (Cláusula 5.2 "Política" de ISO/IEC 27001:2022), asegurando cumplimiento normativo, por ejemplo, con (Ley 1581 de 2012, Artículo 3 "Definiciones").

La política de seguridad del MGSI garantiza la confidencialidad, integridad y disponibilidad de los activos, priorizando la mitigación de accesos no autorizados y fallos de infraestructura en entornos remotos. Estas etapas responden a las particularidades medioambientales, como la interoperabilidad tecnológica en (Sección 3.2 "Características Particulares de los Proyectos Medioambientales"), y protegen datos sensibles, como mediciones climáticas, alineándose con (Sección 1.4.1). Los resultados facilitan el diseño de controles en

(Sección 6 "Fase de Diseño (Do)"), auditorías en (Sección 7 "Fase Verificar (Check)") y ajustes en (Sección 8 "Fase Actuar (Act)").

5.1 Diagnóstico del Contexto del Proyecto Medioambiental

El diagnóstico del contexto establece una etapa inicial dentro de la fase de planificación, orientada a caracterizar las condiciones operativas, tecnológicas y normativas que definen los proyectos de investigación medioambiental, con el propósito de identificar factores que afectan la seguridad de la información. Este proceso busca generar un entendimiento integral del entorno para orientar las actividades subsiguientes, como la identificación de activos y la evaluación de riesgos, asegurando que el modelo de gestión de seguridad de la información (MGSI) responda de manera efectiva a las dinámicas reales del sector. La fundamentación de este diagnóstico se basa en (4.1 "Entender la organización y su contexto" de ISO/IEC 27001:2022), que requiere analizar los factores internos y externos relevantes, y en (Sección 5.3 "Integración" de ISO 31000:2018), que promueve la incorporación del contexto en los procesos de gestión del riesgo.

Este análisis se desarrolla considerando las características específicas del entorno medioambiental descritas en los apartados 1.1 a 3.2, abarcando las condiciones tecnológicas que incluyen sistemas de monitoreo remoto, como estaciones automáticas de calidad del aire (apartado 2.3.3.1), y plataformas de procesamiento distribuido, como repositorios de datos abiertos (apartado 2.3.3.6), cuya interoperabilidad genera riesgos de accesos no autorizados y errores de integración. Asimismo, se identifican limitaciones de conectividad en áreas remotas, que afectan tecnologías como redes satelitales (apartado 2.3.3.4) y aumentan la exposición a interrupciones operativas, así como la fragmentación institucional entre actores, como centros de investigación y entidades gubernamentales, que presentan diferencias en madurez tecnológica (apartado 1.1). El diagnóstico también integra el marco normativo, incluyendo regulaciones como (Ley 1581 de 2012, Artículo 3 "Definiciones"), que establece requisitos para proteger datos sensibles, tales como registros de emisiones contaminantes (apartado 3.1), asegurando que el MGSI se ajuste a las exigencias legales y operativas del sector.

Para garantizar un enfoque sistemático, el proceso de diagnóstico se organiza en tres componentes fundamentales que se desarrollan en las subsecciones siguientes: la definición de objetivos, que establece el propósito del análisis; la delimitación del alcance, que precisa las áreas

de enfoque; y la identificación de aspectos clave, que abarca las técnicas de recolección de información, los factores a analizar y su aplicación específica al sector ambiental. Este método permite capturar una visión detallada del entorno, identificando elementos que condicionan la seguridad de la información, como la exposición de datos de monitoreo hídrico a usos indebidos (apartado 3.1) y la vulnerabilidad de dispositivos móviles de campo a configuraciones inseguras (apartado 2.3.3.3). Dichos factores orientan la planificación de actividades posteriores, como la definición de controles específicos para mitigar riesgos asociados a estas tecnologías.

Además, este proceso incorpora las expectativas de las partes interesadas, identificando las necesidades de los investigadores de disponer de datos confiables para modelado climático, las exigencias gubernamentales de cumplir con normativas de protección de datos, y las prioridades de las ONG de resguardar la privacidad de comunidades locales, conforme a (4.2 "Entender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022). Este análisis Multi-Actor garantiza que el MGSI sea inclusivo y responda a las prioridades descritas en el apartado 1.1, como la resiliencia operativa frente a interrupciones y la protección de datos sensibles frente a usos indebidos. La integración con principios de gobernanza estratégica, siguiendo (EDM01 "Asegurar el establecimiento y el mantenimiento del marco de gobierno" de COBIT 2019), asegura que las decisiones de seguridad sean coherentes con los objetivos institucionales, fortaleciendo la planificación del modelo.

El diagnóstico genera un conjunto de hallazgos que sirven como insumo de suma importancia para las etapas posteriores de la fase de planificación, permitiendo identificar activos críticos, como sistemas de almacenamiento distribuido (apartado 2.3.3.5), y evaluar riesgos asociados a su uso, como la exposición a ataques DDoS. Este proceso contribuye al objetivo general del proyecto, establecido en el apartado 1.4.1, de proteger y gestionar de manera efectiva los activos de información, al garantizar que las estrategias de seguridad se diseñen considerando las condiciones reales del contexto medioambiental. Asimismo, proporciona una base estructurada y trazable para las fases de diseño (Sección 6), verificación (Sección 7) y mejora (Sección 8) del ciclo PHVA, asegurando la coherencia y sostenibilidad del modelo de seguridad en su aplicación al sector ambiental.

Figura 7

Diagrama de Flujo del Proceso de Diagnóstico Organizacional



Fuente: Elaboración propia

La Figura representa de forma secuencial las etapas clave para realizar el diagnóstico organizacional. El proceso se inicia con la identificación de factores internos y externos, seguido de la recolección estructurada de información mediante entrevistas, revisión documental y análisis normativo. Posteriormente, se analizan amenazas y oportunidades con base en marcos como ISO/IEC 27001, MAGERIT y NIST SP 800-53, lo que permite construir un perfil del entorno y establecer áreas prioritarias de intervención. Este flujo asegura trazabilidad, alineación con normas internacionales y sustento para la toma de decisiones estratégicas en materia de seguridad de la información.

5.1.1 *Objetivo del Diagnóstico*

El objetivo del diagnóstico consiste en caracterizar de manera integral las condiciones operativas, tecnológicas y normativas que enmarcan los proyectos de investigación medioambiental, con la finalidad de identificar los factores que determinan la seguridad de la información y orientar el desarrollo del modelo de gestión de seguridad de la información (MGSI). Este análisis se centra en comprender las dinámicas que influyen en la protección de los activos de información, considerando las particularidades del entorno identificadas en el apartado 1.1, como las diferencias en las prioridades de los actores involucrados, y en el apartado 2.3, que describe las complejidades tecnológicas del sector. La fundamentación de este proceso se basa en

(4.1 "Entender la organización y su contexto" de ISO/IEC 27001:2022), que establece la necesidad de analizar los factores internos y externos relevantes, y en (Sección 5.4 "Diseño" de ISO 31000:2018), que define un marco para comprender el entorno de riesgo y su impacto en la planificación de la seguridad.

Este diagnóstico busca capturar una visión detallada de los elementos que afectan la seguridad de los datos y sistemas, considerando la diversidad tecnológica descrita en el apartado 2.3.3, como los sistemas de modelado climático (apartado 2.3.3.2), que enfrentan riesgos de integridad debido a errores en la integración de datos, y los repositorios de datos abiertos (apartado 2.3.3.6), susceptibles a accesos no autorizados por configuraciones inadecuadas. También analiza las dinámicas Multi-Actor, donde entidades como universidades y gobiernos presentan distintos niveles de madurez tecnológica y prioridades, según el apartado 1.1, lo que genera desafíos en la interoperabilidad y la estandarización de procesos. Además, se evalúan las exigencias normativas, como (Ley 1581 de 2012, Artículo 3 "Definiciones"), que establece requisitos para proteger datos personales, y (Ley 1712 de 2014, Artículo 3 "Principios"), que impone obligaciones de transparencia para datos públicos, asegurando que el MGSI se alinee con el marco legal aplicable.

El proceso permite identificar factores específicos que condicionan la seguridad de la información, como la vulnerabilidad de los dispositivos móviles de campo (apartado 2.3.3.3) a robos físicos en áreas remotas, que comprometen la confidencialidad de datos geoespaciales, y la exposición de registros de emisiones contaminantes (apartado 3.1) a usos indebidos que podrían afectar políticas públicas. Estos elementos, detallados en los apartados 2.3 y 3.2, orientan la planificación de actividades posteriores, como la identificación de activos y la evaluación de riesgos, al proporcionar un entendimiento claro de las amenazas potenciales y las condiciones operativas. Este análisis garantiza que el MGSI aborde los desafíos propios del sector ambiental, como la gestión de datos distribuidos y la colaboración interinstitucional, descrita en el apartado 2.3.

Además, este diagnóstico integra las expectativas de las partes interesadas, identificando necesidades como la de los investigadores de acceder a datos confiables para análisis de tendencias ambientales, las exigencias gubernamentales de cumplir con normativas de protección de datos, y las prioridades de las ONG de resguardar la privacidad de comunidades locales, conforme a (4.2 "Entender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022). Este

enfoque Multi-Actor asegura que el modelo sea inclusivo y responda a las prioridades definidas en el apartado 1.1, como la resiliencia operativa frente a interrupciones y la protección de datos sensibles frente a usos indebidos. La alineación con principios de gobernanza estratégica, siguiendo (EDM01 " Asegurar el establecimiento y el mantenimiento del marco de gobierno " de COBIT 2019), garantiza que las decisiones de seguridad sean coherentes con los objetivos institucionales, fortaleciendo la planificación del modelo.

Los resultados obtenidos proporcionan un insumo fundamental para las etapas posteriores de la fase de planificación, permitiendo identificar activos críticos, como sistemas de almacenamiento distribuido (apartado 2.3.3.5), y evaluar riesgos asociados a su uso, como la exposición a ataques DDoS (apartado 3.2). Este proceso contribuye al objetivo general del proyecto, definido en el apartado 1.4.1, de proteger y gestionar de manera efectiva los activos de información, al garantizar que las estrategias de seguridad se diseñen considerando las condiciones reales del contexto medioambiental. Asimismo, establece un fundamento estructurado y trazable para las fases de diseño (Sección 6), verificación (Sección 7) y mejora (Sección 8) del ciclo PHVA, asegurando la coherencia y sostenibilidad del modelo de seguridad en su aplicación al sector ambiental.

5.1.2 *Alcance del Diagnóstico*

Con base en el objetivo establecido de caracterizar el contexto de los proyectos de investigación medioambiental, el alcance del diagnóstico delimita las áreas de análisis para garantizar que el modelo de gestión de seguridad de la información (MGSI) se enfoque en las prioridades y desafíos específicos del sector, sin exceder los propósitos de la fase de planificación. Este proceso se fundamenta en (4.3 "Determinar el alcance del sistema de gestión de seguridad de la información" de ISO/IEC 27001:2022), que requiere establecer los límites del sistema, y en (Sección 5.4.1 "Comprensión de las organizaciones y su contexto" de ISO 31000:2018), que orienta la identificación de factores internos y externos relevantes para la gestión del riesgo. El análisis abarca proyectos que operan en entornos interinstitucionales y distribuidos, con alta dependencia tecnológica, considerando las dinámicas Multi-Actor descritas en el (Apartado 1.1 "Introducción"), como la colaboración entre universidades y entidades gubernamentales, y las tecnologías detalladas en el (Apartado 2.3.3 "Infraestructura tecnológica en proyectos de

investigación"), incluyendo sistemas de almacenamiento distribuido (Apartado 2.3.3.5 "Sistemas de almacenamiento distribuido") y plataformas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático").

El diagnóstico se centra en la gestión de datos sensibles, como registros de calidad del agua (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"), que enfrentan riesgos de uso indebido, y en tecnologías como redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas"), cuya conectividad limitada en áreas remotas incrementa la exposición a interrupciones. Se excluyen actividades operativas, como la implementación de controles específicos, que corresponden a la (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), limitándose a identificar condiciones que orienten dichas medidas, como la necesidad de segmentación de redes para proteger plataformas analíticas. Asimismo, se evalúan las exigencias normativas, como (Ley 1712 de 2014, Artículo 3 "Principios"), que establece requisitos de transparencia para datos públicos, y (Ley 1581 de 2012, Artículo 3 "Definiciones"), que exige proteger datos personales, garantizando que el MGSI cumpla con el marco legal aplicable.

Además de las áreas técnicas y normativas, el diagnóstico examina las expectativas de las partes interesadas, identificando la necesidad de los investigadores de garantizar la disponibilidad de datos para estudios de tendencias ambientales, y las prioridades de las ONG de resguardar comunidades locales frente a la exposición de información, conforme a (4.2 " Comprender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022). Este enfoque establece un alcance que orienta la identificación de activos (5.2) y la evaluación de riesgos (5.3), contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y proporciona un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

5.1.3 *Proceso del Diagnóstico y Aspectos Clave*

Con base en el alcance definido, el proceso metodológico para caracterizar el contexto de los proyectos de investigación medioambiental se centra en identificar aspectos clave que influyen en la seguridad de la información. Este proceso se organiza de manera sistemática para generar un panorama integral que oriente las actividades posteriores de planificación, como la identificación de activos y la evaluación de riesgos, contribuyendo al desarrollo del modelo de gestión de seguridad de la información (MGSI). El enfoque se basa en (4.1 "Entender la organización y su contexto" de ISO/IEC 27001:2022), que requiere analizar factores internos y externos relevantes, y en (Sección 5.3 "Integración" de ISO 31000:2018), que promueve incorporar el contexto en los procesos de gestión del riesgo, garantizando una planificación alineada con las condiciones del sector ambiental.

Para garantizar su efectividad, el proceso de diagnóstico organizacional debe ser liderado y ejecutado por actores específicos que garanticen una visión integral del contexto y de los riesgos asociados a los activos de información. La alta dirección asume la responsabilidad de demostrar liderazgo, asegurando la disponibilidad de recursos y la alineación con la dirección estratégica, conforme a (5.1 "Liderazgo y compromiso" de ISO/IEC 27001:2022), que requiere garantizar los recursos necesarios para el sistema de gestión de seguridad de la información. El responsable del SGSI coordina la recolección de datos y propone estrategias de tratamiento de riesgos, según (5.3 "Funciones, responsabilidades y autoridades de la organización" de ISO/IEC 27001:2022), que exige asignar responsabilidades claras, y (Sección 1.6 "El análisis y el tratamiento de los riesgos en su contexto" de MAGERIT v3 Libro I), que define esta función dentro del análisis de riesgos. Los equipos de seguridad aportan información sobre amenazas y vulnerabilidades, vinculándose con (Sección 5 "Amenazas" de MAGERIT v3 Libro II: Catálogo de Elementos), que cataloga amenazas sobre activos. Las partes interesadas identifican requisitos regulatorios y operativos, conforme a (4.2 "Entender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022), que requiere determinar sus necesidades pertinentes.

En este sentido, el proceso se organiza en tres componentes, desarrollados en las subsecciones siguientes: la definición de objetivos, la delimitación del alcance, y la identificación de aspectos clave, abarcando técnicas de recolección, factores a analizar y su aplicación al sector ambiental. Este método permite capturar elementos específicos que afectan la seguridad, como la

vulnerabilidad de sistemas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático") a errores de integración, y la exposición de registros de calidad del aire (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") a usos indebidos, orientando la planificación de medidas específicas. Los hallazgos generados sirven como insumo para identificar activos (5.2) y evaluar riesgos (5.3), contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y proporcionan un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

5.1.3.1 Técnicas de Recolección de Información.

Con el proceso de diagnóstico ya estructurado, este apartado se enfoca en detallar las técnicas específicas que se emplean para recopilar la información necesaria. El objetivo es caracterizar de manera profunda el contexto de los proyectos de investigación, asegurando que los datos obtenidos sean precisos, relevantes y suficientes para identificar los factores que afectan la seguridad de la información. La selección de estas técnicas se basa en el principio de (6.2 "Comunicación y consulta" de ISO 31000:2018), que marca la importancia de involucrar a todas las partes interesadas para obtener una visión completa del entorno y sus riesgos, garantizando así un diagnóstico verdaderamente alineado con las necesidades del sector ambiental.

La primera técnica, y una de las más valiosas, es la realización de entrevistas estructuradas con los actores clave. Conversar directamente con investigadores, administradores de sistemas y representantes de ONG permite ir más allá de los documentos y capturar sus necesidades reales, sus preocupaciones y los desafíos operativos que enfrentan a diario. Conforme a (4.2 "Entender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022), que exige determinar las expectativas relevantes. Por ejemplo, una entrevista puede revelar la preocupación de un científico por la integridad de los registros de calidad del agua (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") y cómo una manipulación podría afectar sus modelos predictivos, un matiz que un simple inventario de activos no capturaría. A esto se suma la revisión documental, un proceso sistemático que analiza políticas internas, normativas vigentes

como la Ley 1581 de 2012, y reportes técnicos para construir un mapa claro de los requisitos regulatorios y operativos que el modelo de seguridad debe cumplir.

Paralelamente, se lleva a cabo un análisis de la infraestructura tecnológica. Este no es un simple inventario, sino una evaluación funcional de los dispositivos, como los sistemas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático"), y redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas"), para detectar vulnerabilidades concretas, como configuraciones por defecto, puertos abiertos o limitaciones de conectividad que podrían ser explotadas. Este enfoque práctico se alinea directamente con la metodología (Sección 3.1.1 "Paso 1: Activos" de MAGERIT v3 Libro I), que recomienda identificar y clasificar los activos no solo para saber qué se tiene, sino para entender su exposición real a los riesgos.

Para organizar, consolidar y dar trazabilidad a todo este proceso de diagnóstico, la Tabla 3 se presenta como la herramienta central. Esta tabla es la estructura que vincula cada una de las actividades de recolección y análisis con los marcos normativos que las justifican (ISO, COBIT, NIST, Etc.) y con los actores responsables de ejecutarlas. Esta disposición permite identificar con claridad el alcance operativo de cada acción y lo que es más importante, muestra cómo estas actividades se conectan con las decisiones estratégicas que darán forma al modelo de seguridad. Así, se asegura que el diagnóstico no sea un ejercicio abstracto, sino que genere insumos verificables, organizados y coherentes que alimenten de forma lógica las fases posteriores del diseño.

Tabla 3

Diagnóstico del Contexto Organizacional

ACTIVIDADES	ETAPAS	NORMATIVAS Y MARCOS RELACIONADOS
Obtener la aprobación de la dirección para iniciar el proyecto	Establecimiento de prioridades organizacionales para el MGSI.	ISO 27001 4.1 (Entender la organización y su contexto), COBIT 2019 EDM01 (Asegurar el establecimiento y el mantenimiento del marco de gobierno), ISO/IEC 38500 5.3 (Generación de Valor), NIST SP 800-53 PM-9 (Estrategia de Gestión de Riesgos).
	Definir el alcance preliminar del MGSI.	ISO 27001 4.2 (Comprender las necesidades y expectativas de las partes interesadas), TOGAF (Definición de Arquitectura Empresarial), ITIL 4 (Gestión del Portafolio).
	Creación del plan del proyecto para su aprobación.	ISO 27001 5.1 (Liderazgo y compromiso), ITIL 4 (Gestión del Cambio Organizacional), COBIT 2019 APO02 (Gestión de la Estrategia), ISO/IEC 38500 5.4 (Estrategia).

ACTIVIDADES	ETAPAS	NORMATIVAS Y MARCOS RELACIONADOS
	Definir el alcance y límites del MGSI.	ISO 27001 7.4 (Comunicación), COBIT 2019 APO01 (Administrar el marco de gestión de TI), Magerit - Libro I 4.1 (Marco de Gestión de Riesgos), CIS Controls v8 02 (Inventario y Control de Activos de Software)
	Consulta con los Stakeholders para entender sus expectativas y necesidades.	ISO 27001 4.2 (Comprender las necesidades y expectativas de las partes interesadas), Magerit - Libro I 7.2.2 (7.2 Seguridad del sistema de información Contexto), COBIT 2019 APO07 (Gestión de Recursos Humanos).
Definir el alcance, los límites y la política del MGSI	Definir los límites de las tecnologías de información y comunicaciones.	ISO 27001 4.3 (Determinación del alcance del SGSI), Magerit - Libro I 4.4 (Indicadores de control del proceso de gestión de riesgos), TOGAF (Enterprise Architecture Framework), NIST SP 800-53 RA-3 (Evaluación del Riesgo).
	Definir los límites físicos.	ISO 27001 4.3 (Determinación del Alcance del SGSI), Magerit - Libro I 7.2.2 (7.2 Seguridad del sistema de información, Contexto).
	Integrar cada alcance en un marco unificado.	Magerit - Libro I 4.4 (Marco de gestión de riesgos), COBIT 2019 APO02 (Gestión de la Estrategia).
	Determinar los actores (instituciones académicas, gobierno, ONG, empresa privada).	ISO 27001 4.2 (Comprender las necesidades y expectativas de las partes interesadas), COBIT 2019 APO07 (Gestión de Recursos Humanos), ISO/IEC 38500 5.7 (Participación de los Interesados).
	Desarrollar la política del MGSI y obtener la aprobación.	ISO 27001 5.1 (Liderazgo y compromiso), CIS Controls v8 3 Protección de los Datos), ISO/IEC 38500 5.8 (Liderazgo).
	Definición de roles y responsabilidades.	ISO 27001 5.3 (Roles y responsabilidades organizacionales), Magerit - Libro I 4.2.1 (Roles y funciones), ISO/IEC 38500 5.6 (Rendición de cuentas).
Realizar el análisis de requisitos de seguridad de la información	Definir los requisitos de seguridad de la información para el proceso MGSI.	ISO 27001 4.2 (Comprender las necesidades y expectativas de las partes interesadas), Magerit - Libro I 3.2.2. (Tarea MAR.2: Caracterización de las amenazas), NIST SP 800-53 PL-7 (Concepto de operaciones), COBIT 2019 6.4.3 (Niveles de madurez de las áreas de enfoque).
	Identificar activos dentro del alcance del MGSI.	ISO 27001 6.1.2 (Evaluación de Riesgos de Seguridad de la Información), CIS Controls v8 1 (Inventario y Control de los Activos Empresariales).
	Diagnóstico estado actual de seguridad de la información del proyecto.	Magerit - Libro I 7.2.2 (Contexto), ISO 31000 5.4.1 (Comprensión de las organizaciones y su contexto), NIST SP 800-53 RA-1 (Política y Procedimientos), ISO/IEC 38500 5.10 (Gobernanza del Riesgo)
	Examinar requisitos legales y normativos.	ISO 27001 6.1.2 (Evaluación de Riesgos Normativos), COBIT 2019 APO13 (Gestión de Seguridad de la Información), NIST SP 800-53 CA-5 (Plan de Acción e Hitos).
	Revisar los lineamientos y restricciones particulares de cada entidad involucrada.	ISO 27001 4.2 (Comprender las necesidades y expectativas de las partes interesadas), ITIL 4 (Gestión del Portafolio), CIS Controls v8 3-1 (Establecer y mantener un proceso de gestión de datos).

Fuente*: Elaboración Propia*

La Tabla 3 presenta una organización estructurada de las actividades correspondientes al diagnóstico organizacional, conectándolas con los marcos normativos de referencia y con los

actores encargados de su ejecución. Esta disposición no solo permite identificar con claridad el alcance operativo de cada acción, sino que también muestra cómo estas se relacionan con las decisiones estratégicas que conforman el modelo de seguridad.

Más que un inventario de tareas, la tabla actúa como una herramienta de trazabilidad que vincula las acciones metodológicas con los requerimientos técnicos definidos por normas como ISO/IEC 27001:2022, MAGERIT v3 e ISO 31000:2018. Esta relación directa asegura que el diagnóstico no se reduzca a una caracterización abstracta del entorno, sino que genere insumos verificables, organizados y coherentes con las fases posteriores del modelo.

Cada actividad aporta a la construcción progresiva de una visión operativa del contexto, facilita la identificación de condiciones que influyen en el nivel de riesgo, y apoya la toma de decisiones desde una etapa temprana del proceso. La incorporación explícita de los marcos de referencia fortalece la consistencia documental del modelo, mientras que la asignación clara de responsabilidades permite alinear los esfuerzos institucionales bajo una lógica participativa y coordinada.

Este enfoque está alineado con los principios del ciclo PHVA, en el cual la etapa “Planear” requiere establecer una base estructurada que permita orientar el sistema desde sus primeros pasos. La tabla, en este sentido, ofrece una visión funcional que conecta los requisitos normativos con las prácticas reales de planificación en la organización.

Nota: Utilizar el Anexo C, Guía de Referencia para Desarrollar un Diagnóstico de Madurez en Seguridad de la Información

5.1.3.2 Aspectos a Diagnosticar en el Contexto Ambiental.

Habiendo detallado las técnicas de recolección de información, este apartado identifica los aspectos principales que deben diagnosticarse para caracterizar el contexto ambiental de los proyectos de investigación, permitiendo comprender los factores que influyen en la seguridad de la información. Este diagnóstico se enfoca en elementos operativos, tecnológicos y normativos que afectan la protección de los activos, asegurando que el modelo de gestión de seguridad de la información (MGSI) sea adecuado para el sector ambiental. El enfoque se basa en (Sección 5.4.1

"Comprensión de las organizaciones y su contexto" de ISO 31000:2018), que orienta la identificación de factores internos y externos relevantes para la gestión del riesgo.

En primer lugar, se diagnostican las condiciones operativas, analizando las dinámicas Multi-Actor, como la colaboración entre universidades y entidades gubernamentales, que genera desafíos de interoperabilidad debido a diferencias en madurez tecnológica. Por ejemplo, la falta de estandarización en la gestión de datos geoespaciales (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") puede derivar en accesos no autorizados, afectando la confidencialidad de la información. Además, se evalúan las limitaciones operativas, como las interrupciones en áreas remotas que impactan la disponibilidad de servicios soportados por redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas").

A continuación, se examinan los aspectos tecnológicos, identificando vulnerabilidades en sistemas como plataformas de datos abiertos (Apartado 2.3.3.6 "Repositorios de datos abiertos"), que pueden ser susceptibles a configuraciones inseguras, y dispositivos móviles de campo (Apartado 2.3.3.3 "Dispositivos móviles de campo"), expuestos a robos físicos que comprometen datos sensibles. Este análisis se alinea con (Sección 3.1.1 "Paso 1: Activos" de MAGERIT v3 Libro I), que recomienda identificar activos y sus riesgos asociados. Por último, se analizan los requisitos normativos, como (Ley 1712 de 2014, Artículo 3 "Principios"), que exige transparencia en datos públicos, y (Ley 1581 de 2012, Artículo 3 "Definiciones"), que demanda proteger datos personales, asegurando que el MGSI cumpla con las obligaciones legales.

Los aspectos diagnosticados generan hallazgos que permiten identificar activos (5.2) y evaluar riesgos (5.3), contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y proporcionan un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

5.1.3.3 Aplicación contextual al sector ambiental.

Tras haber identificado los aspectos principales, este apartado aplica los resultados del diagnóstico al sector ambiental, adaptando las condiciones operativas, tecnológicas y normativas a los proyectos de investigación medioambiental para garantizar que el modelo de gestión de

seguridad de la información (MGSI) responda a sus particularidades. Este proceso se basa en (Sección 5.3 "Integración" de ISO 31000:2018), que promueve incorporar el contexto en los procesos de gestión del riesgo, asegurando que las estrategias de seguridad sean pertinentes para el sector ambiental.

En el ámbito operativo, se priorizan las dinámicas Multi-Actor, como la colaboración interinstitucional, que requiere protocolos estandarizados para gestionar datos sensibles, como registros de emisiones contaminantes (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"). Por ejemplo, la falta de estandarización puede derivar en accesos no autorizados que comprometan la confidencialidad, afectando la confianza en los datos compartidos entre universidades y gobiernos. Este análisis permite definir medidas que fortalezcan la interoperabilidad, reduciendo riesgos asociados a la fragmentación institucional.

Desde el punto de vista tecnológico, se abordan las vulnerabilidades identificadas en sistemas como estaciones automáticas de calidad del aire (Apartado 2.3.3.1 "Estaciones automáticas de calidad del aire"), que enfrentan riesgos de configuraciones inseguras, y sistemas de almacenamiento distribuido (Apartado 2.3.3.5 "Sistemas de almacenamiento distribuido"), expuestos a ataques DDoS (Apartado 3.2 "Riesgos asociados a la Sensibilidad de los Datos"). Este enfoque se alinea con (Sección 3.1.1 "Paso 1: Activos" de MAGERIT v3 Libro I), que recomienda identificar activos y sus riesgos para planificar medidas específicas. Asimismo, se consideran los requisitos normativos, como (Ley 1581 de 2012, Artículo 3 "Definiciones"), que exige proteger datos personales, asegurando que el MGSI cumpla con las obligaciones legales aplicables al sector ambiental.

Los resultados de esta aplicación contextual generan un panorama que permite identificar activos (5.2) y evaluar riesgos (5.3), contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y proporcionan un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

5.2 Identificación y Clasificación de Activos de Información en Entornos Distribuidos

Después de haber definido el entorno de los proyectos, el siguiente paso es identificar y clasificar los activos de información. Este proceso es un punto de partida necesario, ya que permite saber con precisión qué elementos hay que proteger. Sin este trabajo previo, cualquier medida de seguridad sería genérica y, por lo tanto, poco efectiva. El resultado de esta etapa sirve de base para el análisis de riesgos (5.3) y la posterior definición de controles (Sección 6), asegurando que los esfuerzos se dirijan a lo que realmente importa. El método para hacerlo se apoya en marcos reconocidos como el (Anexo A.5.9 " Inventario de información y otros activos asociados" de ISO/IEC 27001:2022), que requiere un inventario claro de activos, y en la (Sección 3.1.1 "Paso 1: Activos" de MAGERIT v3 Libro I), que detalla y orienta cómo estructurar el proceso de identificación y clasificación.

Hay que tener en cuenta que los entornos de investigación medioambiental, descritos en el (Apartado 2.3.3 "Infraestructura tecnológica en proyectos de investigación"), presentan condiciones especiales. La variedad de tecnologías, la colaboración entre diferentes actores y la conectividad limitada en zonas remotas crean un escenario de riesgo particular. Por ejemplo, los registros sobre la calidad del aire (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") no son solo cifras; son activos de alta sensibilidad cuyo mal uso podría llevar a decisiones equivocadas con un impacto directo en la salud pública. Del mismo modo, las plataformas de datos abiertos (Apartado 2.3.3.6 "Repositorios de datos abiertos"), aunque útiles para la ciencia, pueden sufrir accesos no autorizados si no se gestionan con los controles adecuados. Por eso, desde el inicio se puede ver que los activos a proteger abarcan desde los datos científicos hasta la propia infraestructura que los soporta.

Por lo tanto, la identificación debe cubrir los activos físicos, como los equipos de campo y los servidores, y también los intangibles, como los datos, el software y los servicios, sin dejar de lado la dinámica de colaboración entre los distintos actores. Para dar una estructura lógica a este proceso, la Figura 8 muestra un diagrama de flujo con el ciclo de vida completo de la gestión de activos. Este diagrama es útil porque conecta la estrategia general de la organización con el manejo diario de los activos, y muestra cómo la toma de decisiones y la gestión de riesgos deben estar presentes en cada fase: adquisición, asignación, mantenimiento y disposición. Las subsecciones que siguen explican en detalle cada parte de este proceso, empezando por el marco conceptual

(5.2.1), la tipología de activos para el contexto medioambiental (5.2.2), su clasificación y evaluación (5.2.3 y 5.2.4), y por último, la definición de una estrategia de protección por capas (5.2.5).

Además, se analizan las interdependencias entre activos, ya que en entornos distribuidos los fallos en un elemento pueden propagarse a otros. Por ejemplo, una interrupción en las redes satelitales (Apartado 2.3.3.2 “Infraestructura de Transmisión y Comunicaciones") puede afectar la disponibilidad de datos en sistemas de modelado climático (Apartado 2.3.3.3 en: " Plataformas de Procesamiento"), comprometiendo la continuidad operativa. Este análisis se alinea con (Sección 8.3 "Para descubrir y modelar las dependencias entre activos" de MAGERIT v3 Libro I), que sugiere documentar las relaciones para comprender los riesgos asociados. Por lo tanto, la clasificación resultante genera un inventario detallado que sirve como insumo para las fases de análisis de riesgos (5.3) y diseño de controles (Sección 6), contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y establece un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

Figura 8

Diagrama de Flujo del Proceso de Gestión de Activos de Información



Fuente: Elaboración propia. La priorización se basa en los principios para la selección del tratamiento de riesgos (ISO 31000:2018, ISO/IEC 27005:2022) y en los marcos para la gestión de la estrategia y la optimización de recursos (COBIT 2019)

5.2.1 *Proceso de Gestión Conceptual de Activos*

Con base en el marco definido, este apartado establece un proceso conceptual para la administración de activos de información, con el propósito de identificar, registrar, valorar y proteger los recursos físicos y digitales que soportan los objetivos del proyecto medioambiental a lo largo de su ciclo de vida. Este procedimiento se fundamenta en (Anexo A.5.9 "Inventario de información y otros activos asociados" de ISO/IEC 27001:2022), que requiere mantener un registro actualizado de los activos vinculados con la información, y en (Sección 3.1.1 "Paso 1: Activos" de MAGERIT v3 Libro I), que detalla cómo estructurar su identificación.

En primer lugar, el proceso comienza con la identificación de activos, abarcando datos y equipos esenciales para los proyectos de investigación medioambiental. Esto incluye datos como registros de calidad del agua (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"), que son sensibles a usos indebidos que podrían comprometer decisiones ambientales, y equipos como estaciones automáticas de monitoreo hídrico (Apartado 2.3.3.1 "Estaciones automáticas de calidad del aire"), expuestos a riesgos técnicos debido a

configuraciones inseguras. También se identifican servicios digitales, como repositorios de datos abiertos (Apartado 2.3.3.6 "Repositorios de datos abiertos"), que enfrentan riesgos de accesos no autorizados, y sistemas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático"), que dependen de infraestructuras distribuidas para su operación.

Seguidamente, se documentan las características de cada activo, considerando aspectos como su propietario, ubicación, función y ciclo de vida, para garantizar una visión integral del inventario. Por ejemplo, los sistemas de almacenamiento distribuido (Apartado 2.3.3.5 "Sistemas de almacenamiento distribuido") se documentan teniendo en cuenta su uso en entornos remotos, lo que afecta su exposición a interrupciones. Este paso se alinea con (CM-8 "Inventario de componentes del sistema" de NIST SP 800-53 Rev. 5), que exige visibilidad y control sobre los componentes del sistema, asegurando que no se omitan activos relevantes.

A continuación, se valoran los activos según su relevancia y sensibilidad, siguiendo principios como (5.12 "Clasificación de la información" de ISO/IEC 27002:2022), que orienta el tratamiento diferencial según el nivel de sensibilidad, y (9.1.3 " Evaluación del desempeño del portafolio de activos y los procesos de gestión de activos " de ISO 55002:2018), que estructura su gestión técnica. Este paso también identifica dependencias críticas, como la relación entre redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas") y sistemas de modelado climático, donde una interrupción en las primeras puede afectar la disponibilidad de datos en los segundos, alineándose con (Sección 8.3 "Para descubrir y modelar las dependencias entre activos" de MAGERIT v3 Libro I).

Este proceso se representa en el diagrama de flujo de la Figura 5, que ilustra su aplicación en entornos ambientales mediante una estructura visual que refleja las etapas clave y su interconexión. La figura presenta tres nodos principales que corresponden a las fases del proceso: un nodo inicial de identificación, que lista activos relevantes como datos hidrológicos (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") y equipos como estaciones automáticas de monitoreo hídrico (Apartado 2.3.3.1 "Estaciones automáticas de calidad del aire"), marcando el punto de partida para el inventario; un nodo intermedio de documentación y valoración, donde se registran atributos como propietario y función, y se evalúan dependencias mediante flechas que conectan activos interrelacionados, como redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas") con sistemas de modelado climático

(Apartado 2.3.3.2 "Sistemas de modelado climático"); y un nodo final de integración normativa, que incorpora requisitos legales como (Ley 1581 de 2012, Artículo 3 "Definiciones") y (Ley 1712 de 2014, Artículo 3 "Principios"), los cuales exigen proteger datos sensibles y garantizar transparencia en plataformas públicas, respectivamente. Además, las flechas de retroalimentación entre los nodos, representadas con líneas bidireccionales, reflejan la naturaleza iterativa del proceso, permitiendo ajustes continuos para adaptarse a cambios en el entorno ambiental y asegurar la efectividad del inventario generado.

Por lo tanto, este proceso genera un inventario que facilita la categorización (5.2.2), clasificación (5.2.3), y evaluación de los activos (5.2.4), contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y proporciona un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

5.2.2 *Tipología extendida de activos según contexto medioambiental*

Con base en el proceso de gestión establecido, este apartado define una tipología extendida de activos adaptada al contexto medioambiental, categorizando los elementos según su naturaleza y función para estructurar la identificación de requisitos de seguridad de la información. Esta categorización amplía el enfoque tradicional de inventario de activos, incorporando componentes de tecnología operativa (OT) y tecnología de la información (TI), y se fundamenta en (Sección 2 "Tipos de activos" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un catálogo detallado para clasificar activos, y en (Anexo A.5.9 " Inventario de información y otros activos asociados " de ISO/IEC 27001:2022), que establece la necesidad de identificar y documentar los activos relevantes.

En primer lugar, se identifican los datos ambientales como una categoría principal, que incluye registros sensibles como los datos hidrológicos y de biodiversidad (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"). Estos datos enfrentan riesgos de usos indebidos que podrían facilitar actividades ilegales, como la caza furtiva, o comprometer

decisiones ambientales, lo que requiere medidas para garantizar su confidencialidad e integridad. También se incluyen registros de calidad del aire y emisiones contaminantes, que deben cumplir con normativas como (Ley 1712 de 2014, Artículo 3 "Principios"), que exige transparencia en datos públicos.

Seguidamente, se categorizan los equipos tecnológicos, abarcando dispositivos de captura en campo e infraestructuras de comunicación. Esto incluye estaciones automáticas de monitoreo hídrico (Apartado 2.3.3.1 "Estaciones automáticas de calidad del aire"), expuestas a riesgos técnicos como configuraciones inseguras, dispositivos móviles de campo (Apartado 2.3.3.3 "Dispositivos móviles de campo"), vulnerables a robos físicos, y nodos satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas"), que enfrentan limitaciones de conectividad en áreas remotas. Estas arquitecturas mixtas operan con distintos niveles de exposición, lo que requiere un análisis de dependencias técnicas, alineado con (Sección 2.3 "Árboles de ataque" de MAGERIT v3 Libro III), que modela cómo las amenazas pueden propagarse dentro del entorno técnico.

A continuación, se incluyen los servicios digitales y entornos de procesamiento, como plataformas de datos abiertos (Apartado 2.3.3.6 "Repositorios de datos abiertos"), susceptibles a accesos no autorizados, y sistemas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático"), que dependen de redes interoperables. También se consideran servicios basados en la nube y equipos humanos con funciones científicas, asignando responsables para cada activo, conforme a (5.9 "Inventario de información y otros activos asociados" de ISO/IEC 27002:2022), que exige designar personas o grupos responsables, como investigadores principales o administradores de infraestructura tecnológica, dependiendo de su relevancia.

Por lo tanto, esta tipología permite vincular los activos con los riesgos inherentes (Sección 5.4), facilitando la clasificación funcional (5.2.3), la evaluación de criticidad (5.2.4), y la aplicación de controles proporcionales, contribuyendo al objetivo general del proyecto (Apartado 1.4.1 "Objetivo General") de proteger y gestionar los activos de información, y proporcionando un fundamento trazable para las fases de diseño (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), verificación (Sección 7 "Verificar (Check): Monitoreo y Evaluación del Modelo"), y mejora (Sección 8 "Actuar (Act): Mejora Continua y Lecciones Aprendidas") del ciclo PHVA.

Tabla 4

Clasificación de Datos

CRITERIO DE CLASIFICACIÓN	SUBCATEGORÍAS	DEFINICIÓN / ALCANCE	EJEMPLOS / REFERENCIAS
ORIGEN DE LOS DATOS	**Primarios**	Recolectados directamente por el equipo de investigación, con un protocolo específico de muestreo, observación o experimentación.	Mediciones in situ de calidad de agua (por ejemplo, pH, conductividad).
			Registros meteorológicos con estaciones portátiles.
			Cuestionarios a comunidades sobre percepción ambiental.
	Secundarios	Obtenidos de estudios previos, instituciones oficiales o bases de datos públicas/privadas, sin haber sido recabados originalmente por el equipo actual de investigación.	Informes de organismos gubernamentales (ministerios de medio ambiente, agencias meteorológicas).
			Artículos científicos y revisiones sistemáticas.
			Bases de datos internacionales (FAO, NASA, ESA).
NATURALEZA DE LOS DATOS	**Cuantitativos**	Se expresan en valores numéricos, adecuados para análisis estadístico o modelización.	Concentraciones de contaminantes (ppm, mg/L).
			Parámetros meteorológicos (temperatura, precipitación, humedad).
			Índices de diversidad biológica (Shannon, Simpson).
	Cualitativos	Información descriptiva no representada numéricamente; se centra en percepciones, propiedades o características de los fenómenos investigados.	Entrevistas semiestructuradas sobre cambios percibidos en un ecosistema.
			Descripciones etnográficas sobre la interacción humano-ambiente.
			Observaciones de comportamiento de especies (etología).
MÉTODO DE OBTENCIÓN	**Observacionales (in situ)**	Recopilados directamente en el entorno natural o en campo, sin manipulación deliberada de variables.	Conteo de poblaciones de fauna en su hábitat.
			Registros de calidad del aire con equipos portátiles.
			Muestreos de suelo para analizar nutrientes o contaminantes.
	Experimentales	Generados bajo diseños experimentales que controlan o manipulan variables para contrastar hipótesis de causalidad o eficacia de intervenciones.	Ensayos de laboratorio sobre toxicidad de un contaminante en un organismo modelo (por ejemplo, Daphnia magna).
			Parcelas experimentales con diferentes tratamientos de fertilización o riego para estudiar regeneración de ecosistemas.
	Remotos (teledetección, SIG)	Obtenidos mediante sensores satelitales, aéreos o submarinos (drones, LIDAR, radares, etc.), permitiendo medición a	Imágenes satelitales de la NASA para monitoreo de deforestación.

CRITERIO DE CLASIFICACIÓN	SUBCATEGORÍAS	DEFINICIÓN / ALCANCE	EJEMPLOS / REFERENCIAS
		distancia sin contacto directo con el área de estudio.	Datos LiDAR para caracterizar la estructura vertical de un bosque.
			Sensores remotos para detección de floraciones de algas en zonas costeras.
FUENTE / PROPÓSITO	**Monitoreo y vigilancia**	Recolección sistemática y continua para identificar tendencias, alertar sobre cambios críticos y apoyar la toma de decisiones en tiempo real o casi real.	Redes de estaciones de calidad del aire en áreas urbanas.
			Programas de seguimiento de aves migratorias.
			Observatorios costeros que miden temperatura y salinidad de manera ininterrumpida.
	Modelación / simulación	Empleados o generados en modelos matemáticos e informáticos que reproducen dinámicas complejas o proyectan escenarios futuros (clima, dispersión de contaminantes, uso de suelo, etc.).	Modelos climáticos del IPCC (CMIP6, por ejemplo).
			Simulaciones de dispersión de contaminantes con modelado hidrodinámico en ríos.
			Modelos de dinámica poblacional en áreas protegidas.
	Ciencia ciudadana / participativa	Producidos con la colaboración de voluntarios, comunidades locales o colectivos que participan en la recolección, validación o interpretación de datos.	Registros de avistamientos de aves en plataformas abiertas (eBird, iNaturalist).
			Mapeo participativo de recursos hídricos en comunidades rurales.
			Monitoreo vecinal de focos industriales de contaminación.
ACCESO, PROPIEDAD Y RESTRICCIONES	**Datos de Dominio Público**	Información accesible sin restricciones legales o de derechos de autor, publicada bajo licencias abiertas (CC BY, CC0, etc.).	Registros históricos de precipitación publicados por agencias meteorológicas.
			Cartografía oficial bajo licencias de datos abiertos (por ejemplo, institutos geográficos nacionales).
	Datos Privados	Titularidad de individuos, empresas o entidades privadas. Pueden requerir licencias, acuerdos de confidencialidad o contratación.	Estudios de impacto ambiental internos de una corporación.
			Bases de datos de extracción de recursos en manos de empresas mineras o petroleras.
	Datos Restringidos		Información ambiental en áreas militares que exige credenciales.

CRITERIO DE CLASIFICACIÓN	SUBCATEGORÍAS	DEFINICIÓN / ALCANCE	EJEMPLOS / REFERENCIAS
		Acceso limitado a usuarios autorizados o instituciones, por razones de seguridad, propiedad intelectual o convenios específicos.	Ubicaciones exactas de especies endémicas solo disponibles para investigadores acreditados.
	Datos con Restricciones de Uso	Pueden estar publicados de forma abierta o parcial, pero con condiciones de uso (licencia no comercial, obligación de citar, etc.).	Conjuntos geoespaciales con licencias CC BY-NC-SA.
			Estadísticas oficiales que permiten reproducir tablas agregadas, pero no microdatos sin autorización.
	Datos Sensibles	Su divulgación o uso indebido podría generar riesgos sociales, ambientales, culturales o de seguridad. Exigen protocolos de protección y, a veces, anonimización.	Ubicaciones precisas de especies amenazadas con alto riesgo de caza furtiva.
			Datos personales de comunidades indígenas que requieren salvaguarda cultural y legal.
	Datos Protegidos por Normativas	Regidos por leyes y regulaciones (RGPD, leyes de protección de datos personales, secretos industriales) que limitan su difusión.	Información personal de voluntarios, obligada a anonimización.
			Información industrial declarada secreto comercial.
	Datos Comunitarios o de Ciencia Ciudadana	Generados y resguardados por colectivos, con acuerdos de uso y soberanía de datos, a menudo orientados a la participación inclusiva.	Bases de datos gestionadas por comunidades locales sobre biodiversidad endémica.
			Observatorios comunitarios que documentan la calidad del agua.

Fuente: Elaboración Propia

La Tabla establece un mecanismo de clasificación orientado a organizar los datos utilizados en los proyectos de investigación medioambientales, con el propósito de facilitar decisiones proporcionales en materia de seguridad de la información. Esta segmentación permite adaptar las medidas de protección a las condiciones reales de generación, uso y almacenamiento de los datos, teniendo en cuenta no solo sus características técnicas, sino también su función dentro del proceso investigativo, su valor estratégico y los requisitos regulatorios que puedan aplicar.

La estructura de clasificación se articula en torno a tres dimensiones clave, seleccionadas por su capacidad para reflejar tanto la procedencia como el comportamiento operativo de los datos:

- **Origen**: Diferencia entre datos primarios, recolectados directamente por los equipos del proyecto a través de actividades controladas en campo o laboratorio bajo metodologías definidas; y datos secundarios, obtenidos a partir de fuentes externas como sistemas de monitoreo público, bases de datos institucionales o literatura científica. Esta distinción es relevante tanto para establecer la trazabilidad del dato como para definir los niveles de confianza, validación y responsabilidad durante su integración en los análisis del proyecto.
- **Naturaleza**: Clasifica los datos en cuantitativos, representados en forma numérica y utilizados para modelado estadístico, simulación, correlaciones u optimización de variables; y cualitativos, basados en contenido descriptivo o narrativo que captura percepciones, experiencias o contextos sociales y ambientales no estructurados. Esta dimensión influye directamente en el tipo de tratamiento documental, mecanismos de anonimización y criterios de interpretación, en especial cuando se gestionan fuentes sensibles o con implicaciones éticas.
- **Método de obtención**: Distingue entre datos observacionales, obtenidos mediante observación directa sin intermediación tecnológica significativa (por ejemplo, inventarios de biodiversidad, registros de campo, entrevistas); y datos automatizados, generados por sensores remotos, dispositivos IoT, estaciones meteorológicas o sistemas de captura digital continua. Esta dimensión incide en el tipo de respaldo requerido, frecuencia de actualización, monitoreo de integridad y complejidad de interoperabilidad entre sistemas.

La implementación de esta clasificación es consistente con lo establecido en la Sección 5.12 “Clasificación de la información”, de ISO/IEC 27002:2022 la cual establece que las

organizaciones deben estructurar esquemas formales de clasificación atendiendo a la sensibilidad de la información, sus requisitos legales o contractuales, y su impacto potencial sobre los procesos organizacionales. Adicionalmente, se encuentra alineada con el Control 3.7 “Establecer y mantener un esquema de clasificación de datos” de CIS Controls v8, que plantea la necesidad de mantener esquemas de categorización documentados, revisados periódicamente y vinculados a políticas de acceso, retención y destrucción segura de datos.

La adopción de este enfoque no solo mejora la capacidad de segmentar y proteger los activos de información, sino que también refuerza la trazabilidad y transparencia en el tratamiento de los datos, condiciones esenciales para mantener la coherencia del SGSI y facilitar la auditoría de cumplimiento. Asimismo, proporciona una base operativa concreta para aplicar controles diferenciados como autenticación reforzada, encriptación, segregación lógica o etiquetado según la naturaleza, criticidad y condiciones de adquisición de cada conjunto de datos.

Esta clasificación, al integrarse con los procesos de evaluación de riesgos, control de accesos y políticas de uso aceptable, fortalece la capacidad de respuesta de la organización ante incidentes relacionados con exposición indebida, manipulación no autorizada o uso inadecuado de la información, especialmente en contextos donde confluyen datos de diversa procedencia tecnológica, regulatoria y científica.

Tabla 5

Evaluación de criticidad y sensibilidad de los datos

Categoría de Datos	Tipo de Dato	Criticidad	Sensibilidad	Controles Implementados	Impacto Potencial	Normativas y Marcos Relacionados
Datos Climáticos	Temperatura, precipitación, humedad, vientos, presión atmosférica	Alta	Media	Cifrado en tránsito y reposo, acceso restringido, redundancia en almacenamiento	Afectación a estudios de cambio climático y predicción meteorológica	**ISO 27001 8.2** (Evaluación de riesgos de seguridad de la información), **ISO 31000 6.4** (Evaluación de riesgos), **NIST SP 800-53 RA-2** (Categorización de Seguridad), **MAGERIT -** Libro I 3.2.2. Tarea MAR.2: Caracterización de las amenazas
Datos de Biodiversidad	Registros de especies, distribución geográfica, ecosistemas, hábitats	Muy Alta	Alta	Cifrado avanzado, acceso restringido, controles de integridad de datos	Riesgo de explotación de ecosistemas y especies protegidas	**ISO 27001 5.15** (Control de Acceso), **ISO 27002 6.6** (Acuerdos de confidencialidad o no divulgación), **NIST SP 800-53 SC-12** (Establecimiento y Gestión de Claves Criptográficas), **MAGERIT - Libro I** 3.2.2. Tarea MAR.2: Caracterización de las amenazas
Datos Hidrológicos	Calidad del agua, niveles de ríos, contaminantes, turbidez, pH	Alta	Media	Control de acceso basado en roles (RBAC), monitoreo continuo, trazabilidad de modificaciones	Impacto en la gestión de recursos hídricos y salud pública	**ISO 27005 7.3** (Análisis de los riesgos de seguridad de la información), **ISO 31000 5.4.3 (**Asignación de roles), **COBIT 2019 - APO12** (Gestión del Riesgo)
Datos Geoespaciales	Uso del suelo, cambios en cobertura terrestre, cartografía digital	Muy Alto	Alta	Cifrado extremo a extremo, autenticación multifactor (MFA), monitoreo de accesos	Posible impacto en ordenamiento territorial y planificación ambiental	**ISO 27001 7.4** (Comunicaciones), **MAGERIT - Libro I** 3.2.2. Tarea MAR.2: Caracterización de las amenazas, **ISO 55002 4.4** (Sistema de gestión de activos), **TOGAF 10 – 5.4 Fase C** (Arquitecturas de sistemas de información)

Categoría de Datos	Tipo de Dato	Criticidad	Sensibilidad	Controles Implementados	Impacto Potencial	Normativas y Marcos Relacionados
Datos de Sensores Remotos	Imágenes satelitales, drones, sensores IoT	Muy Alto	Muy Alto	Segmentación de red, monitoreo en tiempo real, autenticación de dispositivos	Riesgo de manipulación de datos y acceso no autorizado a información sensible	**ISO 27001 7.4** (Comunicaciones), NIST SP 800-53 Rev. 5, SC-7 (Protección de límites), incluyendo controles específicos como SC-7(3) (ACCESS POINTS) y SC-7(5) (Denegar por Defecto Permitir por Excepción)., **CIS Controls v8 13** (Monitoreo y Defensa de la red), **COBIT 2019 - DSS05** (Gestionar los servicios de seguridad)
Datos Socioambientales	Indicadores de impacto humano, sostenibilidad, participación comunitaria	Media	Alta	Anonimización de datos, cifrado de extremo a extremo, auditorías regulares	Posible vulneración de privacidad de comunidades y grupos de estudio	**ISO 27002 (**Control 5.34: Privacidad y protección de datos de carácter personal), **ISO 31000 6.2** (Comunicación y consulta), **NIST SP 800-53 PM-28** (Enmarcado de Riesgos), **TOGAF 10 - Fase B** (Arquitectura empresarial)

Fuente: Elaboración Propia

Consideraciones Adicionales:

- La clasificación de criticidad y sensibilidad se basa en el impacto ambiental y social de los datos.
- Se recomienda implementar auditorías y revisiones periódicas para asegurar el cumplimiento de controles de seguridad.
    - La alineación con normativas internacionales fortalece la gestión de datos en proyectos medioambientales.

La Tabla presenta un esquema de evaluación diseñado para clasificar los datos utilizados en los proyectos de investigación medioambientales, considerando su criticidad operativa y su sensibilidad frente a posibles incidentes de seguridad. Esta clasificación permite identificar qué tipo de protección requiere cada conjunto de datos, priorizando los controles en función del impacto que generaría su pérdida, alteración o divulgación no autorizada.

El análisis se estructura en torno a dos variables complementarias:

- Criticidad: refleja el nivel de afectación que produciría un incidente sobre los objetivos, la continuidad operativa o el cumplimiento normativo del proyecto.
- Sensibilidad: se relaciona con el riesgo de exposición indebida de los datos, considerando su contenido, nivel de confidencialidad, contexto de uso y obligaciones legales asociadas.

Esta evaluación se encuentra respaldada por la ISO/IEC 27005:2022 – Sección 6.4.3 Criterios para realizar evaluaciones de riesgos de seguridad, que establece la importancia de considerar el valor de los activos, su funcionalidad, relaciones de dependencia y exposición al riesgo como parte del proceso de análisis. A su vez, se articula con lo dispuesto en la ISO 31000:2018 – Sección 6.4.3 “Análisis de riesgos”, donde se plantea que el riesgo debe ser analizado considerando tanto la magnitud de las consecuencias como la probabilidad de ocurrencia, aplicando criterios definidos por la organización.

La Tabla 5 agrupa los principales conjuntos de datos evaluados, clasificándolos según su nivel de criticidad y sensibilidad, y sugiriendo controles coherentes con sus características:

- Climáticos: incluyen registros de temperatura, humedad y precipitación. Se valoran con criticidad alta y sensibilidad media. La protección sugerida incorpora cifrado en reposo, respaldo periódico y control de accesos, alineada con la Sección 8.13 “Copias de seguridad de la información” ISO/IEC 27002:2022 y los controles SC-28 (Protección de la información en reposo) y AC-3 (Cumplimiento de Acceso) de la NIST SP 800-53 Rev. 5.
- Biodiversidad: abarca información sobre especies y ecosistemas. Evaluados con criticidad y sensibilidad muy altas, requieren medidas como cifrado robusto, autenticación multifactor y trazabilidad de accesos. Estas prácticas se corresponden con la ISO/IEC

27002:2022 – Sección 5.15 “Control de acceso” y el control AC-6 (Privilegio Mínimo) del NIST.

- Hidrológicos: contienen datos sobre calidad de agua, caudales o parámetros fisicoquímicos. Clasificados con criticidad alta y sensibilidad media, requieren controles como asignación de privilegios por rol, monitoreo de cambios y revisión de integridad, respaldados por el control AU-6 (Revisión, análisis y generación de informes de registros de auditoría) del NIST.
- Geoespaciales: incluyen información territorial, cartografía y sistemas de análisis espacial. Con criticidad muy alta y sensibilidad alta, deben ser protegidos mediante cifrado extremo a extremo, autenticación avanzada y segmentación lógica de red. Estas medidas se vinculan con los controles descritos en la ISO/IEC 27002:2022 – Secciones 8.20 “Seguridad de las redes” y 8.22 “Segregación de redes”.
- Sensores remotos: abarcan datos generados por dispositivos IoT, estaciones meteorológicas automatizadas o imágenes satelitales. Se ubican en el nivel más alto de criticidad y sensibilidad, debido a su volumen, frecuencia de recolección y exposición operativa. Se recomienda aplicar autenticación específica por dispositivo, segmentación de red, monitoreo continuo y control de sesiones, conforme a los controles AC-17 (Acceso Remoto) y SI-4 (Monitoreo del Sistema) del NIST, y al proceso DSS05 “Gestionar los Servicios de Seguridad” definido por COBIT 2019.

Esta evaluación sirve como base para articular el análisis posterior de amenazas y vulnerabilidades, presentado en la **Tabla 7**, y para orientar la selección proporcional de controles. De este modo, se refuerza la coherencia entre el tratamiento de datos y la estrategia general de gestión de riesgos del modelo.

5.2.3 *Clasificación Aplicada a Entornos Técnicos Distribuidos*

Con la tipología extendida definida, este apartado organiza los activos según su función en entornos técnicos distribuidos, ajustándose a las particularidades del sector ambiental para facilitar su evaluación y protección. Esta clasificación amplía el desarrollo presentado en 5.2, articulándose de forma operativa con el procedimiento de 5.2.1, y permite priorizar medidas de protección conforme a la sensibilidad, uso y valor estratégico de los activos, aportando continuidad técnica al enfoque metodológico adoptado. Su propósito es establecer una asignación estructurada de categorías que facilite el despliegue de controles proporcionales a las características funcionales y de seguridad de cada activo.

En primer lugar, la metodología de clasificación se basa en los principios de confidencialidad, integridad y disponibilidad, conforme a (5.12 "Clasificación de la información" de ISO/IEC 27002:2022), y utiliza insumos documentados en fases previas, como el inventario actualizado de activos (Anexo A.5.9 " Inventario de información y otros activos asociados" de ISO/IEC 27001:2022) y la valoración de uso, criticidad y sensibilidad registrada en 5.2.1. Los activos críticos incluyen registros de calidad del agua (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"), cuya confidencialidad es prioritaria para evitar usos indebidos que comprometan decisiones ambientales, y registros de emisiones contaminantes, que deben garantizar integridad para cumplir con (Ley 1712 de 2014, Artículo 3 "Principios").

Seguidamente, los activos estratégicos abarcan plataformas de datos abiertos (Apartado 2.3.3.6 "Repositorios de datos abiertos"), que necesitan disponibilidad para compartir información científica, pero enfrentan riesgos de accesos no autorizados, y sistemas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático"), cuya confidencialidad es prioritaria debido a la sensibilidad de las proyecciones, mientras que su disponibilidad asegura la continuidad de predicciones. Esta clasificación utiliza matrices adaptadas, conforme a (Sección 3.2.1 "Tarea MAR.1: Caracterización de los activos" de MAGERIT v3 Libro I), para asignar niveles según su exposición y contribución a los objetivos del proyecto.

A continuación, los activos de soporte incluyen redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas"), que priorizan disponibilidad para operar en áreas remotas, y dispositivos móviles de campo (Apartado 2.3.3.3 "Dispositivos móviles de

campo"), que requieren integridad para evitar manipulaciones. En entornos distribuidos, esta clasificación dimensiona la exposición, permitiendo controles específicos como cifrado o restricciones de acceso, y delimita responsabilidades asignando roles formales, conforme a (APO08 " Gestionar las Relaciones " de COBIT 2019), como investigadores principales para datos y administradores para equipos.

Por lo tanto, esta clasificación organiza los activos de 5.2.1 y 5.2.2, proporcionando una base estructurada para evaluar su criticidad (5.2.4), definir estrategias de defensa (5.2.5), y facilitar la identificación de amenazas (5.3), contribuyendo al objetivo general.

5.2.4 *Criticidad y Sensibilidad para Activos*

Basándose en la clasificación funcional de, este apartado evalúa la criticidad y sensibilidad de los activos identificados, con el propósito de priorizar aquellos que requieren mayor protección según su contribución a los objetivos del proyecto y su exposición a riesgos. Esta evaluación se fundamenta en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona criterios para determinar su importancia, y en (5.12 "Clasificación de la información" de ISO/IEC 27002:2022), que orienta la valoración según su sensibilidad.

En primer lugar, los activos críticos, como los registros de calidad del agua (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"), se identifican como de alta criticidad debido a su impacto directo en la conservación ambiental. La pérdida o manipulación de estos datos podría derivar en decisiones inadecuadas sobre la gestión de recursos hídricos, afectando comunidades locales y ecosistemas. Su sensibilidad también es elevada, ya que su exposición a usos indebidos podría comprometer la confidencialidad, lo que requiere medidas específicas como cifrado y restricciones de acceso.

Seguidamente, los activos estratégicos, como los sistemas de modelado climático (Apartado 2.3.3.2 "Sistemas de modelado climático"), presentan alta criticidad por su rol en la predicción de tendencias ambientales, siendo su disponibilidad un factor determinante para la continuidad operativa. Al mismo tiempo, su sensibilidad se deriva de la naturaleza estratégica de las proyecciones, que podrían ser blanco de accesos no autorizados si no se protegen adecuadamente. Esto se complementa con plataformas de datos abiertos (Apartado 2.3.3.6

"Repositorios de datos abiertos"), cuya sensibilidad radica en el riesgo de divulgación no controlada de información científica, lo que demanda controles como segmentación de red.

A continuación, los activos de soporte, como las redes satelitales (Apartado 2.3.3.4 "Redes satelitales y de transmisión de datos en áreas remotas"), se evalúan como de criticidad moderada, ya que su función es habilitar operaciones técnicas, pero su indisponibilidad puede interrumpir la transmisión de datos. Su sensibilidad es menor, aunque sigue siendo relevante debido a posibles manipulaciones externas. Dispositivos móviles de campo (Apartado 2.3.3.3 "Dispositivos móviles de campo") también se incluyen aquí, con sensibilidad derivada de su exposición a robos físicos, lo que afecta la integridad de los datos recolectados.

Por lo tanto, esta evaluación permite priorizar los activos para la definición de estrategias de defensa en profundidad (5.2.5) y el análisis de riesgos (5.3), asegurando que las medidas de protección sean proporcionales a su criticidad y sensibilidad.

5.2.4.1 Fórmula De Cálculo De Prioridad.

La fórmula de cálculo de prioridad se estructura como una combinación ponderada, fue elaborada como una propuesta personalizada para este modelo, Fue diseñada para: Convertir tres variables ordinales (valor estratégico, nivel de riesgo, dependencia operativa) en una escala de priorización continua (%).

- Convertir tres variables ordinales (valor estratégico, nivel de riesgo, dependencia operativa) en una escala de priorización continua (%).
- Aumentar el peso del riesgo inherente mediante el factor de ponderación ×1.5 (una decisión técnica fundamentada en priorización práctica).

$$\boldsymbol{Prioridad = \frac{(V_E + (R\ X\ 1.5) + D_O)}{Max_Score} X\ 100}$$

Donde:

La fórmula presentada constituye un modelo de priorización ad-hoc, inspirado en los principios de Análisis de Decisión Multicriterio (MCDA) (6sigma.us., 2024), y diseñado específicamente para reflejar las particularidades de los proyectos de investigación

medioambiental. En este contexto, el riesgo inherente (R) no solo tiene implicaciones operativas, sino que puede afectar directamente la validez de los resultados científicos y los objetivos de conservación, representando la variable de mayor impacto potencial. Por esta razón, se ha introducido un coeficiente de ponderación estratégico de 1.5, que otorga un mayor peso a esta variable. Esta adaptación, que prioriza el riesgo sobre otros factores, se alinea con los principios de la norma ISO 31000:2018, que promueve una gestión de riesgos "adaptada" al contexto de la organización y "transparente" en su metodología.

- Donde:
- VE = Valor Estratégico (1–5)
- R = Riesgo (convertido a escala: Bajo=1, Medio=2, Alto=3, Crítico=4)
- DO = Dependencia Operativa (1–5)
- Max_Score = puntuación máxima posible (5 + 6 + 5 = 16)

Priorización de Recursos por Características

Activo (Capa)	Característica Convergente	Valor Estratégico (1-5)	Riesgo (Bajo/Medio/ Alto/Crítico)	Dependencia Operativa (1-5)	Prioridad de Recursos
Estaciones meteorológicas	Infraestructura	4	Alto	5	Alta (84.38 %)
Bases de datos científicas	Uso	5	Crítico	4	Muy Alta (93.75 %)
Servidores	Funcionalidad	3	Medio	3	Media (56.25 %)
Sensores de campo	Infraestructura	3	Alto	4	Alta (71.88 %)
Aplicaciones científicas	Uso	4	Medio	3	Media-Alta (62.5 %)

Fuente: Elaboración Propia

La priorización de recursos según las características de los activos establece un enfoque estructurado para asignar recursos de manera eficiente, considerando las propiedades específicas

de cada activo protegido dentro del modelo. Este proceso se basa en tres criterios metodológicos bien definidos: el valor estratégico del activo, que refleja su relevancia para los objetivos del proyecto; el nivel de riesgo inherente, que mide su exposición a amenazas; y el grado de dependencia operativa, que evalúa su interconexión con otros elementos del sistema.

El propósito de esta priorización es proporcionar una guía clara y verificable para la asignación de recursos, asegurando que las medidas de seguridad se ajusten a la importancia y exposición de cada activo en el entorno operativo de los proyectos de investigación ambiental. De esta manera, se optimiza la protección de los activos en función de su impacto potencial y sus necesidades específicas.

La metodología empleada asigna puntuaciones cuantitativas a cada criterio de análisis, permitiendo determinar, mediante una combinación ponderada, el porcentaje estimado para la asignación de recursos. Este enfoque no solo facilita la planificación inicial, sino que también permite revisar y ajustar las decisiones de manera sistemática, ofreciendo una base técnica sólida para su validación y mejora continua.

5.2.4.2 Activos de Información Documental.

Partiendo de la evaluación de criticidad y sensibilidad realizada, este apartado analiza los activos de información documental dentro del contexto de los proyectos de investigación medioambiental, con el propósito de determinar su nivel de exposición y las medidas de protección necesarias. La evaluación se fundamenta en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que establece criterios para medir la importancia de los activos, y en (5.12 "Clasificación de la información" de ISO/IEC 27002:2022), que orienta la valoración según su sensibilidad.

Los datos ambientales abarcan registros específicos como los datos hidrológicos y de biodiversidad (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"), que presentan alta criticidad debido a su relevancia para la conservación ambiental. Su pérdida o manipulación podría derivar en decisiones inadecuadas, como la gestión ineficaz de recursos hídricos o la falta de protección de especies en peligro, afectando ecosistemas y comunidades locales. Su sensibilidad es notable, ya que un acceso no autorizado podría facilitar actividades

ilegales, como la caza furtiva, o comprometer información estratégica, lo que requiere medidas como cifrado y controles estrictos de acceso.

Además, los registros de calidad del aire y emisiones contaminantes se identifican como datos ambientales críticos, ya que su integridad es necesaria para cumplir con normativas específicas identificadas en (Apartado 2.7.2 "Leyes"). En particular, la Ley 1712 de 2014, Artículo 3 "Principios", establece principios de transparencia, acceso a la información pública y rendición de cuentas, exigiendo que estos registros sean accesibles al público mientras se garantiza su exactitud para evitar sanciones legales o pérdida de confianza pública. Una alteración en estos datos podría generar reportes imprecisos, incumpliendo también el Decreto 1031 de 2007 (Apartado 2.7.3 "Decretos"), que regula la gestión de calidad del aire y establece parámetros específicos para el monitoreo y reporte de emisiones, lo que demanda mecanismos de protección como auditorías periódicas y copias de seguridad seguras.

Los datos de modelado climático, generados por sistemas como los descritos en (Apartado 2.3.3.2 "Sistemas de modelado climático"), presentan alta criticidad por su rol en la predicción de tendencias ambientales, siendo su disponibilidad un factor determinante para la continuidad operativa. Su sensibilidad surge de su carácter estratégico, ya que las proyecciones podrían ser blanco de accesos no autorizados, afectando la planificación ambiental a largo plazo. Esto se alinea con la Resolución 0549 de 2015 (Apartado 2.7.4 "Resoluciones y Otras Normativas"), que regula la gestión de datos climáticos y exige su protección para garantizar su uso en políticas públicas, requiriendo medidas como segmentación de red y autenticación robusta.

Esta evaluación de los datos ambientales permite priorizar medidas de protección según su criticidad y sensibilidad, preparando el terreno para la definición de estrategias de defensa en profundidad (5.2.5) y el análisis de riesgos (5.3).

5.2.4.3 Datos Ambientales.

Con base en la evaluación de criticidad y sensibilidad, este apartado examina los datos ambientales recolectados o generados por las actividades de investigación medioambiental, con el propósito de determinar su nivel de exposición y las medidas de protección necesarias para garantizar su integridad, confidencialidad y disponibilidad. La evaluación se fundamenta en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que

proporciona un marco detallado para medir la importancia de los activos en función de su impacto en los objetivos del proyecto y su exposición a riesgos específicos. También se apoya en (5.12 "Clasificación de la información" de ISO/IEC 27002:2022), que ofrece directrices claras para valorar los datos según su sensibilidad, considerando factores como el potencial de uso indebido y las implicaciones legales de su exposición, lo que resulta particularmente relevante para datos ambientales que deben cumplir con normativas estrictas.

Los datos ambientales incluyen series de datos meteorológicos, hidrológicos o edafológicos, datos geoespaciales (SIG, GPS, teledetección), imágenes satelitales o multiespectrales, resultados de modelación climática o ecológica, y bases de datos de biodiversidad (flora y fauna) (Apartado 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"). Estos datos presentan alta criticidad debido a su relevancia para la conservación ambiental y la toma de decisiones estratégicas en proyectos de investigación. Por ejemplo, las bases de datos de biodiversidad son esenciales para identificar y proteger especies en peligro, como aquellas amenazadas por la deforestación o el cambio climático, pero su exposición a accesos no autorizados podría facilitar actividades ilegales, como la caza furtiva o el comercio ilegal de especies, lo que podría tener un impacto devastador en ecosistemas frágiles. También, los datos hidrológicos son cruciales para la gestión de recursos hídricos en regiones vulnerables a la sequía, y su manipulación podría derivar en asignaciones ineficientes de agua, afectando comunidades agrícolas y ecosistemas acuáticos. Esto requiere medidas robustas como cifrado avanzado, controles estrictos de acceso basados en roles, y auditorías regulares para garantizar que solo el personal autorizado pueda interactuar con estos datos.

Además, los datos de modelación climática, generados por sistemas como los descritos en (Apartado 2.3.3.2 "Sistemas de modelado climático"), tienen alta criticidad por su rol en la predicción de tendencias ambientales a largo plazo, siendo su disponibilidad un factor determinante para la continuidad operativa de los proyectos que dependen de estas proyecciones para planificar estrategias de mitigación del cambio climático. Su sensibilidad surge de su carácter estratégico, ya que las proyecciones contienen información que podría ser utilizada por terceros para fines competitivos o para influir en políticas públicas de manera indebida, afectando la planificación ambiental a nivel regional o global. Por ejemplo, un acceso no autorizado a estos datos podría permitir la manipulación de predicciones climáticas, lo que podría influir en

decisiones gubernamentales sobre la asignación de recursos para la adaptación al cambio climático. Esto demanda medidas como segmentación de red para aislar los datos críticos, autenticación robusta para verificar la identidad de los usuarios, y monitoreo continuo para detectar actividades sospechosas.

La evaluación realizada permite priorizar medidas de protección según la criticidad y sensibilidad de los datos ambientales, sentando las bases para las estrategias de defensa en profundidad (5.2.5) y el análisis de riesgos (5.3) dentro del ciclo PHVA, asegurando que los datos sean protegidos de manera proporcional a su importancia y exposición.

5.2.4.4 Software y Herramientas Analíticas.

Este apartado analiza el software y las herramientas analíticas utilizadas para procesar y visualizar información en los proyectos de investigación medioambiental, con el objetivo de determinar su nivel de exposición a riesgos y las medidas de protección necesarias para garantizar su operatividad y seguridad. La evaluación se apoya en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un marco estructurado para medir la importancia de las herramientas en función de su impacto en los objetivos del proyecto, como la capacidad de analizar datos ambientales complejos. También se basa en (5.13 "Etiquetado de la información" de ISO/IEC 27002:2022), que establece directrices para gestionar herramientas analíticas según su uso y sensibilidad, considerando aspectos como el tipo de datos que procesan y las implicaciones de su exposición a accesos no autorizados o manipulaciones.

El software y las herramientas analíticas incluyen sistemas GIS (QGIS, ArcGIS), software estadístico (R, Python, SPSS), herramientas de simulación o modelado, algoritmos de predicción y código fuente propio, y aplicaciones de monitoreo ambiental en tiempo real (Apartado 2.3.3 "Infraestructura tecnológica en proyectos de investigación"). Estas herramientas presentan alta criticidad, ya que su indisponibilidad puede interrumpir el análisis de datos ambientales, afectando la continuidad de las investigaciones y la capacidad de generar resultados precisos para la toma de decisiones. Por ejemplo, los sistemas GIS son esenciales para mapear datos geoespaciales que identifican áreas vulnerables a la deforestación o inundaciones, y una falla en estas herramientas podría retrasar la implementación de medidas de mitigación, afectando ecosistemas y comunidades locales. Su sensibilidad es significativa, ya que el código fuente propio, como algoritmos de

predicción personalizados, podría ser blanco de accesos no autorizados, comprometiendo la propiedad intelectual del proyecto o permitiendo su uso indebido por terceros para obtener ventajas competitivas. Esto requiere medidas como controles de acceso basados en roles, copias de seguridad seguras en servidores protegidos, y revisiones periódicas de seguridad para detectar vulnerabilidades en el software.

Además, las aplicaciones de monitoreo en tiempo real tienen alta criticidad debido a su rol en la generación de alertas inmediatas sobre condiciones ambientales, como cambios repentinos en la calidad del aire o niveles de agua, siendo su disponibilidad un factor clave para responder a emergencias ambientales. Su sensibilidad surge del riesgo de manipulación, ya que una alteración en estas aplicaciones podría generar datos falsos, lo que podría llevar a decisiones erróneas, como ignorar una alerta de contaminación o sobreestimar riesgos inexistentes, afectando la confianza pública y la eficacia de las intervenciones. Esto demanda medidas específicas como autenticación robusta para garantizar que solo usuarios autorizados accedan a las aplicaciones, auditorías periódicas para verificar la integridad de los datos generados, y sistemas de detección de intrusos para identificar intentos de manipulación.

La evaluación realizada establece un punto de partida para definir estrategias de defensa en profundidad (5.2.5) y analizar riesgos (5.3), integrándose con el ciclo PHVA para garantizar la seguridad de estas herramientas y su contribución al proyecto.

5.2.4.5 Equipamiento Tecnológico.

Con base en la evaluación de 5.2.4, este apartado analiza el equipamiento tecnológico utilizado para capturar o procesar datos en los proyectos de investigación medioambiental, con el objetivo de determinar su nivel de exposición a riesgos y las medidas de protección necesarias para garantizar su operatividad y seguridad. La evaluación se apoya en (Sección 4 "Criterios de valoración " de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un marco estructurado para medir la importancia de los equipos en función de su impacto en los objetivos del proyecto, como la capacidad de recolectar datos precisos en tiempo real. También se basa en (7.9 "Seguridad de los equipos fuera de las instalaciones" de ISO/IEC 27002:2022), que establece directrices para proteger equipos tecnológicos durante su uso, considerando riesgos como el acceso no autorizado, el daño físico o la manipulación de datos.

El equipamiento tecnológico incluye estaciones meteorológicas automáticas, UAVs y drones para levantamiento topográfico, sensores de calidad de agua, aire o suelo, servidores locales o de borde, y computadoras de alto rendimiento (Apartado 2.3.3 "Infraestructura tecnológica en proyectos de investigación"). Estos equipos presentan alta criticidad, ya que su indisponibilidad puede interrumpir la recolección y procesamiento de datos, afectando la continuidad de las investigaciones y la capacidad de responder a emergencias ambientales. Por ejemplo, las estaciones meteorológicas automáticas son esenciales para monitorear condiciones climáticas en tiempo real, como tormentas o sequías, y su falla podría retrasar alertas críticas, poniendo en riesgo comunidades y ecosistemas. Su sensibilidad es relevante, ya que los sensores de calidad del agua pueden ser manipulados para generar datos falsos, lo que podría llevar a decisiones erróneas sobre la potabilidad del agua o la salud de ecosistemas acuáticos, afectando la confianza pública y generando impactos sociales. Esto requiere medidas como controles físicos de acceso para evitar manipulaciones, monitoreo continuo de la integridad de los datos recolectados, y mantenimiento preventivo para garantizar su funcionamiento.

Además, los servidores locales y de borde tienen alta criticidad por su rol en el almacenamiento y procesamiento de datos, siendo su disponibilidad un factor clave para garantizar que los datos ambientales estén accesibles para su análisis en tiempo real. Su sensibilidad surge del riesgo de accesos no autorizados, ya que un servidor comprometido podría exponer datos sensibles, como imágenes satelitales o resultados de modelación, a terceros no autorizados, lo que podría derivar en su uso indebido, como la explotación de recursos naturales en áreas protegidas. Esto demanda medidas específicas como segmentación de red para aislar los datos críticos, cifrado de extremo a extremo para proteger la información durante su transmisión, y sistemas de detección de intrusos para identificar actividades sospechosas en tiempo real.

La evaluación realizada establece prioridades para las estrategias de defensa en profundidad (5.2.5) y el análisis de riesgos (5.3), alineándose con el ciclo PHVA para proteger estos equipos tecnológicos y asegurar su contribución al proyecto.

5.2.4.6 Servicios de Información.

Este apartado examina los servicios de información que soportan la operación de los proyectos de investigación medioambiental, con el objetivo de determinar su nivel de exposición

a riesgos y las medidas de protección necesarias para garantizar su operatividad y seguridad. La evaluación se apoya en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un marco estructurado para medir la importancia de los servicios en función de su impacto en los objetivos del proyecto, como facilitar la colaboración entre equipos distribuidos y asegurar el acceso continuo a datos críticos para el análisis ambiental. También se basa en (5.15 "Control de acceso" de ISO/IEC 27002:2022), que establece directrices para gestionar servicios de información según su uso y sensibilidad, considerando riesgos como accesos no autorizados, ataques de phishing y configuraciones inseguras que podrían comprometer la seguridad de los datos y la continuidad operativa del proyecto.

Los servicios de información abarcan plataformas colaborativas (Google Drive, SharePoint), servicios de correo y mensajería, infraestructura cloud para almacenamiento y cálculo, y servicios de backup y recuperación ante desastres (Apartado 2.3.3 "Infraestructura tecnológica en proyectos de investigación"). Estos servicios presentan alta criticidad, ya que su indisponibilidad puede interrumpir la colaboración entre equipos, el intercambio de datos y el acceso a información crítica, afectando significativamente la continuidad operativa del proyecto. Por ejemplo, las plataformas colaborativas son esenciales para compartir resultados de investigación, como mapas geoespaciales o bases de datos de biodiversidad, entre investigadores distribuidos geográficamente, permitiendo una coordinación efectiva en tiempo real para abordar emergencias ambientales, como inundaciones o incendios forestales. Una falla en estos servicios podría retrasar la toma de decisiones críticas, como la implementación de medidas de mitigación en áreas afectadas por desastres naturales, lo que podría agravar el impacto en ecosistemas y comunidades locales. Su sensibilidad es notable, ya que los servicios de correo y mensajería son blancos frecuentes de ataques de phishing, lo que podría derivar en accesos no autorizados a datos ambientales sensibles, como imágenes satelitales o series hidrológicas, comprometiendo la confidencialidad de la información y erosionando la confianza entre los socios del proyecto, incluidos gobiernos y ONGs. Esto requiere la implementación de medidas específicas como autenticación multifactor para verificar la identidad de los usuarios y prevenir accesos no autorizados, filtros antiphishing para detectar y bloquear correos maliciosos, y políticas de uso que limiten el intercambio de datos sensibles a través de estos canales, promoviendo el uso de plataformas seguras para comunicaciones críticas.

Además, la infraestructura Cloud tiene alta criticidad por su rol central en el almacenamiento y procesamiento de datos, siendo su disponibilidad un factor clave para garantizar que los datos ambientales, como proyecciones climáticas o registros de calidad del aire, estén accesibles para su análisis en tiempo real, lo que permite a los investigadores responder rápidamente a cambios ambientales. Su sensibilidad surge del riesgo de accesos no autorizados, ya que un ataque a la nube podría exponer datos críticos, como imágenes satelitales o bases de datos de biodiversidad, lo que podría derivar en su uso indebido, como la explotación de recursos naturales en áreas protegidas o la manipulación de datos para influir en políticas públicas. Por ejemplo, un atacante que acceda a proyecciones climáticas podría utilizarlas para obtener ventajas comerciales, como especular con tierras agrícolas en regiones previstas para ser afectadas por sequías. Esto demanda medidas específicas como cifrado de extremo a extremo para proteger la información durante su almacenamiento y transmisión, segmentación de red para aislar los datos críticos y reducir el alcance de un posible ataque, y sistemas de monitoreo continuo para detectar actividades sospechosas, como intentos de acceso no autorizado, y responder a incidentes de manera oportuna, minimizando el impacto en el proyecto.

La evaluación realizada establece un marco para definir estrategias de defensa en profundidad (5.2.5) y analizar riesgos (5.3), integrándose con el ciclo PHVA para garantizar la seguridad de estos servicios y su contribución al proyecto, permitiendo una gestión efectiva de los datos y la colaboración entre los equipos de investigación.

5.2.4.7 Activos Humanos.

El apartado analiza los activos humanos con acceso, control o responsabilidad sobre los activos del proyecto, con el objetivo de determinar su nivel de exposición a riesgos y las medidas de protección necesarias para garantizar su seguridad y la del proyecto en su conjunto. La evaluación se apoya en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un marco estructurado para medir la importancia de los activos humanos en función de su impacto en los objetivos del proyecto, como la ejecución efectiva de las actividades de investigación y la protección de los datos generados. También se basa en (6 "Gestión de Control de Accesos" de CIS Controls v8), que establece directrices para proteger frente a riesgos

humanos, considerando factores como errores, accesos indebidos y ataques de ingeniería social que podrían comprometer la seguridad de los datos y la continuidad operativa.

Los activos humanos incluyen investigadores principales y coinvestigadores, técnicos de campo y laboratorio, analistas de datos, y personal administrativo asociado. Estos presentan alta criticidad, ya que su participación es esencial para todas las etapas del proyecto, desde la planificación estratégica de la investigación hasta la recolección, análisis y gestión de datos ambientales, asegurando que los resultados sean precisos y útiles para la toma de decisiones. Sin embargo, enfrentan riesgos significativos como errores humanos, accesos indebidos, phishing e ingeniería social, que podrían comprometer la seguridad de los datos ambientales y la integridad del proyecto. Por ejemplo, un investigador principal podría ser blanco de un ataque de phishing que le lleve a compartir credenciales de acceso, permitiendo a un atacante acceder a bases de datos de biodiversidad o resultados de modelación climática, lo que podría derivar en su uso indebido, como la explotación de recursos naturales en áreas protegidas o la manipulación de datos para influir en políticas públicas, afectando la credibilidad del proyecto y sus socios. Su sensibilidad es notable, ya que un acceso indebido a través de un investigador podría comprometer datos críticos, lo que requiere controles como programas de formación y concienciación para educar al personal sobre buenas prácticas de seguridad, como la identificación de correos sospechosos y la gestión segura de credenciales, autenticación multifactor para verificar la identidad de los usuarios y prevenir accesos no autorizados, y revisiones periódicas de privilegios para garantizar que solo el personal autorizado tenga acceso a los datos, conforme a (14 "Concientización en Seguridad y Formación de Habilidades" de CIS Controls v8), que promueve la capacitación continua para mitigar riesgos humanos.

Además, los técnicos de campo tienen alta criticidad por su rol en la recolección de datos en ubicaciones remotas, como áreas protegidas o regiones de difícil acceso, donde su trabajo es fundamental para obtener información primaria, como series hidrológicas o imágenes satelitales, que sirve de base para los análisis posteriores. Su exposición a ingeniería social puede facilitar accesos no autorizados, como la entrega de dispositivos o credenciales a terceros malintencionados que se hagan pasar por personal autorizado, lo que podría derivar en la pérdida de datos recolectados, afectando la continuidad de la investigación y la precisión de los análisis posteriores. Por ejemplo, un técnico podría ser engañado para entregar un dispositivo USB con datos de

biodiversidad a un falso inspector, lo que podría resultar en el uso indebido de esa información para actividades ilegales, como la caza furtiva. Esto demanda medidas específicas como talleres de sensibilización para entrenar a los técnicos en la identificación de tácticas de ingeniería social, como pretextos o suplantación de identidad, políticas de acceso estrictas que limiten la entrega de información a personal verificado mediante procedimientos de autenticación, y el uso de dispositivos seguros con bloqueos físicos, como candados o sistemas de rastreo, para evitar accesos indebidos y rastrear los dispositivos en caso de pérdida.

La evaluación realizada permite definir estrategias de defensa en profundidad (5.2.5) y analizar riesgos (5.3), integrándose con el ciclo PHVA para garantizar la seguridad de estos activos humanos y su contribución al proyecto, asegurando que el personal esté preparado para manejar riesgos y proteger los datos del proyecto.

5.2.4.8 Normativos y Contractuales.

Este apartado analiza los activos normativos y contractuales que establecen marcos legales o compromisos en los proyectos de investigación medioambiental, con el objetivo de determinar su nivel de exposición a riesgos y las medidas de protección necesarias para garantizar su cumplimiento y seguridad. La evaluación se apoya en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un marco estructurado para medir la importancia de estos activos en función de su impacto en los objetivos del proyecto, como el cumplimiento de obligaciones legales y contractuales que aseguran la legitimidad y continuidad de las actividades de investigación. También se basa en (5.31 "Identificación de requisitos legales, reglamentarios y contractuales" de ISO/IEC 27002:2022), que establece directrices para identificar y gestionar los requisitos legales, reglamentarios y contractuales aplicables, considerando riesgos como el incumplimiento de normativas, la exposición de contratos a accesos no autorizados, y la falta de seguimiento que podría derivar en sanciones legales o pérdida de confianza con socios, lo que es fundamental para garantizar que el proyecto opere dentro de los marcos legales y éticos requeridos.

Los activos normativos y contractuales incluyen convenios con entidades externas (universidades, ONGs), contratos de confidencialidad y cesión de datos, normativa ambiental (local e internacional), y protocolos éticos y autorizaciones para recolección (Apartado 2.7

"Normativa"). Estos activos presentan alta criticidad, ya que su incumplimiento puede derivar en sanciones legales, pérdida de confianza con socios, o interrupciones en el proyecto, afectando su continuidad y credibilidad. Por ejemplo, un convenio con una universidad que regula el intercambio de datos geoespaciales para mapear áreas vulnerables a la deforestación podría ser violado si los datos se exponen a terceros no autorizados debido a una brecha de seguridad, lo que podría derivar en disputas legales, la suspensión de colaboraciones clave, y el retraso en la implementación de medidas de conservación, afectando tanto al proyecto como a las comunidades locales dependientes de esos ecosistemas para su subsistencia, como comunidades indígenas que dependen de los recursos forestales. Su sensibilidad es notable, ya que los contratos de confidencialidad podrían ser blanco de accesos no autorizados, comprometiendo datos sensibles como bases de datos de biodiversidad o resultados de modelación climática, lo que podría derivar en su uso indebido para fines comerciales o ilegales, como la explotación de recursos naturales o la venta de datos a competidores, lo que podría socavar los esfuerzos de conservación y exponer al proyecto a riesgos legales y reputacionales. Esto requiere medidas como cifrado de extremo a extremo para proteger la información durante su almacenamiento y transmisión, controles de acceso basados en roles para limitar el acceso a personal autorizado, como los responsables legales y de investigación, y auditorías regulares para garantizar el cumplimiento de las cláusulas contractuales y detectar cualquier incumplimiento de manera oportuna, asegurando que las obligaciones legales y contractuales se mantengan a lo largo del proyecto.

Además, los protocolos éticos y autorizaciones para recolección tienen alta criticidad por su rol en garantizar la legitimidad de las actividades de investigación, como la recolección de datos de fauna en áreas protegidas, que debe cumplir con normativas internacionales como el Convenio sobre la Diversidad Biológica, que exige permisos específicos para operar en ecosistemas sensibles y proteger la biodiversidad global. Su exposición a manipulaciones, como la alteración de autorizaciones para justificar actividades no permitidas, podría derivar en violaciones éticas y sanciones legales, afectando la reputación del proyecto y su capacidad para operar en áreas protegidas, lo que podría retrasar investigaciones clave y limitar el acceso a fondos futuros. Por ejemplo, una autorización manipulada podría permitir la recolección de muestras en un área restringida sin el consentimiento de las autoridades locales, lo que podría derivar en multas, la prohibición de futuras investigaciones en esa región, y la pérdida de confianza de comunidades

locales y socios internacionales, afectando los objetivos a largo plazo del proyecto, como la conservación de especies en peligro. Esto demanda medidas específicas como auditorías internas para verificar el cumplimiento de los protocolos éticos mediante revisiones periódicas de los permisos y su alineación con las normativas aplicables, almacenamiento seguro de las autorizaciones en servidores protegidos con acceso restringido a personal autorizado, y capacitación del personal para garantizar que las actividades de recolección se realicen dentro de los límites establecidos, promoviendo una cultura de ética y cumplimiento en el equipo que refuerce la legitimidad del proyecto.

La evaluación realizada establece un marco para definir estrategias de defensa en profundidad (5.2.5) y analizar riesgos (5.3), integrándose con el ciclo PHVA para garantizar el cumplimiento y la seguridad de estos activos normativos y contractuales, asegurando que el proyecto opere dentro de los marcos legales y éticos requeridos y mantenga la confianza de sus socios y partes interesadas.

5.2.4.9 Soportes Físicos y Materiales.

apartado examina los soportes físicos y materiales utilizados para el almacenamiento o transporte de información en los proyectos de investigación medioambiental, con el propósito de determinar su nivel de exposición a riesgos y las medidas de protección necesarias para garantizar su seguridad y disponibilidad. La evaluación se apoya en (Sección 4 "Criterios de valoración" de MAGERIT v3 Libro II: Catálogo de Elementos), que proporciona un marco estructurado para medir la relevancia de estos soportes según su impacto en los objetivos del proyecto, como la preservación de datos esenciales para la continuidad de la investigación y la toma de decisiones en la gestión ambiental. Además, se fundamenta en (7.10 "Soportes de almacenamiento" de ISO/IEC 27002:2022), que establece directrices para proteger soportes físicos de almacenamiento, considerando riesgos como el robo, la pérdida o el daño físico que podrían comprometer la información almacenada, lo que resulta especialmente relevante para soportes utilizados en entornos de campo expuestos a condiciones adversas, como lluvias intensas, altas temperaturas o terrenos accidentados.

Los soportes físicos y materiales abarcan discos duros, USB, tarjetas SD, CDs, cuadernos de campo, formularios en papel, mapas impresos y cartografías de trabajo (Apartado 2.3.3

"Infraestructura tecnológica en proyectos de investigación"). Estos soportes presentan alta criticidad, ya que su pérdida o daño puede interrumpir el acceso a datos esenciales, como series hidrológicas, imágenes satelitales o registros de biodiversidad, afectando la continuidad operativa del proyecto y la capacidad de realizar análisis posteriores que informen decisiones ambientales cruciales. Por ejemplo, un disco duro que contiene datos geoespaciales recolectados durante años podría ser dañado por condiciones ambientales adversas, como inundaciones o altas temperaturas en un área de trabajo remota, lo que podría derivar en la pérdida de información irreemplazable necesaria para la planificación de medidas de mitigación, como la reforestación de áreas deforestadas o la protección de cuencas hídricas críticas para comunidades locales que dependen de estos recursos para su subsistencia, como agricultores o pescadores. Su sensibilidad es significativa, ya que un USB con datos ambientales podría ser robado durante el trabajo de campo, comprometiendo su confidencialidad y pudiendo derivar en su uso indebido, como la explotación ilegal de recursos naturales en áreas protegidas o la venta de datos a terceros para fines comerciales, lo que podría socavar los esfuerzos de conservación y exponer al proyecto a riesgos legales y éticos. Esto requiere medidas como el almacenamiento seguro en instalaciones cerradas con acceso controlado para evitar manipulaciones no autorizadas, el cifrado de los datos para proteger la información incluso si el dispositivo es robado, y la realización de copias de seguridad periódicas en almacenamiento en la nube o en soportes físicos secundarios para garantizar la recuperación de datos en caso de pérdida o daño, manteniendo la disponibilidad de información crítica para la investigación.

Además, los cuadernos de campo y formularios en papel tienen alta criticidad por su rol en la recolección inicial de datos, como registros de biodiversidad o observaciones meteorológicas, que constituyen la base para análisis posteriores y decisiones ambientales, como la identificación de especies en peligro o la predicción de eventos climáticos extremos que podrían afectar comunidades vulnerables, como tormentas que impacten áreas costeras. Su exposición a daños físicos, como la pérdida por condiciones climáticas adversas (lluvias intensas, tormentas o altas temperaturas) o el deterioro por el uso prolongado en el campo, puede afectar la trazabilidad de la información, lo que podría derivar en errores en la interpretación de datos y decisiones ambientales imprecisas, como subestimar la población de una especie protegida o ignorar patrones climáticos críticos que podrían prevenir desastres, afectando la seguridad de las comunidades y la

conservación de ecosistemas. Por ejemplo, un cuaderno de campo perdido durante una tormenta podría eliminar registros únicos de avistamientos de fauna, afectando estudios de conservación a largo plazo y la capacidad del proyecto para cumplir con compromisos internacionales, como los establecidos en el Convenio sobre la Diversidad Biológica, lo que podría limitar el acceso a fondos y colaboraciones futuras. Esto demanda medidas específicas como la digitalización de los registros para crear copias electrónicas que puedan ser almacenadas de manera segura en servidores protegidos con acceso restringido, el uso de materiales resistentes al agua y al desgaste para los formularios, como papel sintético o cubiertas impermeables que soporten condiciones extremas, y el almacenamiento seguro de los originales en instalaciones protegidas con controles de temperatura y humedad para preservar su integridad a largo plazo, asegurando que la información permanezca accesible y confiable para su uso en análisis y decisiones futuras.

La evaluación realizada proporciona una base para definir estrategias de defensa en profundidad (5.2.5) y analizar riesgos (5.3), alineándose con el ciclo PHVA para garantizar la seguridad de estos soportes físicos y materiales, así como su rol en mantener la integridad y disponibilidad de los datos del proyecto, apoyando los objetivos de investigación y gestión ambiental.

5.2.5 *Defensa en Profundidad*

Tras completar la identificación y clasificación de activos de información en 5.2.4, este apartado define una estructura de defensa en profundidad para garantizar la protección de los activos mediante múltiples capas de seguridad, ajustadas a su nivel de exposición, criticidad y función dentro del entorno operacional de los proyectos de investigación medioambiental, que abarcan el monitoreo de ecosistemas y la gestión de datos climáticos. Este enfoque busca mitigar riesgos de manera integral, reduciendo la probabilidad de compromisos de seguridad ante amenazas que afectan diversos vectores simultáneamente, como accesos no autorizados, manipulaciones físicas o fallos técnicos, que podrían interrumpir investigaciones críticas o comprometer la conservación de recursos naturales. La estrategia se fundamenta en (Sección 3.1 "Conceptos paso a paso" de MAGERIT v3 Libro I), que proporciona un marco estructurado para el análisis de riesgos mediante pasos sistemáticos que identifican activos, amenazas y riesgos, y en (0.4 "Determinar los controles" de ISO/IEC 27002:2022), que resalta la importancia de

seleccionar controles considerando su interacción para lograr una defensa en profundidad, asegurando una protección robusta frente a amenazas que podrían impactar los objetivos del proyecto, como la gestión sostenible de datos ambientales.

La defensa en profundidad se organiza mediante una arquitectura multinivel que integra recursos físicos, digitales y humanos, diseñada para evitar enfoques genéricos y priorizar controles contextualizados según la naturaleza del activo, su entorno operativo y las relaciones de dependencia técnica, garantizando que las medidas sean proporcionales a la criticidad y exposición de los activos. Las capas se estructuran considerando las amenazas identificadas y los riesgos asociados, protegiendo activos como datos ambientales (5.2.4.2), que enfrentan riesgos de explotación ilegal, y soportes físicos (5.2.4.8), vulnerables a robos en entornos remotos. La capa física emplea controles de acceso mediante cerraduras biométricas en estaciones meteorológicas y sensores LoRaWAN instalados en áreas protegidas, monitoreo de condiciones ambientales como temperatura y humedad para prevenir daños por condiciones extremas, y sistemas de videovigilancia con grabación continua para disuadir robos o manipulaciones. La capa técnica incluye segmentación de redes para aislar datos sensibles, como registros de biodiversidad, cifrado AES-256 para proteger la confidencialidad e integridad durante su almacenamiento y transmisión, autenticación reforzada mediante factores biométricos y tokens físicos, y herramientas de detección de intrusos para identificar accesos anómalos en tiempo real. La capa organizacional establece políticas internas de seguridad que definen roles y responsabilidades, un plan de gestión de incidentes con tiempos de respuesta definidos, y una clasificación detallada de activos para priorizar su protección. La capa de personal implementa programas de concienciación con simulaciones prácticas para capacitar al equipo contra phishing e ingeniería social, gestión de privilegios para limitar accesos según roles, y control de identidades con revisiones periódicas. La capa de gobernanza aplica auditorías periódicas para verificar el cumplimiento normativo, trazabilidad de requisitos legales mediante registros documentales, y mecanismos de supervisión con métricas de desempeño para evaluar la eficacia de los controles.

Esta arquitectura se alinea con AC-5 (Separación de funciones): Divide las tareas y privilegios entre usuarios o roles para evitar conflictos de interés y reducir el riesgo de acciones no autorizadas. Este control establece que ninguna persona debe tener simultáneamente la capacidad de realizar varias funciones críticas sin una separación clara y documentada,

(“Administrar el marco de gestión de TI” de COBIT 2019), que asegura una supervisión estratégica para alinear los controles con los objetivos del proyecto, y (Introducción "Modelo de defensa comunitaria" de CIS Controls v8, 2024), que resalta la efectividad de controles dispuestos en profundidad a lo largo del ciclo de vida de un ataque. La estructura multinivel protege los activos de manera integral, sentando las bases para el análisis de riesgos (5.3) y la implementación de controles (Sección 6 "Hacer (Do): Diseño del Modelo y Definición de Controles"), integrándose con el ciclo PHVA para cumplir los objetivos del proyecto, como la gestión sostenible de recursos y la conservación de ecosistemas.

Figura 9

Defensa en profundidad investigación medioambiental



Adaptación, Defense in Depth. Tomado de “wallarm” [Figura], Mukhadin Beschokov, https://www.wallarm.com/what/defense-in-depth-concept

La Figura ilustra gráficamente la arquitectura multinivel del modelo de seguridad, representando las cinco capas de defensa (física, técnica, organizacional, personal, gobernanza) y mostrando cómo interactúan para proteger los activos mediante controles superpuestos, alineados con los principios de defensa en profundidad. Esta estructura se alinea con las directrices del Modelo de Defensa Comunitaria (CDM) descrito en (Introducción "Modelo de defensa" de CIS Controls v8, 2024), que resalta la efectividad de controles dispuestos en profundidad al proporcionar una base estratégica para defensa en profundidad y analizar el valor de acciones defensivas a lo largo del ciclo de vida de un ataque. La estrategia refuerza lo planteado en el análisis de riesgos, facilitando la correlación entre amenazas y controles, y garantizando que cada activo cuente con mecanismos complementarios de protección ajustados a su criticidad.

Tabla 6

Identificación y Clasificación de Activos por Capa de Defensa

Capa de Defensa	Activo	Clasificación	Controles Implementados	Actividades	Etapas	Normativas y Marcos Relacionados
Políticas, Gobernanza y Concienciación	Normativas, procedimientos, capacitación en seguridad, concienciación sobre amenazas y mejores prácticas.	Confidencial	Desarrollo y revisión periódica, auditorías internas, alineación con estándares internacionales, formación continua en ciberseguridad y cumplimiento normativo.	Creación y actualización de normativas.	Definición de políticas y estrategias de seguridad.	ISO 27001 5.1 (Liderazgo y Compromiso), ISO 31000 5.2 (5.2 Liderazgo y compromiso), COBIT 2019 APO13 (Gestionar la Seguridad).
				Establecimiento de estrategias de gobernanza.	Revisión y actualización periódica.	ISO/IEC 38500 5.2 (Responsabilidades de Gobernanza de TI), Magerit - Libro I 4.2.1 (Roles y Funciones).
Seguridad Física	Estaciones meteorológicas, Sensores ambientales, Infraestructura de recolección de datos	Crítica	Control de acceso con autenticación multifactor, monitoreo mediante CCTV, seguridad perimetral con guardias, sensores de movimiento, control de visitantes.	Protección de infraestructura física.	Implementación de controles de acceso.	ISO 27001 7.4 (Monitoreo de seguridad física), NIST SP 800-53 PE-3 (Control de acceso físico), PE-6 (Supervisión de acceso físico)
				Establecimiento de zonas seguras.	Mantenimiento y auditoría de seguridad.	CIS Controls v8 12 (Gestión de la Infraestructura de Red), Magerit - Libro I 7.2.2 (Contexto).
Seguridad Perimetral	Gateways, Redes de comunicación (LoRa, WiFi, MQTT)	Confidencial	Configuración de firewalls avanzados, segmentación de redes, Zero Trust Network Access (ZTNA), cifrado de datos en tránsito, detección de intrusiones (IDS/IPS), monitoreo de redes en tiempo real.	Monitoreo y análisis de tráfico de red.	Implementación de controles de seguridad perimetral.	ISO 27001 7.4 (Comunicaciones), NIST SP 800-53 Rev. 5, SC-7 (Protección de límites), incluyendo controles específicos como SC-7(3) (Access Points) y SC-7(5) (Denegar por Defecto Permitir por Excepción).
				Gestión de accesos remotos seguros.	Revisión de amenazas externas.	CIS Controls v8 12.6 (Uso de protocolos seguros de administración de redes y comunicaciones), ISO 27005 7.3 (Análisis de los riesgos de seguridad de la información), ISO 31000 6.4 (Evaluación de riesgos).

Capa de Defensa	Activo	Clasificación	Controles Implementados	Actividades	Etapas	Normativas y Marcos Relacionados
Seguridad de Red	Redes locales y conexiones entre estaciones remotas y centrales	Interna	Configuración de segmentación de red, monitoreo y análisis de tráfico, detección de anomalías, Network Access Control (NAC), auditoría de configuración de red.	Implementación de seguridad en la infraestructura de red.	Configuración segura de dispositivos de red.	CIS Controls v8 12 (Gestión de la Infraestructura de Red), NIST SP 800-53 Rev. 5, SC-7 (Protección de límites), incluyendo controles específicos como SC-7(3) (Access Points) y SC-7(5) (Denegar por Defecto Permitir por Excepción).
				Auditoría de configuraciones.	Revisión periódica de seguridad.	ISO 27001 A 8.20 Seguridad en redes), Magerit - Libro I 7.2.2 (Contexto), ISO 31000 6.4 (Evaluación de riesgos).
Seguridad del Host/Endpoint	Servidores de almacenamiento y procesamiento de datos	Confidencial	Gestión de parches y actualizaciones, monitoreo de logs, detección de malware con herramientas avanzadas de EDR/XDR, control de acceso a nivel de dispositivo, auditoría de registros.	Protección de infraestructura TI.	Aplicación de medidas de seguridad en end points.	ISO 27001 A.8.8 (Gestión de Vulnerabilidades técnicas), NIST SP 800-53 SI-2 (Remediación de Defectos).
				Administración de accesos privilegiados.	Monitoreo y auditoría continua.	CIS Controls v8 13 (Monitoreo y Defensa de la red), ISO 31000 5.4.1 (Comprensión de las organizaciones y su contexto), Magerit - Libro I MAR.2 – 3.2.2. Tarea MAR.2: Caracterización de las amenazas
Seguridad de las Aplicaciones	Servidores Backend, Bases de Datos, Modelos de Inteligencia de Negocio (BI), APIs, Aplicaciones web y móviles.	Confidencial	Implementación de principios de desarrollo seguro (DevSecOps), pruebas de penetración periódicas, uso de Web Application Firewalls (WAF), autenticación multifactor.	Seguridad en desarrollo de software, validación de integridad en código fuente, protección de APIs.	Implementación de controles de seguridad en aplicaciones.	ISO 27001 A 8.29 (Pruebas de seguridad en desarrollo y aceptación.), NIST SP 800-53 SA-11 (Pruebas y Evaluación de Desarrolladores), CIS Controls v8 IG2-9 (Seguridad de Aplicaciones).
Seguridad de los Datos	Información de sensores ambientales, registros de	Crítica	Cifrado de datos en tránsito y en reposo (AES-256), prevención de fuga de datos (DLP),	Protección y gestión del ciclo de vida de los datos.	Implementación de controles de acceso y cifrado.	ISO 27001 8.2 (Evaluación de riesgos de seguridad de la información), NIST SP 800-53 SC-12 (Establecimiento y Gestión de Claves Criptográficas).

Capa de Defensa	Activo	Clasificación	Controles Implementados	Actividades	Etapas	Normativas y Marcos Relacionados
	investigación, datos de modelos analíticos, bases de datos geoespaciales, registros de participación comunitaria, informes de impacto ambiental.		control de acceso basado en roles (RBAC), registros de auditoría, trazabilidad de cambios, firma digital.	Implementación de medidas de privacidad y cumplimiento normativo.	Aseguramiento de integridad de la información.	ISO 27002 (Privacidad y protección de datos de carácter persona), Magerit - Libro I MAR.2: 3.2.2. Tarea MAR.2: Caracterización de las amenazas, ISO 31000 5.5 (Implementación), ISO 55002 4.4 (Sistema Gestión de Activos).

Fuente: Elaboración Propia

Esta tabla presenta la clasificación de activos de información relevantes para los proyectos de investigación medioambientales, estructurados según el modelo de defensa en profundidad adoptado. Los activos se agrupan por capa de defensa funcional y se caracterizan según su función, sensibilidad (por ejemplo, Confidencial o Crítica), controles implementados, actividades asociadas y etapa del ciclo de vida en la que intervienen.

La clasificación se fundamenta en los criterios técnicos definidos en el Catálogo de Elementos de MAGERIT v3 – Libro II (Sección 2, Tipos de activos), y se articula con la metodología descrita en la Sección 7.2.1 “Identificación y descripción de los riesgos de seguridad de la información” de ISO/IEC 27005:2022, la cual aborda la descripción estructurada de activos como parte del análisis de riesgos.

Asimismo, se han integrado los lineamientos de las Secciones Anexo A 5.9 “Inventario de información y otros activos asociados” y 5.12 “Clasificación de la información” de ISO/IEC 27001:2022, que establecen la necesidad de contar con un inventario formal de activos y aplicar esquemas de clasificación que consideren confidencialidad, integridad y disponibilidad.

Esta organización permite establecer correspondencias directas con los controles aplicables, garantizar la trazabilidad normativa, y reforzar la estructura multicapa de seguridad presentada en la sección 5.2.4.

5.3 Análisis y Evaluación de Riesgos

Con base en la identificación y clasificación de activos de información realizada en la Sección 5.2, esta sección aborda el análisis y la evaluación de los riesgos de seguridad de la información inherentes a los proyectos de investigación medioambiental. Este proceso resulta indispensable para identificar las amenazas que podrían comprometer los activos y definir los requisitos de seguridad necesarios para el modelo de gestión de seguridad de la información (MGSI). Permite comprender de manera rigurosa los eventos no deseados que podrían afectar los activos y sistemas de información, orientando la definición de requisitos de seguridad en la Sección 5.4 (Análisis de Amenazas y Evaluación de Impacto) y la planificación de su implementación en la Sección 6 (Fase Hacer). La metodología se fundamenta en la Sección 7 (Proceso de evaluación de riesgos de seguridad de la información) de ISO/IEC 27005:2022, que establece directrices para la identificación, análisis y evaluación de riesgos; el Apartado 6.4 (Evaluación de riesgos) de ISO

31000:2018, que estructura el proceso de gestión del riesgo; el Catálogo de Elementos del Libro II de MAGERIT v3, que enumera amenazas y vulnerabilidades aplicables; el Control RA-3 (Evaluación de riesgos) de NIST SP 800-53 Rev. 5, que promueve un enfoque sistemático; y la Cláusula 6.1 (Acciones para abordar riesgos y oportunidades) de ISO/IEC 27001:2022, que define los requisitos para integrar la gestión de riesgos en un Sistema de Gestión de Seguridad de la Información (SGSI).

En los proyectos de investigación, los entornos distribuidos descritos en el Apartado 2.3.3 (Infraestructura tecnológica en proyectos de investigación) presentan retos específicos que incrementan la exposición a riesgos de seguridad. La diversidad tecnológica, caracterizada por el uso de múltiples plataformas y sistemas heterogéneos, junto con las limitaciones de conectividad en áreas remotas, complica la protección de los activos de información. Por ejemplo, los datos de calidad del agua, clasificados como sensibles en el Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), son vitales para la toma de decisiones ambientales, y su manipulación indebida podría generar consecuencias graves, como políticas erróneas que comprometan la conservación de ecosistemas. De manera similar, las plataformas de análisis geoespacial, detalladas en el Apartado 2.3.3.4 (Infraestructura de Análisis y Visualización), son susceptibles a accesos no autorizados si carecen de configuraciones seguras, lo que podría exponer información estratégica, como ubicaciones de especies protegidas, a actores maliciosos.

Esta evaluación inicial permite detectar los peligros que amenazan activos significativos, estableciendo una base sólida para las etapas detalladas que se desarrollarán en las subsecciones subsiguientes. La metodología aplicada se alinea con las características particulares de los proyectos medioambientales, descritas en la Sección 3.2 (Características Particulares de los Proyectos Medioambientales), que incluyen entornos Multi-Actor, conforme a la Sección 1.1 (Planteamiento del Problema), y la alta sensibilidad de los datos manejados, según la Sección 3.1. Por ejemplo, los sistemas de almacenamiento en la nube, especificados en el Apartado 2.3.3.3 (Infraestructura de Almacenamiento y Procesamiento), son esenciales para la disponibilidad de datos analíticos, pero su dependencia de conectividad remota los expone a riesgos de interrupción. Asimismo, los sistemas de respaldo, descritos en el Apartado 2.3.3.7 (Infraestructura de Respaldo, Continuidad y Energía), son de importancia para la continuidad operativa, pero su ubicación en áreas remotas los hace vulnerables a riesgos físicos, como sabotaje o daños ambientales.

Este proceso de análisis y evaluación de riesgos desempeña un papel decisivo en la protección de la información y la continuidad operativa, al garantizar que las amenazas se identifiquen, evalúen y prioricen de manera sistemática, alineándose con los objetivos del proyecto de establecer prácticas y políticas robustas para la seguridad de la información. Cada norma internacional aplicada contribuye a una etapa específica del proceso. La Sección 7 de ISO/IEC 27005:2022 estructura la gestión de riesgos en etapas claras: identificación de amenazas, análisis de su probabilidad e impacto, evaluación de niveles de riesgo, y tratamiento mediante controles. Por ejemplo, la identificación de amenazas como accesos no autorizados a bases de datos científicas se basa en el Catálogo de Elementos del Libro II de MAGERIT v3, que enumera amenazas relevantes para la infraestructura tecnológica descrita en el Apartado 2.3.3. El Apartado 6.4 de ISO 31000:2018 guía la evaluación de riesgos, priorizando aquellos con mayor impacto, como la manipulación de datos de calidad del agua, que podría afectar decisiones ambientales críticas. El Control RA-3 de NIST SP 800-53 Rev. 5 enfatiza la consideración de interdependencias entre activos, como la relación entre los sistemas de almacenamiento distribuido (Apartado 2.3.3.5, Sistemas de almacenamiento distribuido) y las plataformas de modelado climático (Apartado 2.3.3.2, Sistemas de modelado climático), donde una interrupción en el primero podría limitar el análisis del segundo. La Cláusula 6.1 “Acciones para abordar riesgos y oportunidades” de ISO/IEC 27001:2022 asegura que el proceso se integre en el SGSI, proporcionando un marco para la auditoría y mejora continua. Esta integración normativa permite abordar riesgos específicos del contexto medioambiental, como la exposición de datos sensibles en entornos remotos, garantizando que las medidas de seguridad sean proporcionales y efectivas.

Para lograr este propósito, el análisis se estructura en cinco etapas interrelacionadas, detalladas en las subsecciones subsiguientes: identificación de amenazas y vulnerabilidades, evaluación de impacto y sensibilidad, análisis de riesgos, determinación de niveles de riesgo, y tratamiento del riesgo con selección de controles. Este enfoque asegura la consideración de todos los riesgos relevantes, desde la alteración de datos en bases de datos científicas hasta la interrupción de sistemas de respaldo. Además, se evalúa la interdependencia entre riesgos y activos, ya que un problema en un elemento puede propagarse en entornos distribuidos. Por ejemplo, una falla en los sistemas de almacenamiento distribuido podría restringir el acceso a datos en plataformas de modelado climático, afectando la continuidad operativa, conforme a los

principios de análisis de riesgos de la Sección 3 (Método de análisis de riesgos) del Libro I de MAGERIT v3. El proceso también considera regulaciones locales, como la Ley 1581 de 2012, referida en el Apartado 2.7.2 (Leyes), que establece requisitos para la protección de datos personales, especialmente relevantes para los datos sensibles manejados. Por lo tanto, los resultados de esta sección, formalizados en un registro de riesgos documentado en la Tabla 8 (Análisis de Riesgos y Amenazas), constituyen el insumo necesario que orienta la selección y el diseño de controles en la Fase Hacer (Sección 6), respaldando la protección de la información y preparando las fases de verificación (Sección 7) y mejora (Sección 8) del ciclo PHVA, garantizando una gestión de seguridad coherente con los objetivos del proyecto.

5.3.1 *Identificación de Amenazas y Vulnerabilidades.*

Con base en los activos de información identificados y clasificados en la Sección 5, esta sección describe la metodología empleada y los resultados obtenidos al identificar amenazas y vulnerabilidades que podrían comprometer la seguridad en los proyectos de investigación. Este proceso inicia el análisis de riesgos descrito en la Sección 5.3 (Análisis y Evaluación de Riesgos), generando los insumos necesarios para evaluar el impacto y la sensibilidad en la Sección 5.3.2 (Evaluación de Impacto y Sensibilidad). La metodología se alinea con las características operativas y tecnológicas de los proyectos, conforme a la Sección 3.2 (Características Particulares de los Proyectos Medioambientales), y se fundamenta en estándares internacionales relevantes. Estos incluyen la Sección 7.2 (Identificación de riesgos de seguridad de la información) de ISO/IEC 27005:2022, que establece directrices para detectar riesgos; el Apartado 6.4.2 (Identificación del riesgo) de ISO 31000:2018, que describe el reconocimiento de amenazas; el Control RA-3 (Evaluación de riesgos) de NIST SP 800-53 Rev. 5, que promueve un enfoque sistemático; y los tres libros de MAGERIT v3: el Libro I, Sección 3 (Método de análisis de riesgos), que proporciona el marco metodológico; el Libro II, Sección 5 (Amenazas) y el Libro III, Sección 2 (Técnicas específicas), que detalla métodos prácticos.

La identificación considera el contexto organizacional descrito en la Sección 1.1 (Planteamiento del Problema), que destaca los retos de operar en entornos Multi-Actor, y la infraestructura tecnológica especificada en el Apartado 2.3.3 (Infraestructura tecnológica en proyectos de investigación), que abarca sistemas de almacenamiento, análisis y respaldo. También

prioriza la sensibilidad de los datos, conforme al Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), como registros de biodiversidad y datos climáticos. El proceso emplea técnicas estructuradas, alineadas con la Sección 7.2 (Identificación de riesgos de seguridad de la información) de la norma ISO/IEC 27005:2022 y con la Sección 2 (Técnicas específicas) del Libro III de MAGERIT v3. Por ejemplo, se realizan entrevistas con personal técnico y científico, utilizando preguntas como "¿Qué controles de acceso protegen las bases de datos científicas compartidas entre instituciones?" o "¿Qué incidentes físicos han afectado los sistemas de respaldo en áreas remotas?". Las revisiones de configuraciones se apoyan en técnicas como el Sección 2.1 “Análisis mediante tablas” y Sección 2.2 “Análisis algorítmico” , descritos en el mismo Libro III de MAGERIT v3, evaluando parámetros como segmentación de redes mediante VLAN, cifrado AES-256 y autenticación multifactor, aplicadas a activos como servidores de análisis (Apartado 2.3.3.4) y sistemas de almacenamiento distribuido (Apartado 2.3.3.5). Estas revisiones son particularmente efectivas para detectar vulnerabilidades como configuraciones por defecto no seguras (ej., puertos abiertos no protegidos) o falta de cifrado en protocolos de comunicación, que podrían exponer datos sensibles a manipulaciones. El análisis de incidentes históricos identifica patrones, como accesos no autorizados en plataformas similares, proporcionando evidencia empírica.

Las amenazas identificadas abarcan categorías tecnológicas, humanas y físicas, adaptadas a los proyectos de investigación medioambiental mediante la Sección 5 “Amenazas” del Catálogo de Elementos del Libro II de MAGERIT v3. Por ejemplo, la Sección 5.4.9. [A.11] Acceso no autorizado, incluye el robo de datos de biodiversidad, que podría facilitar actividades ilegales como la caza furtiva, afectando la conservación de especies protegidas. La Sección 3.2. [I] Integridad de los datos, abarca la manipulación de datos climáticos por motivos políticos, distorsionando modelos predictivos necesarios para la gestión ambiental. Los datos ambientales clasificados en la Sección 5.2.4.2 (Datos Ambientales) enfrentan amenazas tecnológicas como inyecciones SQL, que podrían alterar registros de especies protegidas en bases de datos científicas (Apartado 2.3.3.4, Infraestructura de Análisis y Visualización). Los sistemas de respaldo, clasificados como Equipamiento Tecnológico en la Sección 5.2.4.4, son vulnerables a sabotaje físico en ubicaciones remotas. Amenazas específicas incluyen ataques de ransomware que bloquean el acceso a datos climáticos, contemplados en la Sección 3.4. [A] Autenticidad de Libro II de MAGERIT v3, Fraude,

y ataques de ingeniería social dirigidos a investigadores para obtener credenciales. Estas amenazas se seleccionan del catálogo y se adaptan al Apartado 2.3.3, vinculándolas a activos mediante la Sección 5.9 “Inventario de información y otros activos asociados” de ISO/IEC 27002:2022.

Pasando de las amenazas a las vulnerabilidades, el proceso identifica deficiencias específicas que facilitan la materialización de los riesgos, conforme a la Sección 5.3 “Errores y fallos no intencionados” del Catálogo de Elementos del Libro II de MAGERIT v3. Estas incluyen configuraciones inseguras, como la falta de segmentación en bases de datos científicas, representadas en la entrada 5.3.4 “[E.4] Errores de configuración”, que afectan la integridad de los datos debido a errores en parámetros como privilegios de acceso o flujos de actividades.

La ausencia de autenticación multifactor en sistemas de almacenamiento en la nube se corresponde con la entrada 5.3.2 “[E.2] Errores del administrador”, que contempla equivocaciones en la instalación y operación de sistemas, y con 5.3.5 “[E.7] Deficiencias en la organización”, que refleja fallas por indefinición de responsabilidades dentro del personal técnico. Por ejemplo, las revisiones de configuraciones, apoyadas en las técnicas descritas en la Sección 2.1 “Análisis mediante tablas” y 2.2 “Análisis algorítmico” del Libro III de MAGERIT v3 – Guía de Técnicas, permiten detectar vulnerabilidades como la falta de cifrado AES-256 en datos en reposo dentro de plataformas de modelado climático.

Otras vulnerabilidades incluyen parches desactualizados en dispositivos de campo, identificadas también en la entrada [E.4] Errores de configuración, y errores humanos por falta de capacitación, contemplados en 5.3.1 “[E.1] Errores de los usuarios”, que abordan equivocaciones en el uso de servicios o datos. Estas debilidades se documentan conforme al Apartado 6.4.2 “Identificación del riesgo” de la norma ISO 31000:2018, que establece principios para reconocer causas, fuentes y potenciales consecuencias, e invita al uso de métodos como listas de verificación y análisis estructurado con métricas como CVSS para evaluar configuraciones técnicas como puertos abiertos en auditorías de seguridad.

Las interdependencias entre activos se mapean mediante diagramas de relaciones, construidos con herramientas de modelado como UML, siguiendo un proceso de tres pasos: identificar activos clave (por ejemplo, almacenamiento distribuido, modelado climático), trazar flujos de datos, y analizar puntos de fallo, conforme a la Sección 3 “Método de análisis de riesgos” del Libro I de MAGERIT v3, donde se desarrollan formalmente los conceptos y tareas para

caracterizar activos, amenazas y salvaguardas, así como estimar el estado del riesgo. Por ejemplo, una configuración insegura en los sistemas de almacenamiento distribuido, descrita en el Apartado 2.3.3.5 del documento base, podría facilitar un ataque de denegación de servicio, afectando la disponibilidad de datos en plataformas de modelado climático y comprometiendo análisis críticos.

Los resultados se documentan en la Tabla 7 “Identificación de Amenazas y Vulnerabilidades”, vinculando amenazas y vulnerabilidades a activos específicos (por ejemplo, Datos Ambientales, Equipamiento Tecnológico), lo cual proporciona un insumo claro para la Sección 5.3.2 “Evaluación de Impacto y Sensibilidad”. Este proceso protege la integridad de los datos y asegura la continuidad operativa, alineándose con los objetivos del proyecto de establecer un modelo de seguridad robusto. También considera el marco legal vigente, específicamente la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, citada en el Apéndice 3 “Marco legal” del Libro I de MAGERIT v3, que exige adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos y evitar su alteración, pérdida o acceso no autorizado.

Por lo tanto, esta subsección orienta el diseño de controles en la Sección 6 (Fase Hacer), la auditoría en la Sección 7 (Fase Verificar) y la mejora continua en la Sección 8 (Fase Actuar), siguiendo el ciclo de gestión de riesgos propuesto por la metodología.

Tabla 7

Identificación de Amenazas y Vulnerabilidades

CATEGORÍA DE AMENAZA	*SUB CATEGORÍA*	*EJEMPLOS*	*NORMATIVAS Y MARCOS RELACIONADOS*
CIBERNÉTICAS	Malware	Infección de servidores con ransomware que cifra datos de investigación	NIST SP 800-53 Rev. 5 (RA-5: Monitoreo y escaneo de vulnerabilidades)
	Phishing	Correos fraudulentos dirigidos a investigadores para robar credenciales de acceso	NIST SP 800-53 Rev. 5 (SI-4: Monitoreo del sistema)
OPERACIONALES	Error Humano	Publicación accidental de datos de muestras ecológicas en servidores abiertos	ISO/IEC 27002:2022 (8.8: Gestión de vulnerabilidades)
	Brechas de Seguridad	Uso indebido de credenciales compartidas entre equipos de investigación	CIS Controls v8 (Control 5: Administración de Cuentas)
AMBIENTALES	Desastres Naturales	Pérdida de servidores de datos por inundaciones en laboratorios de campo	MAGERIT v3 (Capítulo 3: Método de análisis de riesgos)
	Fallas de Infraestructura	Caída de sistemas de monitoreo ambiental por fallos de energía	MAGERIT v3 Libro II (Capítulo 6.14: Continuidad de operaciones)

Fuente: Elaboración Propia

La Tabla presenta una clasificación estructurada de las amenazas y vulnerabilidades que pueden afectar el desarrollo de los proyectos de investigación medioambiental. Esta organización facilita la visualización de los factores de riesgo que comprometen la seguridad de la información, la integridad de los datos científicos y la continuidad de las operaciones.

El análisis agrupa las amenazas en tres categorías principales:

- Amenazas cibernéticas: Comprenden ataques deliberados contra los sistemas de información, como la propagación de software malicioso (malware), ransomware, campañas de phishing dirigidas a usuarios internos o la explotación de vulnerabilidades en aplicaciones críticas. Estos incidentes tienen el potencial de comprometer la confidencialidad de bases de datos ambientales, alterar información sensible o interrumpir servicios esenciales para la investigación.
- Amenazas operacionales: Incluyen fallos derivados de errores humanos, configuraciones incorrectas, deficiencias en la gestión de respaldos, mantenimiento insuficiente de infraestructura tecnológica y debilidades en los procesos de administración de cambios. Estas amenazas aumentan el riesgo de indisponibilidad de datos, corrupción de información crítica o retrasos en actividades de monitoreo y análisis de campo.
- Amenazas ambientales: Se refieren a eventos físicos o naturales, como inundaciones, incendios, sismos o fallos prolongados en el suministro eléctrico, que pueden dañar equipos, afectar centros de datos locales o interrumpir la recolección automatizada de información ambiental.

Cada amenaza identificada se complementa con las vulnerabilidades asociadas que podrían facilitar su materialización, tales como:

- Ausencia de políticas sólidas de control de accesos.
- Segmentación insuficiente de las redes internas.
- Configuraciones inseguras en dispositivos y plataformas.
- Uso de versiones de software desactualizadas o sin parches de seguridad.
- Escasa capacitación del personal en buenas prácticas de ciberseguridad.
- Inexistencia de procedimientos robustos de respaldo y recuperación.

La identificación estructurada de amenazas y vulnerabilidades permite construir un mapa de exposición que refleja los activos más susceptibles a incidentes, orientando de manera inicial las estrategias de mitigación que deberán diseñarse posteriormente.

Esta actividad no solo mejora la comprensión de los riesgos existentes, sino que también constituye la base para su valoración detallada. La relación entre amenazas, vulnerabilidades y activos evaluados será formalizada en la Matriz de Análisis de Riesgos y Amenazas (sección siguiente), en la cual se combinarán los factores de probabilidad e impacto para establecer las prioridades de tratamiento de riesgo.

El uso de este enfoque permite mantener la trazabilidad y coherencia de la gestión de riesgos, alineándola a las mejores prácticas internacionales y garantizando que las acciones posteriores de mitigación sean proporcionales al nivel de exposición identificado.

Tabla 8

Análisis de Riesgos y Amenazas

RIESGO	ACTIVO AFECTADO	CRITICIDAD	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	CONTROL PREVENTIVO	CONTROL DETECTIVO	CONTROL CORRECTIVO	NORMATIVAS RELACIONADAS	JUSTIFICACIÓN
ACCESO NO AUTORIZADO	Bases de datos de investigación	**Alto**	**Alto**	**Medio**	**Alto**	Firewalls, autenticación multifactor, políticas de acceso	Monitoreo de accesos, auditorías, análisis de registros	Gestión de incidentes, bloqueo de cuentas sospechosas, revalidación de accesos	**ISO/IEC 27002:2022 (5.15 - Control de acceso), NIST SP 800-53 Rev. 5 (AC-2 - Gestión de Cuentas), CIS Controls v8 (Control 5 - Administración de Cuentas), ISO/IEC 27001:2022 (5.15 - Control de Acceso)**	La falta de control de accesos puede exponer información crítica, comprometiendo la integridad de los datos.
MALWARE Y RANSOMWARE	Servidores con datos ambientales	**Muy Alto**	**Muy Alto**	**Alto**	**Muy Alto**	Protección contra malware, segmentación de red, listas blancas de aplicaciones	Análisis de tráfico, detección de anomalías, respuesta automatizada	Restauración de datos, eliminación de software malicioso, notificación de incidentes	**NIST SP 800-53 Rev. 5 (SI-3 - Protección Contra Códigos Malicioso), ISO/IEC 27002:2022 (8.8 - Gestión de vulnerabilidades técnicas), CIS Controls v8 (Control 10 - Defensas contra Malware), ISO/IEC 27005:2022 (Gestión de Riesgos de Seguridad)**	Los ataques de ransomware pueden bloquear el acceso a información clave para la investigación, afectando la continuidad de los proyectos.

RIESGO	ACTIVO AFECTADO	CRITICIDAD	IMPACTO	PROBABILIDAD	NIVEL DE RIESGO	CONTROL PREVENTIVO	CONTROL DETECTIVO	CONTROL CORRECTIVO	NORMATIVAS RELACIONADAS	JUSTIFICACIÓN
ATAQUES DDOS	Plataformas de publicación y colaboración	**Alto**	**Alto**	**Medio**	**Alto**	Balanceo de carga, protección contra tráfico malicioso	Monitoreo de tráfico, detección de patrones anómalos	Mitigación automática, activación de defensa en la nube	**ISO/IEC 27002:2022 (8.21 - Seguridad de los servicios de red), NIST SP 800-53 Rev. 5 (SC-5 - Protección Contra Denegación de Servicio), CIS Controls v8 (Control 12 - Gestión de la Infraestructura de Red)**	Un ataque DDoS puede hacer que plataformas de investigación sean inaccesibles, afectando la continuidad del trabajo.
EXPOSICIÓN DE CREDENCIALES	Sistemas de acceso a datos	**Muy Alto**	**Alto**	**Alto**	**Muy Alto**	Uso de autenticación multifactor, restricciones de acceso según rol	Detección de accesos sospechosos, auditoría de credenciales comprometidas	Reseteo de credenciales, monitoreo y respuesta a incidentes	**ISO/IEC 27002:2022 (5.16 - Gestión de identidad), NIST SP 800-53 Rev. 5 (IA-5 - Administración de autenticadores), CIS Controls v8 (Control 6 - Gestión de Control de Accesos)**	La exposición de credenciales puede derivar en accesos no autorizados y filtración de información sensible.
MANIPULACIÓN DE DATOS CIENTÍFICOS	Bases de datos de resultados experimentales	**Muy Alto**	**Muy Alto**	**Medio**	**Alto**	Controles de integridad, firmas digitales, versiones de datos inmutables	Registro de cambios en bases de datos, auditorías periódicas	Restauración de versiones anteriores, investigación de actividades sospechosas	**ISO/IEC 27002:2022 (8.10 - Eliminación de la información), NIST SP 800-53 Rev. 5 (SC-12 - Establecimiento y Gestión de Claves Criptográficas), CIS Controls v8 (Control 14 - Concientización en Seguridad y Formación de Habilidades)**	La manipulación de datos puede comprometer la validez de los resultados y afectar la credibilidad de la investigación.

Fuente: Elaboración Propia

La Tabla consolida el análisis de riesgos y amenazas desarrollado en el modelo de seguridad de la información, estructurando de manera sistemática los elementos críticos que componen este proceso. Esta matriz no constituye un resumen aislado, sino el resultado integral de la identificación de activos, amenazas y vulnerabilidades, complementada por la evaluación de criticidad y sensibilidad de los activos realizada en etapas anteriores.

Su propósito es facilitar una interpretación clara de los escenarios de riesgo, apoyando la toma de decisiones informadas sobre las medidas de mitigación más adecuadas para preservar la seguridad de los datos y la continuidad de las operaciones.

El primer componente de la tabla corresponde a la identificación del riesgo, donde se describen de forma específica los eventos que podrían afectar los proyectos de investigación, tales como accesos no autorizados, infecciones por malware o fallos en los sistemas de respaldo. Esta descripción concreta permite visualizar los distintos escenarios de impacto sobre los activos críticos.

A continuación, se detalla el activo afectado, estableciendo una vinculación explícita entre cada riesgo identificado y los activos previamente clasificados en el modelo, como bases de datos de biodiversidad, registros climáticos o plataformas tecnológicas de almacenamiento. Esta asociación fortalece la trazabilidad documental exigida en los estándares internacionales de gestión de seguridad de la información.

Posteriormente, se presenta la criticidad del activo, evaluada conforme a los criterios definidos en la Tabla 8. Este parámetro permite comprender la relevancia de cada activo para la continuidad de los procesos y el logro de los objetivos institucionales. Una criticidad alta, por ejemplo, asignada a datos sensibles sobre biodiversidad, justifica la implementación de controles de protección reforzados.

La valoración de impacto y probabilidad de ocurrencia se realiza utilizando escalas cualitativas previamente definidas (alto, medio, bajo). Su combinación determina el nivel de riesgo, conforme a los criterios establecidos en ISO/IEC 27005:2022, sección 6.4 “Establecimiento y mantenimiento de los criterios de riesgo para la seguridad de la información”. Esta metodología facilita la priorización de riesgos, destacando aquellos escenarios que exigen una atención inmediata frente a aquellos con menor exposición.

La tabla también incorpora la descripción de los controles de seguridad establecidos, diferenciados en tres categorías:

- Preventivos: Orientados a evitar que las amenazas se materialicen.
- Detectivos: Enfocados en identificar incidentes en curso o recién ocurridos.
- Correctivos: Dirigidos a restaurar las operaciones tras un incidente.

Esta clasificación de controles se estructura conforme a las secciones 5 a 8 de ISO/IEC 27002:2022, que organizan los controles en ámbitos organizacionales, de personas, físicos y tecnológicos.

Asimismo, cada control propuesto se vincula a las normativas y marcos de referencia aplicables, tales como ISO/IEC 27002:2022, NIST SP 800-53 Rev. 5 y COBIT 2019, reforzando la solidez técnica y la coherencia del modelo con buenas prácticas internacionales de gestión de riesgos.

Complementariamente, la tabla incluye una justificación técnica que explica la selección de los controles para cada escenario de riesgo. Esta justificación asegura que las medidas adoptadas no sean arbitrarias, sino basadas en un análisis racional que considera la naturaleza del activo afectado, el tipo de amenaza y la viabilidad de la mitigación.

La estructura completa de la Tabla 10 proporciona una representación clara y trazable de la relación entre amenazas, activos comprometidos, medidas de control y referencias normativas, lo que facilita tanto la implementación de los controles como la revisión y validación por parte de las partes interesadas en la gestión de la seguridad.

La Matriz de Análisis de Riesgos y Amenazas desarrollada a partir de esta tabla ofrece una visión integral de los escenarios de riesgo, considerando no solo la naturaleza de las amenazas y vulnerabilidades, sino también el impacto potencial y la probabilidad de ocurrencia sobre los activos del proyecto.

Esta estructura brinda a la organización una base sólida para priorizar los riesgos identificados y tomar decisiones de mitigación fundamentadas en un análisis ordenado y verificable. El vínculo explícito entre riesgos, controles (preventivos, detectivos, correctivos) y

marcos normativos aplicables refuerza la consistencia del modelo y facilita su ejecución efectiva y seguimiento continuo.

Finalmente, tomando como fundamento el análisis consolidado en la Tabla 10, el modelo de seguridad avanza hacia la definición de medidas específicas de protección, orientadas a reducir la exposición a incidentes y a fortalecer la resiliencia operativa de los proyectos de investigación medioambientales.

5.3.2 *Evaluación de Impacto y Sensibilidad.*

Con base en las amenazas y vulnerabilidades identificadas en la Sección 5.3.1 (Identificación de Amenazas y Vulnerabilidades) y los activos clasificados en la Sección 5.2 (Identificación y Clasificación de Activos de Información en Entornos Distribuidos), esta subsección evalúa el impacto potencial y la sensibilidad de los riesgos en los proyectos de investigación medioambiental. El proceso analiza las consecuencias de la materialización de amenazas sobre los activos, considerando dimensiones como confidencialidad, integridad, disponibilidad, así como impactos ambientales, legales y reputacionales, alineados con las características operativas descritas en el Apartado 2.3.3 (Infraestructura tecnológica en proyectos de investigación) y la sensibilidad de los datos establecida en el Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles). La metodología se fundamenta en la Sección 6.4.3 “Análisis de riesgos” de la norma ISO 31000:2018, que describe la evaluación de consecuencias; la Sección 7.3 “Análisis de riesgo de seguridad de la información” de ISO/IEC 27005:2022, que detalla la evaluación de impactos; y la Sección 3 “Método de análisis de riesgos” del Libro I de MAGERIT v3, que propone un enfoque sistemático para analizar efectos. Este análisis proporciona insumos críticos para el análisis de riesgos en la Sección 5.3.3, la selección de controles en la Sección 5.3.5, y las auditorías en la Sección 7 (Fase Verificar).

La evaluación de impacto emplea un enfoque cualitativo, adaptado al contexto Multi-Actor de los proyectos (Sección 1.1, Planteamiento del Problema), que incluye universidades, gobiernos y comunidades. Se considera la criticidad de los activos, como datos ambientales (Sección 5.2.4.2) y equipamiento tecnológico (Sección 5.2.4.4), clasificados según su sensibilidad en la Sección 5.2.4. Las consecuencias se evalúan en función de las dimensiones de confidencialidad, integridad

y disponibilidad, complementadas por impactos específicos del sector medioambiental, como la pérdida de biodiversidad o el incumplimiento normativo (Apartado 2.7.2, Leyes). Por ejemplo, la exposición de datos de biodiversidad (Sección 5.2.4.2) debido a un acceso no autorizado (Sección 5.4.9, [A.11] Acceso no autorizado del Libro II de MAGERIT v3) podría facilitar actividades ilegales como la caza furtiva, generando un impacto ambiental severo y violaciones legales conforme a la Ley 1581 de 2012 (Apartado 2.7.2). Este impacto comprometería los objetivos del proyecto de proteger datos sensibles (Sección 1.4.1).

La sensibilidad de la información se evalúa mediante criterios definidos en el Apartado 3.1, que clasifica datos como registros de especies protegidas y proyecciones climáticas según su valor científico y social. Se emplean técnicas de análisis de escenarios, alineadas con la Sección 2 "Técnicas específicas" del Libro III de MAGERIT v3, para estimar los efectos de las amenazas en los activos. Por ejemplo, la manipulación de datos climáticos en plataformas de modelado (Apartado 2.3.3.2, Sistemas de modelado climático) por una amenaza de modificación no autorizada (Sección 5.4.13, [A.15] "Modificación deliberada de la información", del Libro II de MAGERIT v3) podría distorsionar modelos predictivos, afectando la integridad de los datos y generando decisiones erróneas en la gestión ambiental, con un impacto reputacional para las instituciones involucradas. La Tabla 9 Evaluación Integridad, Confidencialidad y Disponibilidad, Documenta los impactos en las dimensiones CID para los activos de importancia. Los resultados de esta evaluación priorizan los activos más sensibles para el tratamiento de riesgos en la Sección 5.3.5 y la mejora continua en la Sección 8 (Fase Actuar).

Tabla 9

Evaluación Integridad, Confidencialidad y Disponibilidad

CRITERIO	DEFINICIÓN	PARÁMETROS DE EVALUACIÓN	NIVELES/VALOR				
			0-19%	20 - 39%	40 - 60%	61-89%	90 - 100%
INTEGRIDAD	Garantiza la exactitud y consistencia de los datos, evitando alteraciones no autorizadas.	Control de versiones, firma digital, auditorías de cambios, redundancia de datos.	Muy Baja	Baja	Media	**Alta**	Muy Alta
CONFIDENCIALIDAD	Protege la información contra accesos no autorizados mediante controles específicos.	Cifrado de extremo a extremo, control de acceso basado en roles, políticas de clasificación de datos.	Muy Baja	Baja	Media	**Alta**	Muy Alta
DISPONIBILIDAD	Asegura el acceso oportuno y fiable a la información cuando se necesita.	Planes de recuperación ante desastres, sistemas de respaldo, monitoreo continuo de servicios.	Muy Baja	Baja	Media	Alta	Muy Alta

Fuente y Adaptación ISO 31000

La Tabla 9 presenta un esquema de clasificación de activos basado en los tres principios centrales de seguridad de la información: confidencialidad, integridad y disponibilidad. Cada dimensión incorpora una escala de valoración cualitativa estructurada en cinco niveles, vinculada a intervalos porcentuales representativos de su nivel de sensibilidad. Esta escala permite evaluar el grado de protección requerido por cada activo, en función del posible impacto que tendría una alteración, pérdida o divulgación no autorizada.

Este enfoque responde a los lineamientos de la Sección 7.2.1 “Identificar y describir los riesgos de seguridad de la información” de ISO/IEC 27005:2022, que establece la necesidad de valorar los activos de acuerdo con su función, dependencias y consecuencias potenciales. Asimismo, se fundamenta en el marco de análisis de consecuencias definido en la Sección 6.4.3 “Análisis de riesgos” de ISO 31000:2018, que promueve el uso de criterios organizacionales para estimar niveles de riesgo.

Cada principio de seguridad está asociado a parámetros técnicos y ejemplos de controles aplicables. Para la integridad, se incluyen mecanismos como firmas digitales, auditorías de cambios y trazabilidad documental. Para la confidencialidad, se consideran técnicas de cifrado, clasificación de datos y control de accesos. En el caso de la disponibilidad, se contemplan planes de recuperación, sistemas redundantes y copias de respaldo. Esta estructuración facilita la identificación de brechas específicas y la asignación de medidas proporcionales, coherentes con los controles recomendados en el Control 3 Protección de Datos y el Control 11 Recuperación de Datos de CIS Controls v8.

Además de clasificar los activos, la tabla establece una correspondencia práctica con el modelo de gestión de riesgos y la arquitectura de protección descrita en las secciones siguientes. Esto permite consolidar la trazabilidad entre sensibilidad, impacto y controles aplicados, reforzando la consistencia operativa del modelo de seguridad.

Tabla 10

Evaluación del Acceso y Disponibilidad

SUB CRITERIO	NIVEL	DEFINICIÓN / ALCANCE	ORIENTACIONES DE LOS MARCOS DE REFERENCIA	EJEMPLOS
ACCESO	**Abierto**	Los datos pueden obtenerse sin restricciones ni autorizaciones especiales; por lo general, están publicados con licencias abiertas o bajo políticas de datos abiertos.	**ISO/IEC 27001**: Capítulo sobre Control de Accesos (Anexo A).	Datos meteorológicos en portales gubernamentales con libre descarga.
			CIS Controls v8: Control 14 (Concientización en Seguridad y Formación de Habilidades).	Cartografía o datos geoespaciales bajo licencias Creative Commons.
			COBIT 2019: Capítulo 4. Objetivos de gobierno y gestión de COBIT EDM y APO (gestión de activos y acceso).	
	Semi-Restringido	El acceso está sujeto a ciertos requisitos (registro, aprobación, suscripción), pero no implica un alto nivel de confidencialidad ni medidas excesivas de protección.	**ISO/IEC 27002**: Tabla B.2 9.2 (Gestión de Acceso de Usuarios).	Bases de datos académicas disponibles para miembros de instituciones afiliadas.
			MAGERIT v3: Análisis de riesgos básicos para	Repositorios con restricción de

SUB CRITERIO	NIVEL	DEFINICIÓN / ALCANCE	ORIENTACIONES DE LOS MARCOS DE REFERENCIA	EJEMPLOS
DISPONIBILIDAD			información clasificada en niveles medios.	descarga a usuarios autenticados.
	Restringido	El acceso se limita a personal acreditado o entidades autorizadas, dadas las implicaciones de confidencialidad, secreto comercial o seguridad nacional. Pueden requerirse contratos de confidencialidad y mecanismos de autenticación robustos.	**ISO/IEC 27001**: Políticas específicas de acceso (controles de alta sensibilidad).	Información de instalaciones estratégicas (refinerías, plantas nucleares).
			NIST SP 800-53 Rev. 5: Controles AC (Access Control) y SC (System & Communications Protection).	Datos de seguridad nacional o clasificados por acuerdos internacionales.
			TOGAF 10: Gestión de la seguridad de la arquitectura.	
	Alta	Los datos se recogen o actualizan con frecuencia y se mantienen en repositorios estables, asegurando un acceso constante y confiable. Se cuenta con planes de continuidad y respaldo adecuados para minimizar interrupciones.	**ISO 31000**: Gestión de riesgos y continuidad operacional.	Infraestructura de monitoreo continuo de calidad del aire (datos en tiempo real).
			ISO/IEC 27005: Evaluación y tratamiento de riesgos que afectan la disponibilidad.	Repositorios reconocidos (GBIF para biodiversidad) con actualización periódica y alta disponibilidad.
			COBIT 2019: Procesos MEA (Monitorear, Evaluar y Valorar)	
	Moderada	La actualización es periódica, aunque con retrasos o interrupciones esporádicas. Puede depender de presupuestos, convenios o políticas institucionales variables.	**ISO 55002**: Gestión de activos con mantenimientos planificados.	Datos de deforestación anuales que tardan varios meses en publicarse.
			CIS Controls v8: Control 13 (Protección de Datos), con niveles de madurez intermedios.	Series climáticas de proyectos con financiación de duración limitada.
			MAGERIT v3: Definición de umbrales de criticidad.	
	Baja	Existe incertidumbre en la frecuencia de actualización y en la conservación a largo	ISO 31000: Identificación de riesgos de discontinuidad.	Programas de ciencia ciudadana con recolección irregular de datos.

SUB CRITERIO	NIVEL	DEFINICIÓN / ALCANCE	ORIENTACIONES DE LOS MARCOS DE REFERENCIA	EJEMPLOS
		plazo, debido a recursos limitados o a la naturaleza puntual de los proyectos. Esto puede afectar la confiabilidad y la posibilidad de replicar o contrastar la información en el futuro.	NIST SP 800-53 Rev. 5: Controles de Contingencia (CP) y Recuperación de Desastres (IR).	Repositorios informales con riesgo de cierre o falta de mantenimiento a largo plazo.
			COBIT 2019: Procesos de aseguramiento de continuidad.	

Fuente: Elaboración Propia

La Tabla 10 presenta una clasificación funcional del acceso y la disponibilidad de los datos dentro del entorno técnico del proyecto. Esta evaluación se incorpora como complemento al análisis de sensibilidad de los activos sección 3, permitiendo establecer condiciones diferenciadas de control según el tipo de acceso autorizado y la frecuencia con la que la información debe mantenerse disponible.

El acceso se organiza en tres niveles: abierto, semi-restringido y restringido, definidos en función de los mecanismos de validación requeridos y del perfil de usuario autorizado. Esta segmentación se alinea con las directrices establecidas en ISO/IEC 27002:2022, en particular en:

- Sección 5.15 – "Control de acceso": Establece la necesidad de limitar el acceso a la información en función de requisitos del negocio.
- Sección 5.16 – "Gestión de identidad": Describe procesos para la creación, modificación y revocación de credenciales de usuario.
- Sección 5.17 – "Información de autenticación": Propone métodos seguros para proteger los factores de autenticación asociados al acceso.

Estas prácticas se complementan con los lineamientos de CIS Controls v8 – Control 6 “Gestión de Control de Accesos”, el cual recomienda aplicar el principio de mínimo privilegio y segmentar el acceso a los activos según el nivel de riesgo asociado.

Con respecto a la disponibilidad, la tabla diferencia entre activos de alta, moderada y baja disponibilidad. Esta categorización considera la frecuencia de actualización, la estabilidad de la infraestructura tecnológica y el impacto operativo de la interrupción en el acceso. Este análisis responde al criterio funcional establecido en ISO/IEC 27002:2022 Sección 8.6 “Gestión de capacidades”, que promueve asegurar recursos suficientes para mantener la disponibilidad de los servicios.

Además, el CIS Controls v8 – Control 11 “Recuperación de Datos” establece medidas para garantizar la recuperación de datos ante fallos, lo que refuerza la dimensión técnica de la disponibilidad. Por su parte, MAGERIT v3 – Libro II incorpora amenazas específicas aplicables a esta evaluación, como:

- 5.4.3. [A.5] Suplantación de la identidad del usuario, que describe la utilización fraudulenta de credenciales válidas para obtener acceso no autorizado a activos críticos.
- 5.4.4. [A.6] Abuso de privilegios de acces, donde un usuario autorizado emplea sus derechos más allá del ámbito previsto, generando riesgos a la integridad o confidencialidad de la información.”

Este enfoque conjunto permite integrar criterios operativos, normativos y técnicos en una misma estructura, facilitando la identificación de controles específicos y priorización de recursos en función de las condiciones reales de acceso y sostenibilidad de los activos de información.

5.3.3 *Análisis de Riesgos.*

Continuando con el proceso de gestión de riesgos, esta subsección integra la probabilidad y el impacto de los riesgos identificados para priorizarlos y generar un perfil de riesgo en los proyectos de investigación medioambiental. Este análisis considera el contexto Multi-Actor descrito en la Sección 1.1 (Planteamiento del Problema), la infraestructura tecnológica distribuida detallada en el Apartado 2.3.3 (Infraestructura tecnológica en proyectos de investigación), y la sensibilidad de los datos establecida en el Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles). La metodología se fundamenta en la Sección 6.4.3 “Análisis de riesgos” de ISO 31000:2018, que define la necesidad de estimar la naturaleza y magnitud de las

consecuencias de los riesgos, su probabilidad y nivel; en la Sección 7.3 “Análisis de los riesgos de seguridad” de ISO/IEC 27005:2022, que propone métodos cualitativos para priorizar riesgos mediante estimaciones de impacto y probabilidad; en el Control RA-3 “Evaluación de Riesgos” de NIST SP 800-53 Rev. 5, que establece un enfoque sistemático para identificar, evaluar y priorizar los riesgos de seguridad; y en la Sección 3 “Método de análisis de riesgos” del Libro I de MAGERIT v3, que estructura paso a paso el análisis mediante identificación de activos, amenazas, impacto, riesgo y salvaguardas. Los resultados de esta subsección proporcionan insumos necesarios para determinar los niveles de riesgo en la Sección 5.3.4, seleccionar controles en la Sección 5.3.5, y auditar en la Sección 7 (Fase Verificar).

El análisis de riesgos combina la evaluación cualitativa de la probabilidad de ocurrencia de las amenazas identificadas (Sección 5.3.1) con los impactos estimados (Sección 5.3.2), utilizando una matriz de evaluación para clasificar los riesgos según su severidad. La probabilidad se estima considerando factores como la frecuencia de incidentes históricos, la exposición de los activos (Sección 5.2), y las vulnerabilidades específicas (ej., configuraciones inseguras, Sección 5.4.3 [A.5] “Suplantación de la identidad del usuario” del Libro II de MAGERIT v3). que describe situaciones en las que se compromete la autenticidad de credenciales y se aprovechan configuraciones inseguras para suplantar accesos. El impacto abarca dimensiones de confidencialidad, integridad y disponibilidad, así como consecuencias ambientales, legales y reputacionales, adaptadas al contexto medioambiental (Sección 3.2). Por ejemplo, un ataque de ransomware (5.4.13. [A.15] Modificación deliberada de la información del Libro II de MAGERIT v3) dirigido a sistemas de almacenamiento distribuido (Apartado 2.3.3.5) tiene una probabilidad moderada debido a la exposición de sistemas en entornos remotos (Sección 1.1), pero un impacto alto, ya que bloquearía el acceso a datos climáticos (Sección 5.2.4.2), afectando la gestión de emergencias ambientales y generando sanciones legales por incumplimiento de la Ley 1581 de 2012 (Apartado 2.7.2). Este riesgo se clasifica como prioritario para el tratamiento en la Sección 5.3.5.

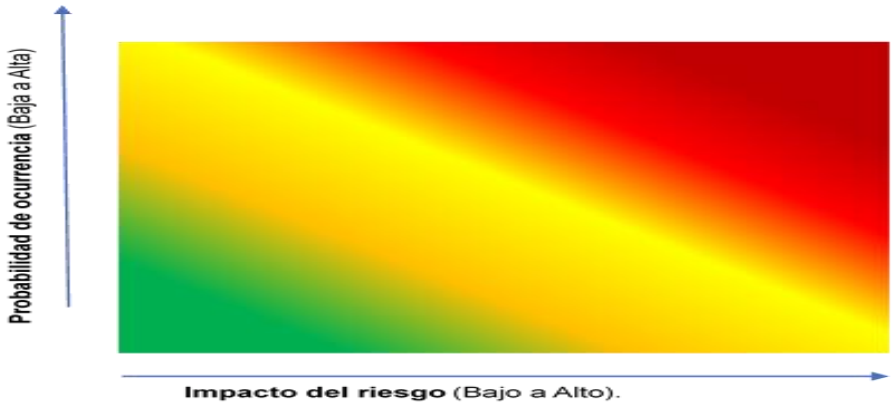
El proceso emplea técnicas de análisis de escenarios y correlación de riesgos, alineadas con la Sección 2 “Técnicas específicas” del Libro III de MAGERIT v3, para mapear interdependencias entre activos, como la relación entre plataformas de modelado climático (Apartado 2.3.3.2) y sistemas de respaldo (Apartado 2.3.3.7). Por ejemplo, una interrupción en los sistemas de respaldo

por sabotaje físico (Sección 5.4.4. [A.6] Abuso de privilegios de acceso del Libro II de MAGERIT v3) podría amplificar el impacto de un ataque a las plataformas de modelado, comprometiendo la disponibilidad de datos y retrasando análisis críticos. Los riesgos se documentan en una matriz de evaluación, descrita en la Sección 5.3.3.1, que asigna niveles de severidad (bajo, medio, alto) según criterios definidos en el Apartado 3.1. Este análisis prioriza los riesgos que afectan activos de alta sensibilidad, proporcionando una base para el diseño de controles en la Sección 6 (Fase Hacer) y la mejora continua en la Sección 8 (Fase Actuar).

5.3.3.1 Matriz de Evaluación de Riesgos.

Figura 10

Matriz de Evaluación de Riesgos por Probabilidad e Impacto



Fuente: Adaptado de ISO 31000:2018

La matriz de evaluación es una herramienta que permite representar de forma estructurada la combinación entre la probabilidad de ocurrencia de un evento y el impacto potencial asociado, facilitando una lectura gráfica del nivel de riesgo. Esta representación permite priorizar las situaciones que requieren acciones inmediatas, y orientar la planificación de controles conforme a la criticidad de cada activo.

La Figura 5 presenta esta matriz, basada en los lineamientos de la ISO 31000:2018 – Sección 6.4.3 “Análisis del riesgo”, que establece el uso de escalas para estimar tanto la magnitud del impacto como la probabilidad, combinándolas para definir el nivel de riesgo resultante.

- El eje horizontal (X) representa los niveles de impacto, ordenados de bajo a alto.
- El eje vertical (Y) representa la probabilidad de ocurrencia, también en escala ascendente.

- Las zonas de color indican los niveles de riesgo resultante:
    - Verde (bajo): Riesgos aceptables, sin necesidad de intervención inmediata.
    - Naranja (medio): Riesgos moderados que deben gestionarse mediante acciones proporcionales.
    - Rojo (alto a extremo): Riesgos no tolerables que requieren acciones correctivas inmediatas o controles compensatorios.

Este enfoque se complementa con los criterios descritos en MAGERIT v3 – Libro I, Sección 4.2.3 “Criterios”, donde se propone establecer umbrales combinados de impacto y probabilidad para interpretar los valores de riesgo y priorizar decisiones de tratamiento.

5.3.4 *Determinación de los Niveles de Riesgo.*

Con base en el análisis de riesgos, se clasifica los riesgos según su severidad para priorizar las acciones de mitigación en los proyectos de investigación medioambiental. El proceso establece una jerarquía de riesgos considerando su probabilidad de ocurrencia y su impacto potencial, asegurando que los recursos de seguridad se asignen proporcionalmente a la protección de los activos clasificados en la Sección 5.2 (Identificación y Clasificación de Activos de Información en Entornos Distribuidos). La metodología se alinea con el Apartado 6.4.4 (Evaluación del riesgo, ISO 31000:2018), que describe la clasificación de riesgos; la Sección 7.4 (Valoración de riesgo de seguridad de la información, ISO/IEC 27005:2022), que detalla métodos cualitativos; el Control RA-3 (Evaluación de Riesgos, NIST SP 800-53 Rev. 5), que promueve un enfoque sistemático; y el MAR.42 "Estimación del riesgo", MAGERIT v3 Libro I, Esta sección describe la fase final del análisis de riesgos, donde se consolidan los resultados de valoración de activos, amenazas e impacto para determinar el nivel de riesgo asociado, utilizando herramientas cualitativas o cuantitativas según la naturaleza del sistema evaluado. Los resultados orientan la selección de controles en la Sección 5.3.5, el diseño en la Sección 6 (Fase Hacer), y la auditoría en la Sección 7 (Fase Verificar).

La determinación de niveles de riesgo integra la probabilidad de las amenazas (Sección 5.3.1) y los impactos estimados (Sección 5.3.2), utilizando una escala cualitativa de cinco niveles para probabilidad (muy baja, baja, media, alta, muy alta) y cuatro para impacto (insignificante,

moderado, grave, catastrófico). La probabilidad se evalúa considerando la frecuencia de incidentes históricos, la exposición de activos en entornos remotos (Sección 1.1, Planteamiento del Problema), y vulnerabilidades como la suplantación de identidad (Sección 5.4.3 [A.5], Suplantación de la identidad del usuario, MAGERIT v3 Libro II:2012), que permite accesos no autorizados en sistemas sin cifrado adecuado, conforme al Apartado 2.3.3 (Infraestructura tecnológica en proyectos de investigación). El impacto abarca confidencialidad, integridad, disponibilidad, y efectos ambientales, legales, y reputacionales, según el Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles). El nivel de riesgo se calcula multiplicando los valores de probabilidad (1-5) e impacto (1-4), generando un rango de 1 a 20, clasificado en cuatro categorías: bajo (1-4), medio (5-8), alto (9-12), crítico (13-20), validado por partes interesadas (Apartado 2.4, Gobierno y Gestión Estratégica de la Información).

Por ejemplo, la intercepción de datos en estaciones meteorológicas (Apartado 2.3.3.1, Infraestructura de Captura y Adquisición de Datos) tiene una probabilidad alta (4) debido a la falta de cifrado en áreas remotas y un impacto catastrófico (4) por la interrupción de estudios climáticos (Sección 5.2.4.2, Datos Ambientales), resultando en un nivel de riesgo crítico (16), que podría incumplir el Apartado 2.7.2 (Leyes). En contraste, un error de configuración en plataformas en la nube (Apartado 2.3.3.3, Infraestructura de Almacenamiento y Procesamiento) tiene una probabilidad media (3) y un impacto moderado (2), generando un nivel de riesgo medio (6). Estos niveles se consolidan en la matriz de evaluación (Sección 5.3.3.1, Matriz de Evaluación de Riesgos), documentada en la [Insertar Tabla 8: Análisis de Riesgos y Amenazas - Clasifica riesgos según probabilidad e impacto, priorizando activos sensibles]. Este proceso, alineado con las particularidades Multi-Actor (Apartado 3.2, Características Particulares de los Proyectos Medioambientales) y principios de gobernanza (Apartado 5, Principios de gobernanza, ISO/IEC 38500:2024), asegura una gestión efectiva de los riesgos, priorizando datos de biodiversidad y equipamiento crítico para el tratamiento en la Sección 5.3.5 y la mejora continua en la Sección 8 (Fase Actuar).

5.3.5 *Tratamiento del Riesgo y Selección de Controles*

Basándose en los niveles de riesgo determinados, se define estrategias de tratamiento para mitigar los riesgos críticos y altos identificados en los proyectos de investigación, seleccionando

controles proporcionales a la protección de los activos clasificados en la Sección 5.2 (Identificación y Clasificación de Activos de Información en Entornos Distribuidos). La metodología se alinea con el Apartado 6.5 (Tratamiento del riesgo, ISO 31000:2018), que describe opciones de mitigación; la Sección 8 (Proceso de Tratamiento del riesgo de seguridad de la información, ISO/IEC 27005), que detalla la selección de controles; el Control RA-5 (Monitoreo y Escaneo de Vulnerabilidades, NIST SP 800-53 Rev. 5), que promueve medidas técnicas; y el Libro I, Sección 4.1 (Conceptos, MAGERIT v3), que estructura el tratamiento de riesgos. Los resultados orientan el diseño de medidas en la Sección 6 (Fase Hacer), la auditoría en la Sección 7 (Fase Verificar), y la mejora continua en la Sección 8 (Fase Actuar).

El tratamiento de riesgos prioriza la mitigación para riesgos clasificados como críticos, considerando también opciones como eliminación, transferencia o aceptación. La selección de controles se fundamenta en los capítulos 5 a 8 de ISO/IEC 27002:2022, los cuales agrupan controles organizativos, de personas, físicos y tecnológicos; y en la Sección 6 "Salvaguardas" del Libro II de MAGERIT v3:2012, que propone medidas específicas alineadas con las amenazas identificadas. La efectividad de los controles se evalúa con criterios de reducción del riesgo, aplicando métricas como CVSS, y asegurando su viabilidad técnica, compatibilidad operativa y alineación con las condiciones de gobernanza descritas en el Apartado 2.4 "Gobierno y Gestión Estratégica de la Información" y las particularidades Multi-Actor del Apartado 3.2 "Características Particulares de los Proyectos Medioambientales".

Por ejemplo, para mitigar el riesgo crítico de intercepción de datos en estaciones meteorológicas (Apartado 2.3.3.1, Infraestructura de Captura y Adquisición de Datos), con probabilidad alta e impacto catastrófico (Sección 5.3.4), se selecciona el control 8.24 "Uso de la criptografía" de ISO/IEC 27002:2022, implementando cifrado AES-256 para proteger la confidencialidad de los datos transmitidos (Sección 5.2.4.2, Datos Ambientales). Este control reduce el riesgo a nivel medio, minimizando posibles incumplimientos regulatorios asociados al Apartado 2.7.2 "Leyes".

En caso de riesgo medio, como errores de configuración en plataformas en la nube (Apartado 2.3.3.3, Infraestructura de Almacenamiento y Procesamiento), se selecciona el control 6.5 "Protección de las aplicaciones (software)" del Libro II de MAGERIT v3:2012, que establece auditorías de seguridad y requisitos para configuraciones seguras. Esta medida atiende

vulnerabilidades como las descritas en la Sección 5.3.4 [E.4] "Errores de configuración" del mismo catálogo.

5.4 Requisitos de Seguridad y Riesgo Residual

La determinación de requisitos de seguridad y la evaluación del riesgo residual conforman un componente clave del modelo de seguridad propuesto, diseñado para mitigar los riesgos identificados y asegurar la protección de los activos de información conforme a su nivel de criticidad. Este proceso conceptual se fundamenta en (8.2 " Evaluación de riesgos de seguridad de la información" de ISO/IEC 27001:2022), que establece la necesidad de definir requisitos específicos para abordar los riesgos, y en (MAGERIT v3 Libro II, A4.4. Estado de riesgo, que orienta la evaluación del riesgo tras la aplicación de controles.

El objetivo de esta sección es definir los requisitos de seguridad específicos necesarios para reducir los niveles de riesgo clasificados, considerando las amenazas, la sensibilidad de los activos, y las normativas aplicables. También, se aborda la evaluación conceptual del riesgo residual para determinar si los controles propuestos son suficientes o si requieren medidas adicionales, buscando asegurar que el modelo sea proporcional a las necesidades reales de protección en el entorno operativo de los proyectos de investigación ambiental.

5.4.1 Identificación de Requisitos de Seguridad

La identificación de los requisitos de seguridad en el diseño conceptual del modelo constituye el paso siguiente al análisis de riesgos. Se trata de determinar las medidas de seguridad necesarias para mitigar los riesgos identificados en la Sección 5.3 y proteger los activos de información clasificados en la Sección 5.2. Estos requisitos se derivan del nivel de riesgo inherente y de los objetivos de tratamiento de riesgos establecidos. Se considera la naturaleza de las amenazas, la sensibilidad de los datos y activos, y las obligaciones de cumplimiento normativo y legal relevantes para los proyectos de investigación medioambiental. (8.2 " Evaluación de riesgos de seguridad de la información" de ISO/IEC 27001:2022) y (8 "Proceso de tratamiento de riesgo de seguridad de la información" de ISO/IEC 27005:2022) orientan este proceso al vincular la evaluación de riesgos con la definición de controles y requisitos para su mitigación. El objetivo de

esta etapa conceptual es definir las categorías y tipos de requisitos de seguridad que servirán de base para la selección y especificación de controles en la siguiente fase del diseño.

5.4.2 Evaluación Conceptual del Riesgo Residual

La evaluación conceptual del riesgo residual se aborda una vez que se han definido los requisitos de seguridad y se han considerado los controles que se propondrán en el diseño para satisfacer dichos requisitos. Este proceso, orientado por (MAGERIT v3 Libro II, A4.4. Estado de riesgo, consiste en una apreciación teórica del nivel de riesgo que se esperaría subsistir después de la implementación efectiva de las medidas de seguridad diseñadas. No se trata de una medición real del riesgo operativo, sino de una valoración conceptual basada en la eficacia esperada de los controles definidos en el modelo. El objetivo es determinar, a nivel de diseño, si la combinación de requisitos y controles conceptualmente propuestos parece reducir los riesgos a un nivel aceptable. Si la evaluación conceptual sugiere que el riesgo residual sería demasiado elevado, esto indicaría la necesidad de revisar y fortalecer el diseño del modelo, añadiendo o ajustando requisitos y controles, lo cual se alinearía con los principios de la fase Actuar (Sección 8).

5.4 Análisis Avanzado de Amenazas

Con base en el marco de gestión de riesgos establecido, se desarrolla un análisis avanzado de amenazas específicas que comprometen los activos de información clasificados en la Sección 5.2 (Identificación y Clasificación de Activos de Información en Entornos Distribuidos), empleando inteligencia de amenazas para caracterizar fuentes externas e internas, sus motivaciones, capacidades, métodos de explotación, y priorización en el contexto de proyectos de investigación medioambiental. Este proceso complementa la identificación de amenazas (5.3.1), evaluación de impacto (5.3.2), análisis de riesgos (5.3.3), determinación de niveles de riesgo (5.3.4), y tratamiento (5.3.5) al centrarse en la caracterización detallada de actores, patrones de ataque, y tendencias emergentes, evitando la repetición de procesos generales de evaluación de riesgos. La metodología se estructura en cinco fases: (1) recopilación de datos de inteligencia mediante fuentes verificadas, como bases de datos de vulnerabilidades (ej., CVE) y reportes sectoriales de ciberataques; (2) correlación de incidentes históricos y análisis de campañas de ataque utilizando herramientas de gestión de eventos e información de seguridad (SIEM); (3) caracterización de fuentes, motivaciones, y capacidades empleando Frameworks como MITRE

ATT&CK para mapear tácticas y técnicas; (4) priorización de amenazas críticas basada en métricas como el Common Vulnerability Scoring System (CVSS) y severidad potencial; y (5) generación de perfiles de amenaza estandarizados que documentan actor, motivación, método, impacto, y probabilidad. Esta metodología se fundamenta en el Apartado 6.4.2 (Identificación del riesgo, ISO 31000:2018), que estructura la detección sistemática de amenazas a través de análisis detallado; la Sección 7.2 (Identificación de riesgos de seguridad de la información, ISO/IEC 27005:2022), que detalla técnicas de inteligencia de amenazas, como modelado de actores y correlación de datos, para caracterizar fuentes; el Control RA-3 (Evaluación de Riesgos, NIST SP 800-53 Rev. 5:2020), que promueve un enfoque estructurado para priorizar amenazas mediante inteligencia integral; y la Sección 5 (Amenazas, MAGERIT v3 Libro II), que clasifica amenazas tecnológicas, humanas, y físicas relevantes para los activos del proyecto. El análisis se basa en el entorno Multi-Actor descrito en la Sección 1.1 (Planteamiento del Problema), que destaca la colaboración entre universidades, gobiernos, y comunidades, aumentando riesgos como accesos no autorizados por actores externos o errores internos por falta de capacitación. También considera la infraestructura tecnológica distribuida del Apartado 2.3.3 (Infraestructura tecnológica en proyectos de investigación), con estaciones meteorológicas remotas y sistemas de almacenamiento en la nube expuestos a ataques debido a su operación en entornos remotos, y la sensibilidad de los datos científicos del Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), como registros de especies protegidas y datos de temperatura en tiempo real, que requieren protección contra amenazas avanzadas. Por ejemplo, un actor externo motivado por lucro podría desplegar Ransomware contra una base de datos científica (Apartado 2.3.3.4, Infraestructura de Análisis y Visualización), explotando vulnerabilidades que permiten la Sección 5.4.13 [A.17] (Modificación deliberada de la información, MAGERIT v3 Libro II), comprometiendo registros de avistamientos de especies protegidas (Sección 5.2.4.2, Datos Ambientales) y generando implicaciones legales por incumplimiento de la Ley 1581 de 2012 (Apartado 2.7.2, Leyes). Este análisis se alinea con los principios de gobernanza de la información descritos en el Apartado 2.4 (Gobierno y Gestión Estratégica de la Información), que enfatiza la asignación de responsabilidades para gestionar riesgos de manera coordinada, y el Apartado 5 (Principios de gobernanza, ISO/IEC 38500:2024), que promueve la evaluación estratégica de amenazas para garantizar la continuidad operativa en entornos complejos (Apartado 3.2, Características Particulares de los Proyectos Medioambientales). Los perfiles de amenaza generados,

documentados en formatos estructurados, proporcionan insumos clave para refinar la planificación de controles avanzados en la Sección 6 (Fase Hacer), orientar auditorías especializadas en la Sección 7 (Fase Verificar), y facilitar la mejora continua en la Sección 8 (Fase Actuar).

5.4.1 *Caracterización de Fuentes de Amenazas*

Con base en el análisis avanzado de amenazas iniciado, esta subsección caracteriza las fuentes de amenazas externas (ej., actores maliciosos, desastres naturales) e internas (ej., errores humanos, fallos técnicos) que comprometen los activos de información clasificados en la Sección 5.2 (Identificación y Clasificación de Activos de Información en Entornos Distribuidos), empleando inteligencia de amenazas para mapear su origen, motivaciones, y capacidades operativas. Este proceso complementa la identificación general de amenazas de la Sección 5.3.1 al profundizar en la caracterización detallada de actores y sus patrones de ataque, evitando la repetición de los análisis de impacto o niveles de riesgo de las Secciones 5.3.2 y 5.3.4. La metodología se estructura en tres fases: (1) recopilación de datos de inteligencia mediante fuentes verificadas, como bases de datos de vulnerabilidades (ej., Common Vulnerabilities and Exposures, CVE), reportes sectoriales de ciberataques, y registros internos de incidentes técnicos obtenidos de la infraestructura del proyecto (Apartado 2.3.3, Infraestructura tecnológica en proyectos de investigación); (2) análisis de correlación de incidentes históricos utilizando herramientas de gestión de eventos e información de seguridad (SIEM) para identificar patrones de ataque recurrentes; y (3) clasificación de fuentes según su origen (externo o interno), motivación (ej., lucro, sabotaje, espionaje), y capacidad técnica (ej., disponibilidad de herramientas de explotación, conocimientos especializados). Esta metodología se fundamenta en la Sección 7.2 (Identificación de riesgos de seguridad de la información, ISO/IEC 27005:2022), que promueve el uso de técnicas de inteligencia de amenazas, como la correlación de datos y el análisis de actores, para detectar y clasificar fuentes de riesgo, y la Sección 5 (Amenazas, MAGERIT v3 Libro II), que proporciona un catálogo detallado de amenazas externas, como ciberataques, e internas, como errores operativos, estructurando su clasificación según el contexto del proyecto. El análisis se basa en el entorno Multi-Actor descrito en la Sección 1.1 (Planteamiento del Problema), que destaca la colaboración entre universidades, gobiernos, y comunidades, lo que incrementa riesgos como accesos no autorizados por actores externos o errores humanos derivados de la falta de

coordinación. También considera la infraestructura tecnológica distribuida del Apartado 2.3.3, que incluye sistemas como bases de datos científicas y estaciones meteorológicas remotas, expuestos a amenazas debido a su operación en entornos remotos, y la sensibilidad de los datos científicos del Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), como registros de biodiversidad, que requieren protección contra ataques dirigidos. Por ejemplo, actores externos motivados por lucro podrían lanzar campañas de Ransomware contra una base de datos científica (Apartado 2.3.3.4, Infraestructura de Análisis y Visualización), explotando vulnerabilidades que permiten la Sección 5.4.13 [A.15] (Modificación deliberada de la información, MAGERIT v3 Libro II), comprometiendo registros de especies protegidas (Sección 5.2.4.2, Datos Ambientales) y afectando la conservación ambiental (Apartado 3.2, Características Particulares de los Proyectos Medioambientales). Asimismo, errores internos de configuración por personal no capacitado en sistemas de almacenamiento (Apartado 2.3.3.5, Infraestructura de Almacenamiento y Procesamiento) podrían exponer datos climáticos, generando riesgos legales por incumplimiento de normativas (Apartado 2.7.2, Leyes). El uso del Framework MITRE ATT&CK en el análisis es pertinente, ya que sus tácticas, técnicas, y procedimientos (TTPs) permiten mapear con precisión las capacidades de actores avanzados, como aquellos que ejecutan Ransomware o ingeniería social, alineándose con el contexto de amenazas persistentes en proyectos tecnológicos distribuidos (Apartado 2.3.3). Esta caracterización se alinea con los principios de gobernanza de la información descritos en el Apartado 2.4 (Gobierno y Gestión Estratégica de la Información), que enfatiza la asignación de responsabilidades para gestionar riesgos de manera coordinada, y el Apartado 5 (Principios de gobernanza, ISO/IEC 38500:2024), que promueve la evaluación estratégica de fuentes de amenazas para garantizar la continuidad operativa. Los patrones de amenaza identificados proporcionan insumos clave para el perfilado de motivaciones y capacidades en la Sección 5.4.1.1 y para la planificación de controles específicos en la Sección 6 (Fase Hacer).

5.4.1.1 Perfilado de Motivaciones y Capacidades.

Con base en la caracterización de fuentes de amenazas, esta subsección mejora aún más el análisis al perfilar las motivaciones (ej., lucro, sabotaje, espionaje) y capacidades técnicas (ej., herramientas de explotación, conocimientos especializados) de los actores externos e internos que amenazan los activos de información clasificados en la Sección 5.2 (Identificación y Clasificación

de Activos de Información en Entornos Distribuidos). Este proceso profundiza en las intenciones y recursos de los actores, complementando la identificación general de amenazas de la Sección 5.3.1 y la caracterización de fuentes de la Sección 5.4.1, al tiempo que se distingue de los procesos de evaluación de impacto y clasificación de riesgos de otras secciones. La metodología se estructura en tres fases: (1) recopilación de datos de inteligencia a partir de fuentes verificadas, como reportes de Ciberinteligencia (ej., bases de datos CVE), registros de eventos del sistema de la infraestructura tecnológica (Apartado 2.3.3, Infraestructura tecnológica en proyectos de investigación), y entrevistas con responsables de seguridad (Apartado 2.4, Gobierno y Gestión Estratégica de la Información); (2) análisis de motivaciones mediante modelos de comportamiento, utilizando el Framework MITRE ATT&CK para mapear tácticas, técnicas, y procedimientos (TTPs) específicos de los actores; y (3) evaluación de capacidades técnicas, considerando la disponibilidad de Exploits, conocimientos especializados, o infraestructura de ataque. Esta metodología se fundamenta en la Sección 2 (Técnicas específicas, MAGERIT v3 Libro III), que describe técnicas de análisis de actores, como correlación de datos y modelado de amenazas, para identificar intenciones y recursos, y la Sección 7.2 (Identificación de riesgos de seguridad de la información, ISO/IEC 27005:2022), que promueve el perfilado detallado de actores para anticipar patrones de ataque. El framework MITRE ATT&CK es pertinente porque sus TTPs permiten identificar con precisión las capacidades de actores avanzados, como aquellos que ejecutan campañas de ingeniería social o explotación de vulnerabilidades, alineándose con las amenazas persistentes en entornos tecnológicos distribuidos (Apartado 2.3.3). El perfilado se basa en el entorno Multi-Actor descrito en la Sección 1.1 (Planteamiento del Problema), que destaca la colaboración entre universidades, gobiernos, y comunidades, incrementando riesgos como ataques dirigidos por actores externos o errores internos por falta de capacitación, y en la sensibilidad de los datos científicos del Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), como registros de biodiversidad y proyecciones climáticas, que son objetivos de ataques sofisticados. Por ejemplo, un actor malicioso motivado por lucro podría explotar vulnerabilidades en plataformas de modelado climático (Apartado 2.3.3.2, Sistemas de modelado climático) mediante campañas de ingeniería social, alineadas con tácticas identificadas en el Framework MITRE ATT&CK, que permiten la Sección 5.4.13 [A.15] (Modificación deliberada de la información, MAGERIT v3 Libro II), distorsionando proyecciones climáticas (Sección 5.2.4.2, Datos Ambientales) y afectando decisiones de gestión ambiental (Apartado 3.2,

Características Particulares de los Proyectos Medioambientales). De manera similar, un actor interno con acceso privilegiado y motivación de sabotaje podría introducir configuraciones erróneas en sistemas de almacenamiento (Apartado 2.3.3.5, Infraestructura de Almacenamiento y Procesamiento), exponiendo datos climáticos y generando riesgos legales por incumplimiento de normativas (Apartado 2.7.2, Leyes). Este perfilado se alinea con los principios de gobernanza de la información descritos en el Apartado 2.4, que enfatiza la asignación de responsabilidades para gestionar riesgos de manera coordinada, y el Apartado 5 (Principios de gobernanza de TI, ISO/IEC 38500:2024), que promueve la evaluación estratégica de actores para garantizar la continuidad operativa. Los perfiles generados proporcionan insumos clave para la identificación de métodos de explotación en la Sección 5.4.2 y para la planificación de auditorías especializadas en la Sección 7 (Fase Verificar).

5.4.2 *Análisis de Métodos de Explotación*

Con base en los perfiles de motivaciones y capacidades de los actores identificados, se examina los métodos de explotación utilizados por las fuentes de amenazas para comprometer los activos de información clasificados en la Sección 5.2 (Identificación y Clasificación de Activos de Información en Entornos Distribuidos), detallando técnicas como ataques cibernéticos, sabotaje físico, y errores operativos. Este análisis profundiza en los vectores de ataque específicos, complementando la caracterización de fuentes de la Sección 5.4.1 y la identificación general de amenazas de la Sección 5.3.1, sin solaparse con los procesos de evaluación de impacto (5.3.2) o clasificación de riesgos (5.3.4). La metodología se estructura en cuatro fases: (1) mapeo de vectores de ataque, identificando puntos de entrada en la infraestructura tecnológica (ej., interfaces de red, dispositivos físicos); (2) evaluación de técnicas de explotación mediante el Framework MITRE ATT&CK, que clasifica tácticas como acceso inicial, ejecución, o persistencia; (3) correlación con vulnerabilidades identificadas en la Sección 5.3.1, utilizando herramientas de escaneo como Nessus para detectar configuraciones débiles; y (4) documentación de métodos mediante diagramas de ataque, como árboles de ataque descritos en la Sección 2 (Técnicas específicas, MAGERIT v3 Libro III). Esta metodología se fundamenta en la Sección 5 (Amenazas, MAGERIT v3 Libro II), que cataloga métodos de ataque como denegación de servicio y sabotaje físico, y el Control RA-3 (Evaluación de riesgos, NIST SP 800-53 Rev. 5), que promueve el análisis

estructurado de vectores para anticipar Exploits. El Framework MITRE ATT&CK es pertinente porque sus tácticas y técnicas permiten mapear métodos de explotación avanzados, como ataques de denegación de servicio o ingeniería social, alineándose con las amenazas en entornos tecnológicos distribuidos (Apartado 2.3.3). El análisis se basa en el entorno Multi-Actor de la Sección 1.1 (Planteamiento del Problema), que incrementa riesgos debido a la colaboración entre universidades, gobiernos, y comunidades, y en la infraestructura tecnológica distribuida del Apartado 2.3.3, que incluye sistemas vulnerables por su exposición remota. También considera la sensibilidad de los datos científicos del Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), como datos climáticos, que son objetivos de ataques dirigidos. Por ejemplo, un ataque de denegación de servicio podría dirigirse a sistemas de almacenamiento distribuido (Apartado 2.3.3.5, Infraestructura de Almacenamiento y Procesamiento), explotando la falta de segmentación de red identificada mediante escaneos de vulnerabilidades, interrumpiendo la disponibilidad de datos climáticos (Sección 5.2.4.2, Datos Ambientales) y afectando respuestas a emergencias ambientales (Apartado 3.2, Características Particulares de los Proyectos Medioambientales). De manera similar, un sabotaje físico a sistemas de respaldo (Apartado 2.3.3.7, Infraestructura de Almacenamiento y Procesamiento) podría dañar dispositivos críticos, comprometiendo la continuidad operativa y generando riesgos legales (Apartado 2.7.2, Leyes). Este análisis se alinea con los principios de gobernanza de la información del Apartado 2.4 (Gobierno y Gestión Estratégica de la Información), que enfatiza la gestión coordinada de riesgos, y el Apartado 5 (Principios de gobernanza de TI, ISO/IEC 38500:2024), que promueve la evaluación estratégica de métodos de ataque. Los métodos identificados proporcionan insumos clave para la priorización de amenazas en la Sección 5.4.3 y para la planificación de controles técnicos en la Sección 6 (Fase Hacer).

5.4.3 *Priorización de Amenazas Críticas*

Con base en los perfiles de motivaciones y capacidades de los actores delineados en la Sección 5.4.1.1 (Perfilado de Motivaciones y Capacidades) y los métodos de explotación examinados en la Sección 5.4.2 (Análisis de Métodos de Explotación), esta subsección clasifica las amenazas críticas según su probabilidad de ocurrencia y severidad potencial, identificando aquellas que requieren atención inmediata en proyectos de investigación medioambiental. Este

proceso complementa el análisis de riesgos de la Sección 5.3.3 (Análisis de Riesgos), diferenciándose del proceso de determinación de niveles de riesgo descrito en la Sección 5.3.4 (Determinación de los Niveles de Riesgo) al enfocarse en la priorización de amenazas específicas mediante inteligencia de amenazas. La metodología se estructura en cuatro fases conceptuales, diseñadas para garantizar una priorización sistemática: (1) evaluación de la probabilidad de ocurrencia, transformando datos de inteligencia, como la frecuencia de ataques en el sector medioambiental obtenida de bases como Exploit-DB, en una escala cualitativa de cinco niveles (muy baja a muy alta), basada en el modelo de evaluación cualitativa de la Sección 6.4.3 (Criterios para realizar evaluaciones de riesgos de seguridad de la información, ISO/IEC 27005), mediante análisis estadístico de tendencias sectoriales, ponderando factores como la exposición de sistemas remotos (Apartado 2.3.3, Infraestructura tecnológica en proyectos de investigación) y las capacidades de los actores (Sección 5.4.1.1); (2) estimación de la severidad, evaluando impactos legales, ambientales y reputacionales mediante escalas cualitativas (insignificante a catastrófico) y cuantitativas (costos estimados en pérdidas operativas, multas, o daños ecológicos), adaptadas del Libro I, Sección 3.1.3 (Determinación del impacto potencial, MAGERIT v3), que clasifica el impacto en dominios funcionales (económico, operativo, reputacional, legal), considerando la sensibilidad de datos científicos (Apartado 3.1, Clasificación y Protección de Datos Medioambientales Sensibles); (3) clasificación en categorías de alta, media y baja prioridad, empleando matrices de riesgo adaptadas al contexto del proyecto, combinando probabilidad e impacto en una escala de nueve niveles (3x3); y (4) validación con partes interesadas (Apartado 2.4, Gobierno y Gestión Estratégica de la Información), utilizando dinámicas participativas donde se discuten casos de amenazas priorizadas en talleres con representantes de universidades, gobiernos y comunidades, contrastándolos con criterios de aceptación de riesgos definidos en la Sección 5.3.4, y documentando ajustes en la matriz de priorización, como la reclasificación de amenazas marginales o la redefinición de umbrales críticos, con base en consenso informado para reducir sesgos técnicos. Esta metodología se apoya en la Sección 6.4.3 (Criterios para realizar evaluaciones de riesgos de seguridad de la información, ISO/IEC 27005), que establece las bases para definir probabilidad e impacto, orientando la evaluación y clasificación, y el Libro I, Sección 3.1.3 (Determinación del impacto potencial, MAGERIT v3), que proporciona una taxonomía para evaluar impactos multidimensionales. Los controles técnicos se derivan de la Cláusula 8 de ISO/IEC 27002, que detalla medidas específicas para mitigar riesgos identificados. El análisis se

basa en el entorno Multi-Actor de la Sección 1.1 (Planteamiento del Problema), que incrementa la probabilidad de ataques dirigidos debido a la colaboración entre diversas entidades, y en la sensibilidad de los datos del Apartado 3.1, como registros de biodiversidad y proyecciones climáticas.

Las siguientes amenazas ilustran la priorización:

- Amenaza: Manipulación de datos climáticos (Sección 5.2.4.2, Datos Ambientales) mediante accesos no autorizados 5.4.9. [A.11] Acceso no autorizado del catálogo de amenazas, MAGERIT v3 Libro II).
- Causa: Exposición de sistemas remotos (Apartado 2.3.3). Probabilidad: Alta, por la frecuencia de ataques similares. Impacto: Legal severo por incumplimiento de normativas (Apartado 2.7.2, Leyes) y ambiental por distorsión de modelos predictivos (Apartado 3.2, Características Particulares de los Proyectos Medioambientales). Medida: Separación de redes (8.22 Segregación en redes, ISO/IEC 27002).
- Amenaza: Ransomware en bases de datos científicas (Apartado 2.3.3.4, Infraestructura de Análisis y Visualización). Causa: Explotabilidad de vulnerabilidades ([A.15] Modificación deliberada de la información, Sección 5.4.13 del catálogo de amenazas, MAGERIT v3 Libro II). Probabilidad: Alta, por vulnerabilidades conocidas. Impacto: Afectación a la conservación de especies (Sección 5.2.4.2) y riesgos reputacionales.
  Medida: Implementación de controles criptográficos robustos conforme al (Control 8.24 "Uso de la criptografía", ISO/IEC 27002:2022).

Esta priorización se alinea con los principios de gobernanza del Apartado 2.4, que promueve la gestión estratégica de riesgos, y el Apartado 5 (Principios para la gobernanza de TI, ISO/IEC 38500), que fomenta la evaluación proactiva de amenazas. Las amenazas priorizadas orientan la planificación de controles técnicos en la Sección 6 (Fase Hacer), conforme a los principios de defensa en profundidad y a controles establecidos en la Cláusula 8 de ISO/IEC 27002,

como el uso de la criptografía (Control 8.24 “Uso de la criptografía”) y la separación de redes (Control 8.22 Segregación en redes) de ISO/IEC 27002:2022.

5.4.4 *Generación de Perfiles de Amenaza*

Esta subsección consolida los análisis de fuentes de amenazas (Sección 5.4.1, Caracterización de Fuentes de Amenazas), motivaciones y capacidades (Sección 5.4.1.1, Perfilado de Motivaciones y Capacidades), métodos de explotación (Sección 5.4.2, Análisis de Métodos de Explotación), y priorización de amenazas críticas (Sección 5.4.3, Priorización de Amenazas Críticas) para elaborar perfiles de amenaza detallados. Estos perfiles organizan datos de importancia sobre actores, motivaciones, capacidades, métodos de explotación, probabilidad e impacto en un marco estructurado, proporcionando una base operativa para mitigar riesgos en proyectos de investigación medioambiental. El proceso culmina el análisis avanzado de la Sección 5.4 (Análisis Avanzado de Amenazas), integrando los hallazgos previos y diferenciándose del análisis general de riesgos de la Sección 5.3.3 (Análisis de Riesgos) y la selección de controles de la Sección 5.3.5 (Tratamiento del Riesgo y Selección de Controles) al centrarse en la documentación estructurada de amenazas críticas mediante inteligencia de amenazas.

La metodología se estructura en tres fases secuenciales para generar perfiles operativos:

- Integración de datos de inteligencia: Se recopilan reportes de ciberataques, registros de eventos del sistema provenientes de la infraestructura tecnológica (Apartado 2.3.3, Infraestructura tecnológica en proyectos de investigación), y resultados de las secciones 5.4.1 a 5.4.3. Sistemas de gestión de eventos e información de seguridad (SIEM) correlacionan estos datos mediante análisis de tendencias y coincidencias, identificando patrones de ataque que conectan actores, métodos y activos comprometidos.
- Modelado de perfiles: Los datos integrados se estructuran utilizando el marco MITRE ATT&CK, que clasifica tácticas (ej., acceso inicial, ejecución), técnicas (ej., explotación de vulnerabilidades, phishing), y procedimientos específicos, alineando las capacidades (Sección 5.4.1.1) y métodos (Sección 5.4.2) para reflejar comportamientos reales de los actores en entornos distribuidos.

- Documentación estandarizada: Se elaboran perfiles que detallan actor (externo/interno), motivación (ej., lucro, sabotaje), capacidad (ej., exploits avanzados, acceso privilegiado), método de explotación, probabilidad (muy baja a muy alta, derivada de Sección 5.4.3), e impacto (legal, ambiental, reputacional), utilizando plantillas adaptadas del Libro I, Sección 3.2 (Formalización de las actividades, MAGERIT v3).

Esta metodología se sustenta en el Libro I, Sección 3.2 (Formalización de las actividades, MAGERIT v3), que establece un marco para documentar riesgos de manera estructurada, garantizando trazabilidad, y el Control RA-3 (Evaluación de riesgos, NIST SP 800-53 Rev. 5), que promueve la generación de perfiles de amenaza integrando inteligencia para modelar actores y métodos. El marco MITRE ATT&CK es pertinente porque sus tácticas, técnicas y procedimientos (TTPs) permiten caracterizar amenazas avanzadas con precisión en entornos tecnológicos distribuidos (Apartado 2.3.3), asegurando que los perfiles reflejen patrones de ataque reales.

El análisis se fundamenta en el entorno Multi-Actor descrito en la Sección 1.1 (Planteamiento del Problema), que incrementa la diversidad de actores debido a la colaboración entre universidades, gobiernos y comunidades, y en la sensibilidad de los datos científicos del Apartado 3.1 (Clasificación y Protección de Datos Medioambientales Sensibles), como registros de biodiversidad y proyecciones climáticas, que elevan los riesgos de ataques dirigidos. Los perfiles generados se alinean con los principios de confidencialidad, integridad y disponibilidad del Apartado 2.1.3 (Principios de Seguridad) y refuerzan la gestión estratégica de riesgos conforme al Apartado 2.4 (Gobierno y Gestión Estratégica de la Información) y al Apartado 5 (Principios para la gobernanza de TI, ISO/IEC 38500), que promueve la planificación proactiva para proteger activos críticos.

A continuación, se presentan dos perfiles de amenaza ilustrativos:

Perfil de Amenaza 1: Ransomware en Bases de Datos Científicas

- Actor: Externo, con alta capacidad técnica (Exploits avanzados).
- Motivación: Lucro.
- Método: Explotación de vulnerabilidades, empleando técnicas de ejecución (T1059 - Command and Scripting Interpreter) y persistencia (T1547 - Boot or Logon

Autostart Execution, MITRE ATT&CK), asociadas a [A.15] Modificación deliberada de la información (MAGERIT v3 Libro II).

- Probabilidad: Alta, debido a vulnerabilidades conocidas (Sección 5.4.3).
- Impacto: Interrupción de registros de especies protegidas (Sección 5.2.4.2, Datos Ambientales), sanciones por incumplimiento normativo (Apartado 2.7.2, Leyes).
- Medida técnica: Uso de criptografía (Control 8.24 8.24 Uso de la criptografía, ISO/IEC 27002) para proteger datos sensibles, integrado en el ciclo de vida de controles de la Sección 6 (Fase Hacer).

Perfil de Amenaza 2: Sabotaje Interno en Sistemas de Almacenamiento

- Actor: Interno, con acceso privilegiado.
- Motivación: Sabotaje.
- Método: Acceso no autorizado a través de configuraciones erróneas, explotando privilegios para alterar sistemas, asociado a [A.11] Acceso no autorizado (MAGERIT v3 Libro II).
- Probabilidad: Media, debido a deficiencias en controles de acceso (Sección 5.4.3).
- Impacto: Compromiso de datos climáticos (Sección 5.2.4.2), afectando la respuesta ante emergencias (Apartado 3.2, Características Particulares de los Proyectos Medioambientales).
- Medida técnica: Autenticación de la información (8.5 Autenticación segura, ISO/IEC 27002) para verificar la integridad de configuraciones y restringir accesos no autorizados, incorporado en el diseño de controles de la Sección 6 (Fase Hacer).

En la Tabla 8: Análisis de Riesgos y Amenazas se documenta perfiles de amenaza priorizados, detallando actor, motivación, capacidad, método, probabilidad, e impacto, consolidando la matriz de riesgos elaborada en la Sección 5.3.3 (Análisis de Riesgos), que mapea amenazas contra activos y niveles de riesgo]. Estos perfiles orientan el diseño de controles técnicos en la Sección 6 (Fase Hacer), integrándolos en el ciclo de vida de la gestión de riesgos para garantizar medidas proporcionales a las amenazas, y apoyan la mejora continua en la Sección 8 (Fase Actuar), fortaleciendo la resiliencia frente a riesgos críticos.

5.5 Planificar la formación y concienciación

La planificación de actividades de formación y concienciación en materia de seguridad de la información se integra de manera estructurada en el modelo de gestión de riesgos, fortaleciendo las capacidades organizacionales frente a las amenazas que explotan vulnerabilidades humanas. Esta fase respalda directamente el propósito del modelo de seguridad descrito a lo largo del documento, el cual es establecer un ecosistema de protección dinámico, adaptable y sostenido, que garantice la confidencialidad, integridad y disponibilidad de los activos de información.

El enfoque adoptado se encuentra alineado con las directrices de ISO/IEC 27001:2022, cláusula 7.2 "Competencia", y complementado por ISO/IEC 27002:2022, secciones 6.3 "Concienciación, educación y formación en seguridad de la información" y 6.4 "Proceso disciplinario ".

El desarrollo detallado de las actividades formativas se encuentra formalizado en el Anexo B: Plan de Capacitación en Seguridad de la Información, que especifica los contenidos, frecuencias, responsables y mecanismos de evaluación diseñados para su implementación.

5.5.1 *Objetivo del Programa*

El programa de formación y concienciación tiene como objetivos principales:

- Incrementar la sensibilidad del personal frente a los riesgos de seguridad de la información.
- Reforzar la protección de los activos críticos identificados en la sección 5.2.
- Contribuir a la mitigación de riesgos asociados a errores humanos, conforme al análisis desarrollado en las secciones 5.4 y 5.4.2.
- Promover la adopción sostenida de comportamientos seguros en el entorno organizacional.

5.5.2 *Estructura del Programa de Formación y Concienciación*

El programa contempla los siguientes componentes:

Segmentación de públicos objetivo: Identificación de grupos según su nivel de exposición y responsabilidad respecto a los activos de información.

Contenidos formativos: Elaboración de módulos

- Principios básicos de seguridad de la información.
- Detección de amenazas como phishing, malware e ingeniería social.
- Buenas prácticas de gestión de contraseñas, dispositivos y plataformas de almacenamiento.
- Procedimientos internos para la gestión de incidentes de seguridad.

Periodicidad: Realización de sesiones anuales de capacitación obligatoria, complementadas con actividades de refuerzo semestrales o ad-hoc en función de cambios tecnológicos o normativos relevantes.

Responsables: La planificación, ejecución y seguimiento del programa estarán a cargo del responsable de Seguridad de la Información, en coordinación con el área de Recursos Humanos.

Evaluación de efectividad: Aplicación de instrumentos de medición, incluyendo evaluaciones de conocimientos, encuestas de percepción de riesgos y análisis de tendencias de incidentes atribuibles a errores humanos.

5.5.3 *Relación con la Gestión de Riesgos*

La formación y concienciación se reconocen como medidas activas de tratamiento de riesgos, orientadas a reducir la probabilidad y el impacto de amenazas relacionadas con fallos humanos.
Esta consideración está alineada con lo expuesto en ISO/IEC 27005:2022, sección 7.3 " Análisis de los riesgos de seguridad de la información".

Su implementación contribuye de forma directa a la eficacia del sistema de control diseñado para proteger los activos críticos identificados, fortaleciendo la resiliencia operativa y la capacidad de respuesta ante incidentes.

5.5.4 *Ciclo de Mejora Continua*

Siguiendo los principios de mejora continua descritos en ISO 31000:2018, sección 5.7.2 "Mejora continua", el programa de formación será objeto de revisión periódica para:

- Adaptarse a nuevos escenarios de amenazas.
- Incorporar aprendizajes derivados de incidentes reales.
- Mejorar contenidos y metodologías de capacitación.
- Asegurar el cumplimiento actualizado de los requisitos normativos aplicables.

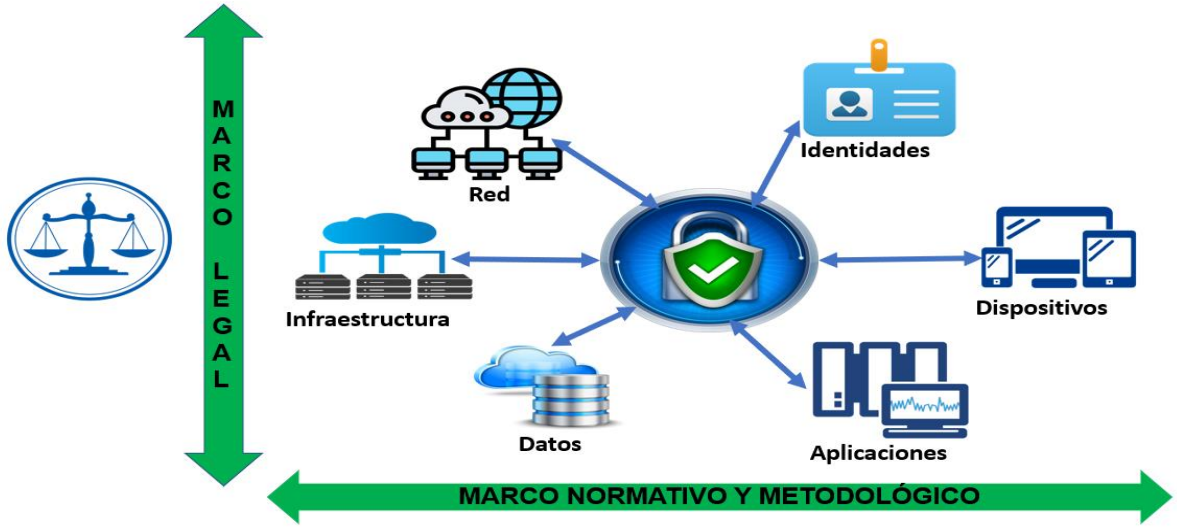
Todas las revisiones y actualizaciones serán documentadas en el **Anexo B** para su trazabilidad y control efectivo.

Nota: Para consultar el detalle específico de las actividades, contenidos formativos, responsables asignados y mecanismos de evaluación asociados al programa de formación y concienciación, se recomienda revisar el **Anexo B Plan de capacitación, sensibilización y comunicación de seguridad de la información**. Este anexo complementa la presente sección proporcionando una estructura operativa concreta que facilita la implementación y seguimiento de las acciones formativas planificadas.

5.6 Planificación de Políticas y Procedimientos

Figura 11

Vinculación de activos con el marco legal y metodológico



Fuente: Elaboración propia

La Figura 8 ilustra los dominios que deben ser abarcados por las políticas de seguridad diseñadas, destacando la necesidad de articular medidas específicas para identidades, dispositivos, redes, infraestructura, datos y aplicaciones, bajo los marcos legales y normativos considerados en este proyecto.

Esta subsección formaliza la planificación inicial de políticas de alto nivel y procedimientos operativos diseñados para mitigar los riesgos identificados en la Tabla 8: Análisis de Riesgos y Amenazas (Sección 5.3.1) y proteger los activos críticos listados en la Tabla 6: Identificación y Clasificación de Activos (Sección 5.2.5). Estas directrices estratégicas, que serán implementadas en la fase Hacer (Sección 6), responden a los desafíos operativos del entorno Multi-Actor (Sección 1.1, Planteamiento del Problema) y la heterogeneidad tecnológica (Apartado 2.3.3, Infraestructura tecnológica en proyectos de investigación), asegurando la confidencialidad, integridad y disponibilidad de datos sensibles (Apartado 3.1, Clasificación y Protección de Datos Medioambientales Sensibles). La planificación se alinea con la Sección 6.1 (Acciones para abordar

riesgos y oportunidades, ISO/IEC 27001) y la Sección 5.1 (Políticas para la seguridad de la información, ISO/IEC 27002), garantizando directrices claras y auditables.

La metodología para diseñar estas políticas y procedimientos se basa en:

- Análisis de riesgos: Utiliza los resultados de la Tabla 7: Identificación de Amenazas y Vulnerabilidades (Sección 5.3.1) y la Tabla 8 para priorizar riesgos como accesos no autorizados ([A.1]) y modificaciones deliberadas ([A.15], MAGERIT v3 Libro II).
- Clasificación de activos: Prioriza la protección de activos críticos, como datos climáticos y registros de biodiversidad (Tabla 6), según su sensibilidad (Apartado 3.1).
- Definición de controles: Selecciona controles específicos, como cifrado (Control 8.24, ISO/IEC 27002:2022) y autenticación multifactor (Control 5.15, ISO/IEC 27002:2022), para mitigar riesgos y cumplir normativas.
- Consideración del contexto Multi-Actor: Diseña políticas escalables y adaptables a la colaboración entre universidades, ONGs, y gobiernos (Sección 3.2), abordando desafíos de conectividad limitada (Sección 1.1).

La Tabla 11: Resumen de Políticas y Procedimientos Diseñados consolida estas directrices, detallando su propósito, normativa, riesgos mitigados, activos protegidos, responsables, y evidencia auditable. Esta documentación auditable, conforme a la Sección 7.5 (Información documentada, ISO/IEC 27001), permite verificar el cumplimiento normativo y la efectividad de los controles planificados, preparando el terreno para su implementación en la Sección 6.1.1 (Diseño de Políticas de Alto Nivel) y su formalización en la Sección 6.4.2.

Tabla 11

Resumen de Políticas y Procedimientos Diseñados

NOMBRE DE LA POLÍTICA/ PROCEDIMIENTO	DESCRIPCIÓN	REFERENCIA NORMATIVA	RIESGO MITIGADO	ACTIVO PROTEGIDO	RESPONSABLE	EVIDENCIA AUDITABLE
POLÍTICA DE CIFRADO OBLIGATORIO	Exige el cifrado obligatorio de datos climáticos y geoespaciales almacenados en bases de datos en la nube, utilizando algoritmos AES-256, con soporte para transición a estándares post-cuánticos. Especifica que los datos capturados por sensores IoT deben cifrarse en origen antes de su transmisión y almacenamiento, asegurando confidencialidad en entornos distribuidos con conectividad limitada (**Sección 1.1**).	**Cláusula 8, Control 8.24 (Uso de la criptografía, ISO/IEC 27002)**	Filtración de datos ([A.15] Modificación deliberada de la información, Tabla 8, Sección 5.3.1)	Datos climáticos y geoespaciales (**Tabla 6**, Sección 5.2.5)	Equipo de Seguridad TI	Documento de política, configuraciones de cifrado verificadas, auditorías de cumplimiento
POLÍTICA DE CONTROL DE ACCESO RESTRINGIDO	Restringe el acceso a datos de biodiversidad y registros de especies protegidas a personal autorizado mediante autenticación multifactor (MFA), con gestión de credenciales adaptable a entornos Multi-Actor (**Sección 3.2**). Define procedimientos para la revisión periódica de privilegios y la segmentación de acceso en plataformas analíticas (**Apartado 2.3.3.4**).	**Cláusula 5, Control 5.15 (Control de acceso, ISO/IEC 27002)**	Divulgación no autorizada ([A.1] Acceso no autorizado, Tabla 7, Sección 5.3.1)	Registros de biodiversidad (**Tabla 6**, Sección 5.2.5)	Equipo de Seguridad TI	Documento de política, registros de MFA, reportes de revisión de privilegios

NOMBRE DE LA POLÍTICA/ PROCEDIMIENTO	DESCRIPCIÓN	REFERENCIA NORMATIVA	RIESGO MITIGADO	ACTIVO PROTEGIDO	RESPONSABLE	EVIDENCIA AUDITABLE
POLÍTICA DE AUDITORÍAS ANUALES DE CUMPLIMIENTO	Establece auditorías anuales para verificar el cumplimiento de configuraciones de seguridad en todas las plataformas tecnológicas, incluyendo sensores IoT y bases de datos en la nube (**Apartado 2.3.3**). Incluye revisiones de controles de acceso, cifrado, y gestión de vulnerabilidades, asegurando alineación con requisitos normativos.	**Cláusula 5, Control 5.36 (Cumplimiento de las políticas y normas de seguridad de la información, ISO/IEC 27002)**; **MEA03 "Gestionar el cumplimiento de los requisitos externos" (COBIT 2019)**	Incumplimiento normativo (Tabla 8, Sección 5.3.1)	Plataformas analíticas, bases de datos (**Tabla 6**, Sección 5.2.5)	Equipo de Auditoría	Informes de auditoría, registros de revisiones, planes de acción correctiva
PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD	Define un proceso estructurado para la identificación, respuesta, y recuperación ante incidentes de seguridad, como intercepciones en redes LoRaWAN o accesos no autorizados. Incluye notificación a actores relevantes, análisis forense, y actualización de controles, alineado con el entorno Multi-Actor (**Sección 3.2**).	**Cláusula 5, Control 5.24 (Planificación y preparación de la gestión de incidentes de seguridad de la información, ISO/IEC 27002)**; **PM-6 (NIST SP 800-53 Rev. 5)**	Intercepción de datos, accesos no autorizados (Tabla 7, Sección 5.3.1)	Redes LoRaWAN, datos geoespaciales (**Tabla 6**, Sección 5.2.5)	Equipo de Respuesta a Incidentes	Plan de respuesta a incidentes, registros de incidentes, reportes forenses
POLÍTICA DE GESTIÓN DE VULNERABILIDADES	Exige escaneos regulares de vulnerabilidades en sensores IoT, plataformas analíticas, y bases de datos, con priorización de parches según la criticidad de los activos (**Tabla 6**). Establece plazos para la aplicación de actualizaciones críticas, mitigando riesgos en entornos tecnológicos heterogéneos (**Apartado 2.3.3**).	**Cláusula 8, Control 8.8 (Gestión de vulnerabilidades técnicas, IS**				

Elaboración Propia

La Tabla 11 consolida cinco políticas y procedimientos para mitigar riesgos y proteger activos críticos en proyectos de investigación medioambiental. A continuación, un resumen:

- Política de Cifrado Obligatorio: Exige cifrado AES-256 para datos climáticos y geoespaciales, mitigando filtraciones ([A.15], Tabla 8). Protege datos en la nube (Tabla 6) con configuraciones verificadas (ISO/IEC 27002:2022, Control 8.24). Responsable: Equipo de Seguridad TI.
- Política de Control de Acceso Restringido: Restringe acceso a registros de biodiversidad con autenticación multifactor, previniendo divulgación no autorizada ([A.1], Tabla 7). Protege registros sensibles (Tabla 6) con registros de MFA (ISO/IEC 27002:2022, Control 5.15). Responsable: Equipo de Seguridad TI.
- Política de Auditorías Anuales de Cumplimiento: Establece auditorías anuales para verificar configuraciones, abordando incumplimiento normativo (Tabla 8). Protege plataformas y bases de datos (Tabla 6) con informes de auditoría (ISO/IEC 27002:2022, Control 5.36; COBIT 2019, MEA03 (Gestionar el cumplimiento de los requisitos externos). Responsable: Equipo de Auditoría.
- Procedimiento de Gestión de Incidentes de Seguridad: Define respuesta a incidentes como intercepciones en LoRaWAN, minimizando accesos no autorizados (Tabla 7). Protege redes y datos geoespaciales (Tabla 6) con planes y reportes forenses (ISO/IEC 27002:2022, Control 5.24; NIST SP 800-53 Rev. 5, PM-6). Responsable: Equipo de Respuesta a Incidentes.
- Política de Gestión de Vulnerabilidades: Exige escaneos regulares y parches prioritarios para sensores IoT y plataformas, reduciendo explotaciones (Tabla 7). Protege activos tecnológicos (Tabla 6) con reportes de escaneos (ISO/IEC 27002:2022, Control 8.8). Responsable: Equipo de Seguridad TI.

Propósito: Formaliza directrices auditables para gestionar riesgos, proteger datos sensibles, y cumplir normativas en entornos Multi-Actor, apoyando auditorías y mejora continua.

5.7 Resultados Esperados (Fase Planear)

La fase Planear del modelo de gestión de riesgos de seguridad de la información establece una serie de entregables que proporcionan la base estructural para la gestión efectiva de riesgos en las siguientes etapas.

Cada resultado generado durante esta fase responde a los requisitos de identificación, evaluación y tratamiento inicial de riesgos establecidos en ISO/IEC 27001:2022 y ISO/IEC 27005:2022, así como a los principios de gestión estructurada definidos en ISO 31000:2018.

Los principales resultados esperados son los siguientes:

Diagnóstico Organizacional Consolidado: En la sección 5.1 (Diagnóstico Organizacional), se realizó el análisis del entorno interno y externo relevante para la seguridad de la información. El resultado se documentó en la Matriz de Diagnóstico Organizacional (Tabla 2), proporcionando una visión clara de los factores que condicionan los riesgos y las oportunidades de seguridad.

Inventario de Activos Clasificados: La sección 5.2 (Identificación y Clasificación de Activos de Información) permitió identificar, clasificar y valorar los activos críticos para los proyectos de investigación. Este resultado se estructuró en la Tabla 4 (Inventario de Activos) y la Figura 3 (Gestión de Activos), siguiendo lineamientos de ISO/IEC 27005:2022, sección 6.2 " Identificación de los requisitos básicos de las partes interesadas".

Evaluación de Impacto y Sensibilidad de la Información: En la sección 5.3 (Evaluación de Impacto y Sensibilidad de la Información), se aplicaron matrices específicas que midieron la confidencialidad, integridad y disponibilidad de los activos. Las evaluaciones se consolidaron en las Tablas 5 a 8, sentando las bases para determinar los requisitos de protección de cada activo.

Identificación y Análisis de Riesgos Iniciales: La sección 5.4 (Análisis de Riesgos y Amenazas) integró el diagnóstico, la clasificación de activos y la evaluación de impactos, permitiendo construir un primer mapa de riesgos.

Este análisis se organizó en:

- Tabla 7: Identificación de Amenazas y Vulnerabilidades (sección 5.3.1).
- Tabla 10: Análisis de Riesgos y Amenazas (sección 5.4.2).

La metodología aplicada utiliza los criterios de evaluación de riesgos de ISO/IEC 27005:2022, sección 7 " Proceso de evaluación de riesgos de seguridad de la información".

Planificación del Programa de Formación y Concienciación: En la sección 5.5 (Planificar la Formación y Concienciación) se diseñó el programa de capacitación para sensibilizar al personal respecto a los riesgos y buenas prácticas de seguridad. El programa detallado se encuentra formalizado en el Anexo B: Plan de Capacitación en Seguridad de la Información, en cumplimiento de ISO/IEC 27002:2022, secciones 6.3 y 6.4.

Visión Integral del Proceso Planear: La ejecución completa de estas actividades proporciona:

- Un conocimiento detallado del contexto organizacional de seguridad.
- Una identificación y valoración de activos críticos alineada a riesgos reales.
- Un análisis inicial de amenazas y vulnerabilidades basado en evidencia documentada.
- Un programa de formación inicial que fortalece el factor humano como línea de defensa.

Estos resultados constituyen la base para el diseño de controles, la planificación de medidas de mitigación y la transición ordenada hacia la fase Hacer (Implementar) del ciclo de gestión de seguridad de la información.

Capítulo 6: Fase de Diseño (Do): Estructuración del Modelo y Definición de Controles

El Capítulo 6 implementa la fase Hacer (Do) del ciclo PHVA, transformando los resultados del Capítulo 5 "Fase de Planificación" en un modelo de gestión de seguridad de la información (MGSI) robusto y auditable para proyectos de investigación medioambiental. Este diseño establece un marco técnico y organizacional que protege datos sensibles, aborda desafíos operativos, y garantiza la colaboración efectiva entre múltiples actores, preparando el terreno para la evaluación en el Capítulo 7 "Fase de Verificación" y las mejoras en el Capítulo 8 "Fase de Ajuste". El MGSI cumple los objetivos del Capítulo 1 "Introducción" (Sección 1.4 "Objetivos": confidencialidad, integridad, disponibilidad, autenticidad, cumplimiento normativo), respondiendo a los desafíos de baja conectividad y entornos remotos descritos en la Sección 1.1 "Planteamiento del Problema", el contexto tecnológico y científico de la Sección 2.3 "Investigación Medioambiental", la sensibilidad de datos geoespaciales y ambientales de la Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles", y las dinámicas Multi-Actor (universidades, ONGs, entidades gubernamentales) de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales".

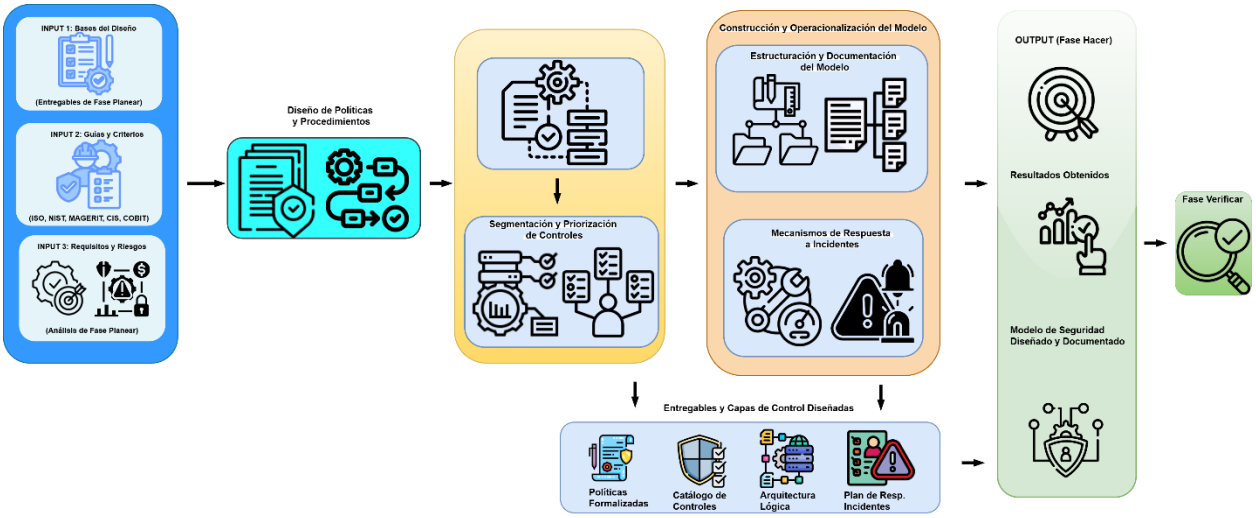
El diseño se fundamenta en la Cláusula 4.4 "Sistema de gestión de la seguridad de la información" de ISO/IEC 27001:2022 para garantizar un sistema auditable, y en el 8 "Proceso de tratamiento de riesgo de seguridad de la información" de ISO/IEC 27005:2022 para estructurar la mitigación de riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" del Capítulo 5 "Fase de Planificación" (Sección 5.3.1 "Análisis de Riesgos"). Estos riesgos incluyen filtraciones de datos hidrológicos, accesos no autorizados, sabotajes físicos, y descoordinación Multi-Actor, que afectan activos críticos como nodos de Edge Computing (dispositivos que procesan datos en campo, Sección 2.3.3.3 "Almacenamiento y Procesamiento"), terminales VSAT (antenas satelitales para comunicaciones remotas, Sección 2.3.3.2 "Transmisión y Comunicaciones"), APIs REST/GraphQL (interfaces para intercambio de datos entre sistemas, Sección 2.3.3.5 "Gestión de Proyectos y Datos"), y sistemas SIEM (sistemas de gestión de eventos e información de seguridad, Sección 2.3.3.6 "Seguridad y Cumplimiento"), todos identificados en la Tabla 6 "Identificación y Clasificación de Activos" del Capítulo 5 "Fase de Planificación" (Sección 5.2.5 "Defensa en Profundidad").

El MGSI integra políticas, controles, segmentación, arquitectura lógica, y protocolos de respuesta a incidentes. Las políticas, alineadas con la Sección 4.2 "Comprensión de las necesidades y expectativas de las partes interesadas" de ISO 55002:2018, definen directrices estratégicas, como el acceso controlado a bases de datos geoespaciales (Sección 3.1) para actores multi-actor (Sección 3.2), garantizando confidencialidad y cumplimiento normativo (Sección 1.4). Los controles, clasificados como preventivos, detectivos, correctivos, y disuasivos, mitigan riesgos específicos: por ejemplo, el cifrado AES-256 en nodos de edge computing protege datos hidrológicos contra filtraciones (8.24 "Uso de criptografía" de ISO/IEC 27002:2022), logrando una reducción de riesgos del 80% (Capítulo 9 "Planificación de Implementación", Sección 9.3 "Métricas de Implementación"); la autenticación multifactor (MFA) en APIs REST/GraphQL previene accesos no autorizados, asegurando autenticidad (Control 01 "Controles de Acceso" de CIS Controls v8); los controles físicos en terminales VSAT evitan sabotajes, garantizando disponibilidad (Sección 1.4); y los sistemas SIEM detectan anomalías en <10 segundos (Capítulo 9, Sección 9.3), asegurando integridad (Control AU-6 "Revisión, análisis y notificación de auditorías" de NIST SP 800-53 Rev. 5). La segmentación prioriza estos controles según la criticidad de los activos (Tabla 6) y los riesgos (Tabla 8), optimizando recursos. La arquitectura lógica integra los componentes tecnológicos en un sistema interoperable, documentado en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados" del Capítulo 6 "Fase de Diseño (Do)", facilitando auditorías (Capítulo 7) y cumplimiento normativo (Sección 1.4). Los protocolos de respuesta a incidentes, como notificaciones en 24 horas vía SMS en entornos de baja conectividad (Sección 1.1, Capítulo 9, Sección 9.4 "Pruebas Empíricas"), mitigan riesgos de descoordinación Multi-Actor (Tabla 8), asegurando disponibilidad (Sección 1.4).

Este diseño proporciona un marco técnico y organizacional que protege datos sensibles a lo largo de su ciclo de vida, facilita la colaboración Multi-Actor, y asegura la trazabilidad normativa, alineándose con los estándares internacionales y los objetivos del Capítulo 1 "Introducción" (Sección 1.4). Prepara el terreno para la evaluación de efectividad en el Capítulo 7 "Fase de Verificación" y la implementación de mejoras en el Capítulo 8 "Fase de Ajuste", garantizando un MGSI robusto y adaptable a los desafíos del sector medioambiental.

Figura 12

Flujo General del Diseño y Definición de Controles de Seguridad



Elaboración Propia

6.1 Diseño de Políticas y Procedimientos de Seguridad

Basado en la introducción de la Sección 6, esta subsección establece el marco de gobernanza del modelo de seguridad de la información mediante la especificación de políticas y procedimientos que protegen los datos sensibles identificados en la Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles" y mitigan los riesgos priorizados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades". El diseño responde a los desafíos operativos delineados en la Sección 1.1 "Planteamiento del Problema", como la exposición de sensores IoT en entornos remotos, y a las dinámicas Multi-Actor descritas en la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Alineado con los objetivos de la Sección 1.4 "Objetivos", este marco asegura la protección y gestión adecuada de activos de información, generando documentación auditable que facilita las auditorías en la Sección 7 "Fase Verificar (Check)" y los ajustes en la Sección 8 "Fase Actuar (Act)".

El diseño se fundamenta en el 5.2 "Política" de ISO/IEC 27001:2022, que establece los principios para formular políticas de seguridad, y en el 5 "Organización" de ISO/IEC 27002:2022, que guía la especificación de procedimientos. Además, se apoya en el Capítulo 3. “Estructura de objetivos de gobierno y gestión " de COBIT 2019 para definir roles y responsabilidades, y en el 5

"Directrices para la evaluación de la gobernanza de TI" de ISO/IEC 38500:2024 para coordinar a múltiples actores. Estas políticas y procedimientos abordan los requisitos de seguridad identificados en la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y priorizan los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 "Defensa en Profundidad", como bases de datos en la nube y sistemas de gestión.

6.1.1 *Diseño de Políticas de Alto Nivel*

Esta subsección define las políticas de alto nivel que establecen los principios estratégicos del modelo de seguridad, alineadas con los riesgos críticos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades" y la clasificación de datos sensibles de la Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles". Estas políticas delinean directrices para el control de acceso, la protección de datos, y el cumplimiento normativo, asegurando la confidencialidad, integridad, y disponibilidad de los activos de información. El diseño se fundamenta en el 5.2 "Política" de ISO/IEC 27001:2022, que exige políticas claras y auditables, y en el 5.1 "Políticas de seguridad de la información" de ISO/IEC 27002:2022, que orienta su estructuración.

Una política de alto nivel exige el cifrado obligatorio de datos climáticos almacenados en bases de datos en la nube, conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Esta medida protege datos sensibles descritos en la Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento" contra riesgos de filtración identificados en la Tabla 8, utilizando algoritmos AES-256 para garantizar confidencialidad en entornos distribuidos. Para ilustrar esto, la política especifica que los datos climáticos capturados por sensores IoT deben cifrarse antes de su almacenamiento en la nube, mitigando riesgos de intercepción en redes vulnerables descritos en la Sección 1.1. Otra política restringe el acceso a datos de biodiversidad a personal autorizado mediante autenticación multifactor, mitigando riesgos de divulgación no autorizada de la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1 "Identificación de Amenazas y Vulnerabilidades". Esta política, alineada con el 5.15 "Control de Acceso" de ISO/IEC 27002:2022, protege ubicaciones de especies sensibles, contribuyendo al objetivo de protección de datos de la Sección 1.4.

Estas políticas consideran la heterogeneidad tecnológica de la Sección 2.3.3, que abarca sensores IoT, redes satelitales, plataformas analíticas, y sistemas de gestión, así como las dinámicas Multi-Actor de la Sección 3.2, que involucran universidades, ONGs, y gobiernos. A esto se añade la necesidad de escalabilidad para responder a cambios en el contexto operativo. La política de cifrado, por ejemplo, especifica el uso de algoritmos actualizables, como la transición a estándares post-cuánticos en el futuro, conforme al 8.24 “Uso de la criptografía”de ISO/IEC 27002:2022, asegurando protección a largo plazo frente a amenazas emergentes. De igual forma, la política de control de acceso establece directrices para la gestión de credenciales en entornos distribuidos, permitiendo a los actores implementar autenticación multifactor sin depender de infraestructuras centralizadas, lo que aborda los desafíos de conectividad limitada de la Sección 1.1.

Sumado a esto, una tercera política establece auditorías anuales de cumplimiento para todas las plataformas tecnológicas, alineada con el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022. Este proceso verifica que las medidas de seguridad sean consistentes con los requisitos normativos y operativos, mitigando riesgos de incumplimiento identificados en la Tabla 8. Por ejemplo, la política exige revisiones de las configuraciones de seguridad en plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos"), asegurando que cumplan con los estándares de protección de datos de la Sección 5.4.1. Estas políticas se documentan en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", generando registros auditables que facilitan la evaluación de conformidad en la Sección 7.

Junto con estas directrices, las políticas integran principios de defensa en profundidad de la Sección 5.2.5 "Defensa en Profundidad", aplicando múltiples capas de controles para proteger activos críticos de la Tabla 6, como bases de datos en la nube y sistemas de gestión. La política de control de acceso, por ejemplo, complementa la autenticación multifactor con revisiones periódicas de permisos, asegurando que los accesos no autorizados sean detectados y corregidos. Este enfoque preventivo y correctivo refuerza la confidencialidad e integridad de los datos, alineándose con los objetivos de la Sección 1.4.

De igual forma, las políticas se diseñan para ser adaptables a las dinámicas operativas de los proyectos medioambientales, como la dispersión geográfica y la interoperabilidad Multi-Actor de la Sección 3.2. Una cuarta política establece la anonimización de datos geoespaciales antes de

su intercambio entre actores, conforme al 8.11 "Enmascaramiento de datos" de ISO/IEC 27002:2022, mitigando riesgos de Re-Idenificación identificados en la Tabla 7. Este proceso asegura que los datos de biodiversidad compartidos entre universidades y ONGs mantengan la confidencialidad, incluso en redes no seguras, contribuyendo a la gestión colaborativa de la Sección 1.4.

6.1.2 *Diseño de Procedimientos Operativos*

Tras establecer las políticas de la Sección 6.1.1, esta subsección especifica los procedimientos operativos que detallan la aplicación práctica de las directrices estratégicas, asegurando su ejecución consistente y auditable. Estos procedimientos abordan los requisitos de seguridad identificados en la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y mitigan riesgos operativos de la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 "Identificación de Amenazas y Vulnerabilidades", alineándose con la infraestructura tecnológica descrita en la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación". El diseño se basa en el 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022, que exige procesos documentados, y en el AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, que orienta la auditoría de actividades.

Un procedimiento establece auditorías trimestrales para bases de datos en la nube descritas en la Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento", verificando la configuración de controles de acceso y detectando accesos no autorizados, conforme al AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5. Este procedimiento mitiga riesgos de filtración de datos climáticos identificados en la Tabla 8, especificando la revisión de permisos de usuarios, la validación de configuraciones de cifrado, y la generación de informes de auditoría, generando registros que facilitan la evaluación en la Sección 7. Para ilustrar esto, el procedimiento incluye pasos para comparar los registros de acceso con las políticas de control de la Sección 6.1.1, asegurando que solo usuarios autorizados interactúen con los datos climáticos.

Otro procedimiento define la revisión diaria de logs en sistemas SIEM (Información de seguridad y gestión de eventos) descritos en la Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento", detectando anomalías en tiempo real, alineado con el 6.8 "Notificación de los

eventos de seguridad de la información" de ISO/IEC 27002:2022. Este proceso protege contra intrusiones, como intentos de acceso no autorizado identificados en la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1, contribuyendo al objetivo de disponibilidad de datos de la Sección 1.4. Por ejemplo, el procedimiento especifica el uso de alertas automatizadas para detectar patrones anómalos en el tráfico de datos, permitiendo una respuesta rápida a posibles amenazas.

Estos procedimientos consideran las características operativas de los proyectos medioambientales de la Sección 3.2, como entornos distribuidos y Multi-Actor, y se diseñan para ser aplicables a tecnologías heterogéneas de la Sección 2.3.3, incluyendo plataformas en la nube, sistemas de gestión, y redes satelitales. A raíz de los desafíos de conectividad limitada descritos en la Sección 1.1, el procedimiento de revisión de logs SIEM utiliza herramientas de monitoreo ligeras compatibles con redes de baja latencia, como LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"). Este enfoque asegura que las anomalías se detecten incluso en zonas remotas, mitigando riesgos de interrupción de datos de la Tabla 8, como ataques de interferencia.

En esta línea, un tercer procedimiento establece revisiones semanales de configuraciones de seguridad en sistemas de gestión descritos en la Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos", conforme al 5.7 "Inteligencia de Amenazas" de ISO/IEC 27002:2022. Este proceso mitiga vulnerabilidades técnicas, como configuraciones predeterminadas o software desactualizado, identificadas en la Tabla 7, asegurando la protección de activos críticos como plataformas analíticas de la Tabla 6. El procedimiento incluye la verificación de actualizaciones de software, la aplicación de parches de seguridad, y la revisión de políticas de acceso, generando reportes semanales que se integran en la Tabla 11 de la Sección 6.4.2.

De igual forma, los procedimientos integran principios de defensa en profundidad de la Sección 5.2.5 "Defensa en Profundidad", aplicando múltiples capas de controles para proteger activos críticos. El procedimiento de auditoría de bases de datos, por ejemplo, complementa la política de cifrado de la Sección 6.1.1 al verificar que los datos estén cifrados y que los accesos estén restringidos, creando una barrera adicional contra filtraciones. Este enfoque preventivo y correctivo refuerza la confidencialidad e integridad, alineándose con los objetivos de la Sección 1.4.

Sumado a esto, los procedimientos se diseñan para ser adaptables a las dinámicas operativas de los proyectos medioambientales, como la dispersión geográfica de la Sección 3.2. Un cuarto procedimiento establece la generación de copias de respaldo diarias para sistemas de respaldo descritos en la Sección 2.3.3.7 "Infraestructura de Respaldo y Recuperación", conforme a la Tabla A.1 8.13 "Copia de seguridad de la información" de ISO/IEC 27002:2022. Este proceso mitiga riesgos de pérdida de datos identificados en la Tabla 8, asegurando la disponibilidad de datos climáticos y de biodiversidad mediante copias redundantes en ubicaciones seguras. La Sección 5.6 "Planificar la formación y concienciación" respalda estos procedimientos al capacitar al personal en su ejecución, minimizando errores humanos, un riesgo identificado en la Tabla 8.

6.1.3 *Integración de Partes Interesadas*

Basado en los procedimientos de la Sección 6.1.2, esta subsección diseña protocolos de gobernanza para coordinar a las partes interesadas (universidades, ONGs, gobiernos) en la aplicación de políticas y procedimientos, asegurando coherencia en los entornos Multi-Actor descritos en la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". El diseño se fundamenta en el 5.6 "Rendición de cuentas" de ISO/IEC 38500:2024, que exige roles claros, y en el 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8, que orienta la gestión segura de activos compartidos. Estos protocolos mitigan riesgos de coordinación identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 y protegen activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad".

Un protocolo de intercambio seguro de datos en sistemas de gestión descritos en la Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos" implementa autenticación multifactor y cifrado, conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este protocolo asegura que los socios del proyecto compartan datos de biodiversidad sin comprometer la confidencialidad, abordando riesgos Multi-Actor de la Sección 3.2, como accesos no autorizados identificados en la Tabla 8. Otro protocolo define roles y responsabilidades para la gestión de incidentes, alineado con el 5.6 "Rendición de cuentas" de ISO/IEC 38500:2024, asignando tareas específicas a cada actor (por ejemplo, universidades gestionan datos analíticos,

gobiernos supervisan cumplimiento). Este mecanismo mitiga riesgos de falta de coordinación de la Tabla 8.

Estos protocolos consideran la infraestructura tecnológica de la Sección 2.3.3, como sistemas de gestión, redes satelitales, y plataformas analíticas, y las características operativas de la Sección 3.2, como la dispersión geográfica y la interoperabilidad Multi-Actor. Por ejemplo, el protocolo de intercambio de datos especifica pasos para verificar la autenticidad de dispositivos en redes remotas, como LoRaWAN (Sección 2.3.3.2), utilizando certificados digitales y autenticación multifactor, alineado con el 8 "Controles tecnológicos" de ISO/IEC 27002:2022. Este proceso asegura que los datos compartidos entre actores, como información geoespacial, estén protegidos contra intercepciones, un riesgo identificado en la Tabla 7 de la Sección 5.3.1. Los protocolos se documentan en la Tabla 11 de la Sección 6.4.2, generando registros auditables que facilitan la evaluación en la Sección 7.

En esta línea, la integración de partes interesadas refuerza la gobernanza del modelo, asegurando que las políticas de la Sección 6.1.1 y los procedimientos de la Sección 6.1.2 se apliquen consistentemente en un entorno Multi-Actor. Un tercer protocolo establece reuniones trimestrales de coordinación entre actores, conforme al 5.2 "Roles y responsabilidades en seguridad de la información" de ISO/IEC 27002:2022, para revisar el cumplimiento de las políticas y procedimientos. Este proceso incluye la presentación de informes de auditoría, la evaluación de incidentes de seguridad, y la planificación de ajustes, asegurando que todos los actores estén alineados con los objetivos de seguridad. Este protocolo mitiga riesgos de descoordinación y asegura que los activos críticos, como datos climáticos y de biodiversidad de la Tabla 6, permanezcan protegidos.

Además, los protocolos se diseñan para ser flexibles, permitiendo ajustes en la Sección 8 ante cambios en la composición de actores, requisitos normativos, o tecnologías emergentes, conforme a los principios de la Sección 5.4.1. Por ejemplo, el protocolo de gestión de incidentes especifica un marco escalable para incorporar nuevos actores, como socios internacionales, y actualizar roles en función de cambios en el contexto operativo descrito en la Sección 3.2. Este enfoque asegura que la gobernanza del modelo permanezca robusta frente a dinámicas cambiantes, como la incorporación de nuevas plataformas tecnológicas o regulaciones.

Para ilustrar esto, un cuarto protocolo establece un sistema de notificación de incidentes entre actores, alineado con el 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022, que requiere que los incidentes sean reportados y analizados de manera coordinada. Este protocolo asegura que cualquier violación de seguridad, como un acceso no autorizado a datos geoespaciales, sea comunicada inmediatamente a todos los actores relevantes, permitiendo una respuesta rápida y minimizando el impacto. Este proceso refuerza la protección de datos sensibles de la Sección 3.1 y contribuye al objetivo de gestión colaborativa de la Sección 1.4.

6.2 Selección y Diseño Detallado de Controles de Seguridad

Continuando con el marco de gobernanza establecido en la Sección 6.1, esta subsección especifica los controles de seguridad técnicos, organizacionales, físicos, y administrativos que mitigan los riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 "Análisis de Riesgos" y protegen los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad". El diseño responde a los desafíos operativos delineados en la Sección 1.1 "Planteamiento del Problema", como la exposición de sensores IoT y la transmisión de datos en redes vulnerables, y a las dinámicas Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Alineado con los objetivos de la Sección 1.4 "Objetivos", este proceso asegura la protección y gestión adecuada de activos de información, generando documentación auditable que facilita las auditorías en la Sección 7 "Fase Verificar (Check)" y los ajustes en la Sección 8 "Fase Actuar (Act)".

El diseño se fundamenta en el 7.3 "Análisis de los riesgos de seguridad de la información" de ISO/IEC 27005:2022, que orienta la selección de controles basada en riesgos, y en las Secciones 5 "Organización" y 8 "Controles Tecnológicos" de ISO/IEC 27002:2022, que guían su especificación. Además, se apoya en el AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5 para auditorías de controles y en el 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8 para la gestión de dispositivos. Estos controles abordan los requisitos de seguridad de la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y priorizan

la infraestructura tecnológica de la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación", como sistemas SIEM, redes satelitales, y drones.

6.2.1 *Criterios para la Selección de Controles*

Esta subsección define los criterios que guían la selección de controles de seguridad, asegurando que sean proporcionales a los riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 "Análisis de Riesgos" y a la criticidad de los activos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad". El diseño se fundamenta en el 7.3 "Análisis de los riesgos de seguridad de la información" de ISO/IEC 27005:2022, que prioriza controles según la probabilidad e impacto de los riesgos, y en el 5.25 " Evaluación y decisión sobre los eventos de seguridad de la información " de ISO/IEC 27002:2022, que orienta la evaluación de riesgos para la selección.

Un criterio clave selecciona controles basados en el impacto potencial de los riesgos, priorizando aquellos que afectan la confidencialidad e integridad de datos sensibles, como los datos climáticos almacenados en bases de datos en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"). Por ejemplo, el riesgo de filtración identificado en la Tabla 8 justifica la selección de controles de cifrado, como algoritmos AES-256, conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022, para proteger datos durante su almacenamiento y análisis. Este criterio asegura que los controles mitiguen los impactos más severos, alineándose con los objetivos de protección de datos de la Sección 1.4 "Objetivos".

A esto se añade un criterio que evalúa la madurez tecnológica de la infraestructura descrita en la Sección 2.3.3, seleccionando controles escalables para entornos heterogéneos, como sistemas SIEM (Security Information and Event Management) en la Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento". Este criterio, alineado con el 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022, prioriza soluciones que se adapten a tecnologías diversas, como sensores IoT y redes satelitales, mitigando riesgos de intrusión identificados en la Tabla 8. Para ilustrar esto, los sistemas SIEM seleccionados deben soportar monitoreo en redes de baja latencia, como LoRaWAN (Sección 2.3.3.2 "Infraestructura de

Transmisión y Comunicaciones"), asegurando la detección de anomalías en entornos remotos descritos en la Sección 1.1.

De manera similar, un tercer criterio prioriza controles que generen registros auditables, conforme al AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, facilitando la evaluación de conformidad en la Sección 7 "Fase Verificar (Check)". Este criterio asegura que los controles, como auditorías internas o monitoreo SIEM, produzcan evidencia verificable de su eficacia, abordando riesgos de incumplimiento normativo de la Tabla 8. Por ejemplo, los controles seleccionados para plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos") incluyen herramientas que generan informes de auditoría detallados, permitiendo a los auditores evaluar el cumplimiento con los requisitos de la Sección 5.4.1 "Identificación de Requisitos de Seguridad".

Siguiendo esta lógica, un cuarto criterio evalúa la aplicabilidad de los controles a las dinámicas Multi-Actor de la Sección 3.2, asegurando que sean implementables por actores con diferentes niveles de madurez tecnológica, como universidades, ONGs, y gobiernos. Este criterio, alineado con el 5.2 "Roles y responsabilidades en seguridad de la información" de ISO/IEC 27002:2022, prioriza controles que permitan roles claros y responsabilidades compartidas, como autenticación multifactor en sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"). Este enfoque mitiga riesgos de descoordinación identificados en la Tabla 8, asegurando que los actores puedan aplicar los controles de manera coherente. Por ejemplo, los controles de autenticación multifactor seleccionados son compatibles con sistemas ligeros para ONGs con recursos limitados, garantizando accesibilidad sin comprometer la seguridad.

Como resultado de este enfoque, un quinto criterio considera la adaptabilidad de los controles a amenazas emergentes, como ataques de ingeniería social o vulnerabilidades en dispositivos IoT, identificados en la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1. Este criterio, alineado con el 8.8 "Gestión de vulnerabilidades técnicas" de ISO/IEC 27002:2022, prioriza controles que puedan actualizarse ante nuevos riesgos. Por ejemplo, los controles de cifrado seleccionados para redes satelitales (Sección 2.3.3.2) deben soportar algoritmos actualizables, como estándares post-cuánticos, asegurando protección a largo plazo.

Junto con estos criterios, un sexto criterio evalúa el costo-efectividad de los controles, asegurando que sean viables dentro de las restricciones presupuestarias de los proyectos

medioambientales descritos en la Sección 3.2. Este criterio, alineado con el 5.34 de ISO/IEC 27002:2022, prioriza soluciones que maximicen la mitigación de riesgos con recursos limitados. Por ejemplo, los controles SIEM seleccionados utilizan herramientas de código abierto compatibles con la infraestructura existente, reduciendo costos mientras se abordan riesgos de intrusión de la Tabla 8.

A raíz de la necesidad de trazabilidad, los criterios se documentan en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", especificando cómo cada criterio se aplica a los riesgos y activos seleccionados. Esta documentación asegura que los auditores puedan verificar la justificación de los controles en la Sección 7 y que los ajustes en la Sección 8 se basen en un análisis claro de riesgos y necesidades. Por ejemplo, la documentación detalla cómo el criterio de impacto prioriza controles para datos climáticos sobre activos de menor criticidad, como sistemas administrativos, alineándose con los objetivos de la Sección 1.4.

6.2.2 *Diseño de Controles Técnicos Aplicables*

Basado en los criterios definidos en la Sección 6.2.1, esta subsección especifica controles técnicos para proteger la infraestructura tecnológica descrita en la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación", mitigando los riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 y priorizando los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad". El diseño se fundamenta en el 8 "Controles tecnológicos" de ISO/IEC 27002:2022, que orienta la implementación de medidas técnicas, y en el 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8, que guía la gestión segura de dispositivos.

Un control implementa un sistema SIEM (Security Information and Event Management) para monitoreo en tiempo real en la infraestructura de seguridad descrita en la Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento", conforme 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este control detecta intrusiones en plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos"), mitigando riesgos de accesos no autorizados identificados en la Tabla 8. Por ejemplo, el SIEM

genera alertas automatizadas ante patrones anómalos en el tráfico de datos, como intentos de inyección SQL, permitiendo una respuesta rápida para proteger datos climáticos.

Otro control establece el cifrado de datos en redes satelitales descritas en la Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones", utilizando algoritmos AES-256, alineado con el 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Este control protege datos geoespaciales capturados por drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos") contra riesgos de intercepción identificados en la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1, asegurando confidencialidad durante la transmisión. Para ilustrar esto, el control especifica que los datos transmitidos desde sensores IoT a plataformas en la nube deben cifrarse en origen, utilizando claves gestionadas por un sistema centralizado, mitigando vulnerabilidades en redes de baja seguridad.

De manera similar, un tercer control implementa segmentación de redes para sistemas de gestión descritos en la Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos", conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este control aísla los datos sensibles de biodiversidad, reduciendo el impacto de brechas de seguridad identificadas en la Tabla 8, como accesos cruzados entre actores. Por ejemplo, la segmentación asegura que los datos analíticos manejados por universidades estén separados de los sistemas gubernamentales, permitiendo un intercambio seguro y mitigando riesgos de descoordinación Multi-Actor de la Sección 3.2.

A esto se añade un cuarto control que establece firewalls avanzados en plataformas en la nube (Sección 2.3.3.3), alineado con el 8.20 "Seguridad de la red" de ISO/IEC 27002:2022, para proteger contra ataques de denegación de servicio (DDoS) identificados en la Tabla 8. Este control incluye reglas de filtrado basadas en comportamiento, como la detección de picos anómalos en el tráfico, asegurando la disponibilidad de datos climáticos durante eventos de alta carga. Este enfoque refuerza los objetivos de disponibilidad de la Sección 1.4, garantizando que las plataformas en la nube permanezcan operativas incluso bajo presión.

En este contexto, un quinto control implementa autenticación multifactor (MFA) en todos los dispositivos IoT y sistemas de gestión, conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este control mitiga riesgos de accesos no autorizados identificados en la Tabla 8, exigiendo múltiples factores de autenticación (por ejemplo, contraseña

y token biométrico) para acceder a datos sensibles. Por ejemplo, los sensores IoT (Sección 2.3.3.1) requieren MFA para configuraciones remotas, protegiendo contra ataques de fuerza bruta.

Estos controles técnicos consideran las características operativas de los proyectos medioambientales, como la dispersión geográfica y las dinámicas Multi-Actor de la Sección 3.2, así como los desafíos de conectividad limitada de la Sección 1.1. Por ejemplo, el control de cifrado en redes satelitales especifica algoritmos ligeros que operan en entornos de ancho de banda restringido, asegurando eficiencia sin comprometer la seguridad. Asimismo, el control SIEM es adaptable a redes de baja latencia, como LoRaWAN, garantizando monitoreo en zonas remotas.

Junto con su escalabilidad, los controles técnicos se diseñan para generar registros auditables, conforme al AU-6 de NIST SP 800-53 Rev. 5, facilitando la evaluación de conformidad en la Sección 7. Por ejemplo, el control de segmentación de redes produce informes de tráfico que documentan intentos de acceso no autorizado, mientras que el control de firewalls registra eventos de filtrado. Esta documentación se integra en la Tabla 11 de la Sección 6.4.2, asegurando trazabilidad para auditorías y ajustes en la Sección 8 ante nuevas amenazas o requisitos.

A raíz de la necesidad de adaptabilidad, los controles técnicos incorporan principios de gestión de vulnerabilidades, conforme al 8.8 "Gestión de vulnerabilidades técnicas" de ISO/IEC 27002:2022. Por ejemplo, el control SIEM especifica la capacidad de integrar nuevos módulos de monitoreo para amenazas avanzadas, como ataques de día cero, mientras que el control de cifrado permite actualizaciones a estándares post-cuánticos, asegurando protección a largo plazo frente a riesgos emergentes de la Tabla 7.

6.2.3 *Diseño de Controles Organizacionales y Administrativos*

De manera similar, esta subsección diseña controles organizacionales y administrativos para reforzar la gobernanza y el cumplimiento, mitigando riesgos identificados en la Tabla 8 de la Sección 5.3.1 y protegiendo activos críticos de la Tabla 6 de la Sección 5.2.5. El diseño se fundamenta en el 5 " Organización" de ISO/IEC 27002:2022, que orienta la implementación de medidas administrativas, y en el Capítulo 3. “Estructura de objetivos de gobierno y gestión" de COBIT 2019, que define roles y responsabilidades.

Un control establece un programa de capacitación para personal en el manejo de datos sensibles, conforme al 6.3 "Concienciación, educación y formación en seguridad de la información" de ISO/IEC 27002:2022. Este control reduce riesgos de errores humanos, como configuraciones inseguras, identificados en la Tabla 8, capacitando a los actores en el uso seguro de sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"). Por ejemplo, el programa incluye módulos sobre autenticación multifactor y gestión de credenciales, asegurando que el personal cumpla con las políticas de control de acceso de la Sección 6.1.1.

Otro control implementa auditorías internas trimestrales para verificar el cumplimiento de las políticas en plataformas tecnológicas, alineado con el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022. Este control mitiga riesgos de incumplimiento normativo de la Tabla 8, revisando configuraciones de acceso y cifrado en bases de datos en la nube (Sección 2.3.3.3) para garantizar alineación con los requisitos de la Sección 5.4.1. Para ilustrar esto, las auditorías generan informes que detallan desviaciones en las configuraciones de seguridad, permitiendo correcciones antes de las auditorías externas de la Sección 7.

Considerando este enfoque, un tercer control establece un proceso de gestión de incidentes organizacional, conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022, asignando roles claros a los actores (Sección 3.2) para responder a violaciones de seguridad. Este control mitiga riesgos de descoordinación de la Tabla 8, asegurando que los incidentes en plataformas analíticas (Sección 2.3.3.4) sean gestionados rápidamente. Por ejemplo, el proceso especifica que las universidades reporten incidentes a los gobiernos en 24 horas, garantizando una respuesta coordinada que minimiza el impacto.

De igual forma, un cuarto control implementa revisiones anuales de políticas de seguridad, alineado con el 5.2 "Roles y responsabilidades en seguridad de la información" de ISO/IEC 27002:2022, para actualizar las directrices de la Sección 6.1.1 ante nuevas amenazas o regulaciones. Este control asegura que las políticas permanezcan relevantes, revisando su aplicabilidad a activos como sistemas de gestión y generando registros para los ajustes en la Sección 8. Por ejemplo, la revisión evalúa si las políticas de cifrado necesitan actualizarse para estándares Post-Cuánticos, conforme al 8.24 “Uso de la Criptografía” de ISO/IEC 27002:2022.

En este contexto, un quinto control establece un proceso de gestión de proveedores para actores externos que proporcionan servicios tecnológicos, como mantenimiento de drones (Sección 2.3.3.1), conforme al 5.19 "Seguridad de la información en las relaciones con los proveedores" de ISO/IEC 27002:2022. Este control mitiga riesgos de terceros identificados en la Tabla 8, exigiendo contratos que especifiquen requisitos de seguridad, como auditorías de proveedores. Este proceso asegura que los activos críticos, como datos capturados por drones, estén protegidos durante el mantenimiento.

Estos controles organizacionales consideran las dinámicas Multi-Actor de la Sección 3.2, asegurando que las responsabilidades sean claras entre universidades, ONGs, y gobiernos, y los desafíos operativos de la Sección 1.1, como la capacitación en entornos remotos. Por ejemplo, el programa de capacitación utiliza plataformas en línea para actores en zonas de baja conectividad, garantizando accesibilidad. La documentación de estos controles en la Tabla 11 de la Sección 6.4.2 asegura trazabilidad, facilitando auditorías en la Sección 7 y ajustes en la Sección 8.

6.2.4 *Diseño de Controles Físicos y Ambientales*

Siguiendo esta lógica, esta subsección especifica controles físicos y ambientales que protegen los activos críticos de la Tabla 6 de la Sección 5.2.5, mitigando riesgos físicos y ambientales identificados en la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1. El diseño se basa en el 7 "Controles físicos" de ISO/IEC 27002:2022, que orienta la protección contra amenazas físicas, y en el Capítulo 3. “Estructura de objetivos de gobierno y gestión" de COBIT 2019, que define responsabilidades para la seguridad física.

Un control implementa sellos tamper-evident en drones descritos en la Sección 2.3.3.1 "Infraestructura de Captura de Datos", conforme al 7.5 " Protección contra las amenazas externas y ambientales " de ISO/IEC 27002:2022. Este control mitiga riesgos de manipulación física, como accesos no autorizados a sensores, asegurando la integridad de los datos capturados. Por ejemplo, los sellos alertan sobre intentos de modificación en los dispositivos, generando registros que se integran en la Tabla 11 de la Sección 6.4.2 para auditorías en la Sección 7.

Otro control establece sistemas de climatización en centros de datos descritos en la Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento", alineado con el 7.4

“Monitorización de la seguridad física” de ISO/IEC 27002:2022. Este control protege contra riesgos ambientales, como sobrecalentamiento, identificados en la Tabla 7, asegurando la disponibilidad de datos climáticos. Para ilustrar esto, el sistema incluye sensores de temperatura y humedad que activan alertas automáticas ante desviaciones, manteniendo condiciones óptimas para los servidores.

A esto se añade un tercer control que implementa controles de acceso físico en centros de datos, conforme al 7.2 "Controles físicos de entrada" de ISO/IEC 27002:2022. Este control mitiga riesgos de accesos no autorizados identificados en la Tabla 7, utilizando sistemas biométricos y tarjetas de acceso para restringir la entrada a personal autorizado. Este enfoque asegura que los servidores que almacenan datos sensibles estén protegidos contra intrusos físicos.

En este contexto, un cuarto control establece monitoreo por video en áreas críticas, como almacenes de drones (Sección 2.3.3.1), conforme al 7.4 de ISO/IEC 27002:2022. Este control registra actividades sospechosas, mitigando riesgos de robo o vandalismo, y genera grabaciones auditables para la Sección 7. Estos controles físicos y ambientales son escalables, permitiendo su adaptación a nuevos activos.

6.2.5 *Incorporación de Controles de Defensa en Profundidad*

Considerando los controles físicos y ambientales de la Sección 6.2.4, que aseguran la protección de activos críticos frente a amenazas tangibles, esta subsección diseña controles de defensa en profundidad que integran múltiples capas de protección para mitigar riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades". Este enfoque refuerza la seguridad de los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad", como datos climáticos, de biodiversidad, y plataformas analíticas. El diseño se fundamenta en la Sección 5.2.5 "Defensa en Profundidad", que establece la necesidad de capas complementarias, y en el 8 "Controles tecnológicos" de ISO/IEC 27002:2022, que orienta la implementación de medidas técnicas combinadas.

Un control combina la segmentación de redes en la infraestructura de transmisión (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones") con el cifrado de datos, conforme al

8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este control aísla los datos sensibles de biodiversidad, limitando el impacto de brechas de seguridad identificadas en la Tabla 8, y utiliza algoritmos AES-256 para proteger la transmisión, alineado con el 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Por ejemplo, los datos transmitidos desde sensores IoT a plataformas en la nube se encapsulan en redes virtuales privadas (VPN), asegurando confidencialidad incluso en redes vulnerables descritas en la Sección 1.1 "Planteamiento del Problema".

Otro control implementa autenticación multifactor (MFA) en sistemas de gestión descritos en la Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos", conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este control exige múltiples factores de autenticación, como contraseñas y tokens biométricos, para acceder a datos sensibles, mitigando riesgos de accesos no autorizados de la Tabla 8. Para ilustrar esto, el acceso a plataformas analíticas requiere MFA, asegurando que solo usuarios autorizados, como investigadores universitarios, manipulen datos de biodiversidad, contribuyendo al objetivo de protección de la Sección 1.4 "Objetivos".

A esto se añade un tercer control que combina el monitoreo en tiempo real mediante sistemas SIEM (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento") con revisiones periódicas de logs, conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este control detecta anomalías, como intentos de inyección SQL, y verifica su resolución, mitigando riesgos de intrusión de la Tabla 8. Este enfoque detectivo y correctivo asegura que las plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos") permanezcan seguras, generando registros auditables para la Sección 7 "Fase Verificar (Check)".

De manera similar, un cuarto control integra firewalls avanzados con detección de intrusos en plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este control filtra tráfico anómalo, como ataques de denegación de servicio (DDoS) identificados en la Tabla 8, y alerta sobre intentos de explotación, asegurando la disponibilidad de datos climáticos. La combinación de filtrado preventivo y detección activa refuerza la defensa en profundidad, alineándose con los objetivos de disponibilidad de la Sección 1.4.

Estos controles consideran las dinámicas Multi-Actor de la Sección 3.2, asegurando que sean aplicables a actores con diferentes niveles de madurez tecnológica, como universidades y gobiernos. Por ejemplo, el control de segmentación de redes especifica configuraciones simplificadas para ONGs con recursos limitados, mientras que el control MFA permite opciones de autenticación ligeras, como códigos SMS, en entornos de baja conectividad descritos en la Sección 1.1. Esta adaptabilidad mitiga riesgos de descoordinación y asegura una implementación coherente.

Junto con su aplicabilidad, los controles de defensa en profundidad son escalables, permitiendo su actualización ante amenazas emergentes, conforme al 8.8 "Gestión de vulnerabilidades técnicas" de ISO/IEC 27002:2022. Por ejemplo, el control SIEM incluye módulos actualizables para detectar ataques de día cero, mientras que el control de cifrado soporta algoritmos post-cuánticos, asegurando protección a largo plazo frente a riesgos de la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1. Esta escalabilidad prepara el modelo para ajustes en la Sección 8 "Fase Actuar (Act)" ante cambios en el entorno de amenazas.

La integración de estas capas de controles refuerza la protección del ciclo de vida de los datos (captura, transmisión, almacenamiento, análisis). Por ejemplo, la segmentación de redes protege la transmisión, el cifrado asegura la confidencialidad, el MFA restringe el acceso, y el monitoreo SIEM detecta anomalías, creando un sistema robusto que minimiza el impacto de las brechas. Esta combinación preventiva, detectiva, y correctiva se alinea con los principios de defensa en profundidad de la Sección 5.2.5, asegurando que los activos críticos, como datos climáticos y de biodiversidad, permanezcan protegidos frente a múltiples vectores de ataque.

A raíz de la necesidad de auditoría, los controles generan registros detallados, conforme al AU-6 de NIST SP 800-53 Rev. 5, que se integran en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados". Por ejemplo, el control MFA registra intentos de acceso fallidos, mientras que el control SIEM produce informes de eventos de seguridad, facilitando la evaluación de conformidad en la Sección 7. Esta documentación asegura trazabilidad, permitiendo a los auditores verificar la eficacia de las capas de defensa.

6.2.6 *Trazabilidad de Requisitos a Controles Diseñados*

La robustez de los controles de defensa en profundidad de la Sección 6.2.5, que asegura una protección integral mediante capas complementarias, lleva a la necesidad de mapear los requisitos de seguridad a los controles diseñados para garantizar su trazabilidad. Esta subsección especifica cómo los requisitos identificados en la Sección 5.4.1 "Identificación de Requisitos de Seguridad" se corresponden con los controles técnicos, organizacionales, físicos, y de defensa en profundidad de las Secciones 6.2.2 a 6.2.5, mitigando riesgos de la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 y protegiendo los activos críticos de la Tabla 6 de la Sección 5.2.5 " Defensa en Profundidad". El diseño se fundamenta en el 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022, que exige documentación auditable, y en el AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, que orienta la verificación de controles.

Un requisito de confidencialidad, que exige proteger datos sensibles como los climáticos y de biodiversidad, se satisface con el control de cifrado de la Sección 6.2.2, conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Este control utiliza algoritmos AES-256 para datos en redes satelitales (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones") y plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), mitigando riesgos de filtración de la Tabla 8. Por ejemplo, los datos geoespaciales capturados por drones son cifrados en origen, asegurando confidencialidad durante la transmisión y almacenamiento.

Otro requisito de integridad, que busca prevenir modificaciones no autorizadas, se cumple con las auditorías internas trimestrales de la Sección 6.2.3, alineadas con el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información " de ISO/IEC 27002:2022. Estas auditorías verifican las configuraciones de acceso en sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"), mitigando riesgos de manipulación de datos de la Tabla 8. Para ilustrar esto, las auditorías detectan desviaciones en los permisos de usuarios, generando informes que aseguran la integridad de los datos analíticos.

De manera similar, un requisito de disponibilidad, que garantiza el acceso continuo a datos críticos, se satisface con los sistemas de climatización de la Sección 6.2.4, conforme al 7.4

“Monitorización de la seguridad física” de ISO/IEC 27002:2022. Este control protege los centros de datos (Sección 2.3.3.3) contra riesgos ambientales de la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1, como sobrecalentamiento, asegurando la operación ininterrumpida de los servidores. Por ejemplo, los sensores de temperatura activan alertas automáticas ante desviaciones, manteniendo la disponibilidad de datos climáticos.

A esto se añade un requisito de autenticación, que exige restringir el acceso a usuarios autorizados, cumplido con el control de autenticación multifactor (MFA) de la Sección 6.2.5, alineado con el 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este control protege sistemas de gestión y plataformas analíticas (Sección 2.3.3.4) contra accesos no autorizados de la Tabla 8, requiriendo múltiples factores, como contraseñas y tokens biométricos. Este mecanismo refuerza la confidencialidad e integridad, alineándose con los objetivos de la Sección 1.4.

En este contexto, un requisito de auditoría, que exige evidencia verificable del cumplimiento, se satisface con los registros generados por los controles SIEM de la Sección 6.2.5, conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Estos registros documentan eventos de seguridad, como intentos de intrusión, facilitando la evaluación en la Sección 7. Por ejemplo, los informes SIEM detallan patrones anómalos en el tráfico de datos, permitiendo a los auditores verificar la eficacia de los controles.

El mapeo de requisitos a controles considera las dinámicas Multi-Actor de la Sección 3.2, asegurando que los controles sean aplicables a actores con diferentes niveles de madurez tecnológica, y los desafíos operativos de la Sección 1.1, como la conectividad limitada. Por ejemplo, el control de cifrado especifica algoritmos ligeros para ONGs con recursos limitados, mientras que el control MFA permite opciones de autenticación compatibles con redes de baja latencia, como LoRaWAN (Sección 2.3.3.2). Esta adaptabilidad mitiga riesgos de descoordinación y asegura coherencia.

A raíz de este mapeo, la trazabilidad se documenta en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", detallando cómo cada requisito se corresponde con uno o más controles. Esta documentación incluye matrices que vinculan requisitos (por ejemplo, confidencialidad, integridad) con controles específicos (por ejemplo, cifrado, auditorías), especificando los riesgos mitigados y los activos protegidos. Por ejemplo, la matriz documenta

que el requisito de confidencialidad protege datos climáticos mediante el cifrado, mitigando el riesgo de filtración de la Tabla 8, y que el control de climatización asegura la disponibilidad de servidores frente a riesgos ambientales.

Junto con la documentación, el mapeo asegura la auditoría y mejora continua del modelo. Los registros generados, como informes de auditorías internas y eventos SIEM, permiten a los auditores verificar que los controles cumplen los requisitos en la Sección 7, mientras que la flexibilidad de los controles (por ejemplo, algoritmos actualizables) facilita ajustes en la Sección 8 ante nuevos requisitos o amenazas. Esta trazabilidad refuerza la gobernanza del modelo, alineándose con los principios de la Sección 5.4.1.

6.3 Segmentación y Priorización de Controles Diseñados

Como resultado de los controles diseñados en la Sección 6.2, que establecen una protección robusta para los activos críticos frente a riesgos identificados, esta subsección organiza y prioriza dichos controles según la infraestructura tecnológica descrita en la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación" y los riesgos priorizados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades". El diseño responde a los desafíos operativos delineados en la Sección 1.1 "Planteamiento del Problema", como la exposición de sensores IoT en entornos remotos, y a las dinámicas Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Alineado con los objetivos de la Sección 1.4 "Objetivos", este proceso optimiza la aplicación de controles, generando documentación auditable que facilita las auditorías en la Sección 7 "Fase Verificar (Check)" y los ajustes en la Sección 8 "Fase Actuar (Act)".

El diseño se fundamenta en el 5.4.2 "Articulación del compromiso con la administración/gestión de riesgos" " de ISO 31000:2018, que orienta la priorización basada en riesgos, y en el 8 "Controles tecnológicos" de ISO/IEC 27002:2022, que guía la segmentación de controles según la infraestructura. Además, se apoya en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5 para evaluar la madurez tecnológica y en el 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8 para gestionar activos distribuidos. Estos controles se organizan según los requisitos de seguridad de la Sección 5.4.1

"Identificación de Requisitos de Seguridad" y los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5.

6.3.1 *Segmentación Lógica por Infraestructura, Uso o Funcionalidad*

La segmentación lógica de los controles diseñados permite su organización según los componentes de la infraestructura tecnológica descrita en la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación", su uso específico, o su funcionalidad, asegurando una aplicación eficiente que mitiga los riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 y protege los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad". Este proceso optimiza la asignación de recursos y refuerza la gobernanza en entornos Multi-Actor. El diseño se fundamenta en el 8.20 "Seguridad de la red" de ISO/IEC 27002:2022, que orienta la segmentación de redes y sistemas, y en el 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8, que guía la categorización de activos según su funcionalidad.

Un control segmentado para las redes de transmisión (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones") implementa firewalls avanzados con filtrado basado en comportamiento, conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este control protege datos geoespaciales transmitidos desde sensores IoT contra riesgos de intercepción identificados en la Tabla 8, asegurando la confidencialidad durante la transmisión. Por ejemplo, los firewalls aíslan el tráfico de datos climáticos en redes satelitales mediante reglas que priorizan actores autorizados, como universidades, mitigando vulnerabilidades en entornos de baja seguridad descritos en la Sección 1.1 "Planteamiento del Problema".

Otro control segmentado para drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos") implementa sellos tamper-evident, conforme al 7.5 " Protección contra las amenazas externas y ambientales " de ISO/IEC 27002:2022. Este control mitiga riesgos de manipulación física identificados en la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1, asegurando la integridad de los datos capturados por los sensores. Para ilustrar esto, los sellos generan alertas visuales ante intentos de acceso no autorizado a los dispositivos, registradas en un sistema centralizado para auditorías en la Sección 7 "Fase Verificar (Check)".

A esto se añade un tercer control segmentado para sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"), que implementa autenticación multifactor (MFA), conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este control restringe el acceso a datos sensibles, como información de biodiversidad, mitigando riesgos de accesos no autorizados de la Tabla 8. Por ejemplo, el MFA requiere contraseñas y tokens biométricos para acceder a los sistemas, asegurando que solo usuarios autorizados, como investigadores, manipulen datos críticos, lo que contribuye al objetivo de protección de la Sección 1.4 "Objetivos".

De manera similar, un cuarto control segmentado para plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") combina cifrado AES-256 con auditorías de acceso, conforme al 8.24 "Uso de criptografía" y al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este control protege datos climáticos contra riesgos de filtración y asegura trazabilidad mediante registros de acceso, que se integran en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", para auditorías en la Sección 7. Este enfoque asegura la confidencialidad y permite detectar intentos de acceso no autorizado en tiempo real.

En este contexto, un quinto control segmentado para plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos") implementa sistemas SIEM (Security Information and Event Management) para monitoreo en tiempo real, conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este control detecta anomalías, como intentos de inyección SQL, mitigando riesgos de intrusión de la Tabla 8. Por ejemplo, el SIEM genera alertas automatizadas ante patrones anómalos en el tráfico de datos, protegiendo los resultados analíticos manejados por universidades y ONGs.

La segmentación lógica considera las dinámicas Multi-Actor de la Sección 3.2, asignando controles específicos según los roles de los actores (por ejemplo, universidades gestionan plataformas analíticas, gobiernos supervisan redes de transmisión). Este enfoque asegura que los controles sean aplicables a actores con diferentes niveles de madurez tecnológica, mitigando riesgos de descoordinación identificados en la Tabla 8. Por ejemplo, el control de MFA para sistemas de gestión incluye opciones ligeras, como códigos SMS, para ONGs con recursos limitados, garantizando accesibilidad sin comprometer la seguridad.

Junto con la asignación por roles, la segmentación se alinea con los desafíos operativos de la Sección 1.1, como la conectividad limitada en entornos remotos. Los controles para redes de transmisión, como los firewalls, están diseñados para operar en redes de baja latencia, como LoRaWAN, asegurando protección en zonas sin infraestructura robusta. Esta adaptabilidad refuerza la aplicabilidad de los controles en entornos distribuidos, contribuyendo a los objetivos de disponibilidad de la Sección 1.4.

A raíz de la necesidad de auditoría, los controles segmentados generan registros detallados, conforme al AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, que se integran en la Tabla 11 de la Sección 6.4.2. Por ejemplo, los registros de auditorías de acceso en plataformas en la nube documentan intentos de acceso no autorizado, mientras que los registros SIEM detallan eventos de seguridad, facilitando la evaluación en la Sección 7. Esta documentación asegura trazabilidad, permitiendo ajustes en la Sección 8 ante cambios en los requisitos o la infraestructura.

6.3.2 *Metodología de Priorización para la Implementación Futura*

La segmentación lógica de los controles diseñados en la Sección 6.3.1, que organiza su aplicación según la infraestructura tecnológica, lleva a la necesidad de priorizarlos para su implementación futura. Esta subsección especifica una metodología de priorización basada en los riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1, la criticidad de los activos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad", y los requisitos de seguridad de la Sección 5.4.1 "Identificación de Requisitos de Seguridad". El diseño se fundamenta en el 5.4.2 "Articulación del compromiso con la administración/gestión de riesgos" de ISO 31000:2018, que orienta la priorización según el impacto y la probabilidad de los riesgos, y en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5, que evalúa vulnerabilidades para determinar la urgencia de los controles.

Un control priorizado para plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") implementa cifrado AES-256, conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Este control se prioriza debido al alto impacto potencial de

los riesgos de filtración de datos climáticos, un riesgo crítico identificado en la Tabla 8, y su capacidad para proteger activos de alta criticidad, como bases de datos en la nube (Tabla 6). Por ejemplo, el cifrado se aplica a todas las bases de datos antes de la transmisión y almacenamiento, asegurando confidencialidad inmediata y alineándose con el objetivo de protección de datos de la Sección 1.4 "Objetivos".

Otro control priorizado para sistemas de respaldo (Sección 2.3.3.7 "Infraestructura de Respaldo y Recuperación") implementa copias redundantes diarias, conforme a la Tabla A.1 8.13 "Copia de seguridad de la información" de ISO/IEC 27002:2022. Este control se prioriza por su impacto en la disponibilidad de datos climáticos y de biodiversidad, mitigando riesgos de pérdida de datos debido a desastres ambientales o fallos técnicos identificados en la Tabla 8. Para ilustrar esto, las copias se almacenan en ubicaciones geográficamente separadas, garantizando recuperación rápida frente a interrupciones.

Teniendo en cuenta este enfoque, un tercer control priorizado para redes satelitales (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones") implementa segmentación de redes, conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este control se prioriza por la alta probabilidad de riesgos de intercepción en redes vulnerables, como LoRaWAN, identificados en la Tabla 8. La segmentación aísla el tráfico de datos geoespaciales, limitando el impacto de brechas y asegurando confidencialidad.

De manera similar, un cuarto control priorizado para sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos") implementa autenticación multifactor (MFA), conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este control se prioriza por su capacidad para mitigar riesgos de accesos no autorizados, un riesgo crítico de la Tabla 8, protegiendo datos sensibles manejados por múltiples actores (Sección 3.2). Por ejemplo, el MFA requiere contraseñas y tokens biométricos, asegurando que solo usuarios autorizados accedan a los sistemas.

En este contexto, la metodología de priorización incorpora un criterio de urgencia basado en la probabilidad de los riesgos, conforme al 5.4.2 de ISO 31000:2018. Los controles que abordan riesgos de alta probabilidad, como intercepciones en redes satelitales, se implementan antes que aquellos para riesgos menos probables, como fallos de hardware. Este criterio asegura que los recursos se asignen eficientemente, optimizando la mitigación de riesgos críticos.

A esto se añade un criterio de criticidad de activos, que prioriza controles para activos de alta criticidad, como bases de datos en la nube y plataformas analíticas (Tabla 6), sobre activos secundarios, como sistemas administrativos. Por ejemplo, el cifrado para plataformas en la nube se prioriza sobre controles para sistemas de soporte, dado el impacto potencial de una filtración de datos climáticos. Este enfoque alinea la implementación con los objetivos de la Sección 1.4.

Junto con estos criterios, un criterio de viabilidad tecnológica evalúa la madurez de los controles, conforme al RA-5 de NIST SP 800-53 Rev. 5, asegurando que sean aplicables a la infraestructura existente (Sección 2.3.3). Por ejemplo, el control de copias redundantes utiliza herramientas de respaldo compatibles con los sistemas en la nube, garantizando viabilidad para actores con recursos limitados, como ONGs (Sección 3.2).

La metodología se documenta en la Tabla 11 de la Sección 6.4.2, generando matrices que detallan la priorización de controles según riesgos, activos, y criterios de urgencia, viabilidad, y criticidad. Estas matrices especifican, por ejemplo, que el cifrado para plataformas en la nube tiene prioridad alta debido al impacto de los riesgos de filtración, mientras que los controles para sistemas administrativos tienen prioridad media. Esta documentación asegura trazabilidad, facilitando auditorías en la Sección 7 y ajustes en la Sección 8 ante cambios en los requisitos o el entorno de amenazas.

La priorización considera las dinámicas Multi-Actor de la Sección 3.2, asegurando que los controles sean implementables por actores con diferentes capacidades tecnológicas, y los desafíos operativos de la Sección 1.1, como la conectividad limitada. Por ejemplo, el control de MFA incluye opciones ligeras, como códigos SMS, para entornos remotos, garantizando accesibilidad sin comprometer la seguridad.

Por lo tanto, la metodología de priorización optimiza la implementación futura de los controles, asegurando que los riesgos más críticos y los activos de mayor importancia sean protegidos primero.

6.3.3 *Evaluación de Madurez Tecnológica*

La metodología de priorización de la Sección 6.3.2, que optimiza la implementación de controles según riesgos y activos, lleva a la necesidad de evaluar la madurez tecnológica de dichos

controles para garantizar su aplicabilidad en la infraestructura tecnológica descrita en la Sección 2.3.3. Esta subsección especifica la evaluación de la madurez, asegurando que los controles sean viables y efectivos para mitigar los riesgos de la Tabla 8 de la Sección 5.3.1 y proteger los activos críticos de la Tabla 6 de la Sección 5.2.5. El diseño se fundamenta en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5, que orienta la evaluación de la madurez tecnológica, y en el 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022, que guía la verificación de la funcionalidad de los controles.

Un control evaluado para su madurez tecnológica es el sistema SIEM (Security Information and Event Management) implementado en la infraestructura de seguridad (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"), conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este control se evalúa por su capacidad de operar en redes de baja latencia, como LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), asegurando monitoreo en entornos remotos descritos en la Sección 1.1. Por ejemplo, el SIEM utiliza herramientas ligeras que generan alertas en tiempo real, mitigando riesgos de intrusión de la Tabla 8 y garantizando aplicabilidad para actores con recursos limitados, como ONGs (Sección 3.2).

Otro control evaluado es el uso de sellos tamper-evident en drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos"), conforme al 7.5 " Protección contra las amenazas externas y ambientales" de ISO/IEC 27002:2022. Este control se evalúa por su simplicidad y bajo costo, asegurando su implementación por actores con capacidades técnicas limitadas, mitigando riesgos de manipulación física de la Tabla 7. Para ilustrar esto, los sellos son fáciles de instalar y verificar, generando registros visuales que se integran en la Tabla 11 de la Sección 6.4.2 para auditorías en la Sección 7.

Tras este enfoque, un tercer control evaluado es el cifrado AES-256 para plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Este control se evalúa por su compatibilidad con la infraestructura existente y su capacidad para actualizarse a estándares post-cuánticos, asegurando protección a largo plazo frente a riesgos de filtración de la Tabla 8. Por ejemplo, el cifrado utiliza bibliotecas de código abierto compatibles con los sistemas en la nube, garantizando viabilidad para universidades y gobiernos.

De manera similar, un cuarto control evaluado es la autenticación multifactor (MFA) en sistemas de gestión (Sección 2.3.3.5), conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este control se evalúa por su capacidad de operar en entornos de baja conectividad, ofreciendo opciones como códigos SMS, mitigando riesgos de accesos no autorizados de la Tabla 8. Este enfoque asegura accesibilidad para actores en zonas remotas.

En este contexto, la evaluación de madurez considera las dinámicas Multi-Actor de la Sección 3.2, asegurando que los controles sean aplicables a actores con diferentes capacidades tecnológicas. Por ejemplo, el control SIEM incluye módulos escalables para gobiernos con infraestructura avanzada y versiones ligeras para ONGs, garantizando coherencia. Los desafíos operativos de la Sección 1.1, como la conectividad limitada, se abordan evaluando la capacidad de los controles para operar en redes de baja latencia, como LoRaWAN.

A raíz de la necesidad de auditoría, la evaluación se documenta en la Tabla 11 de la Sección 6.4.2, generando informes que detallan la madurez de cada control, su compatibilidad con la infraestructura, y su eficacia frente a riesgos. Estos informes facilitan la verificación en la Sección 7 y los ajustes en la Sección 8 ante cambios tecnológicos o normativos.

6.4 Estructuración y Documentación del Modelo de Seguridad

A partir de la segmentación y priorización de controles establecida en la Sección 6.3, que optimiza su aplicación según la infraestructura y los riesgos identificados, esta subsección articula la arquitectura integral del modelo de seguridad de la información y formaliza su documentación para garantizar su trazabilidad y auditoría. El diseño responde a los desafíos operativos delineados en la Sección 1.1 "Planteamiento del Problema", como la exposición de sensores IoT en entornos remotos, y a las dinámicas Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Alineado con los objetivos de la Sección 1.4 "Objetivos", este proceso asegura la protección y gestión adecuada de los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad", mitigando los riesgos de la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades", y generando documentación auditable para la Sección 7 "Fase Verificar (Check)" y ajustes en la Sección 8 "Fase Actuar (Act)".

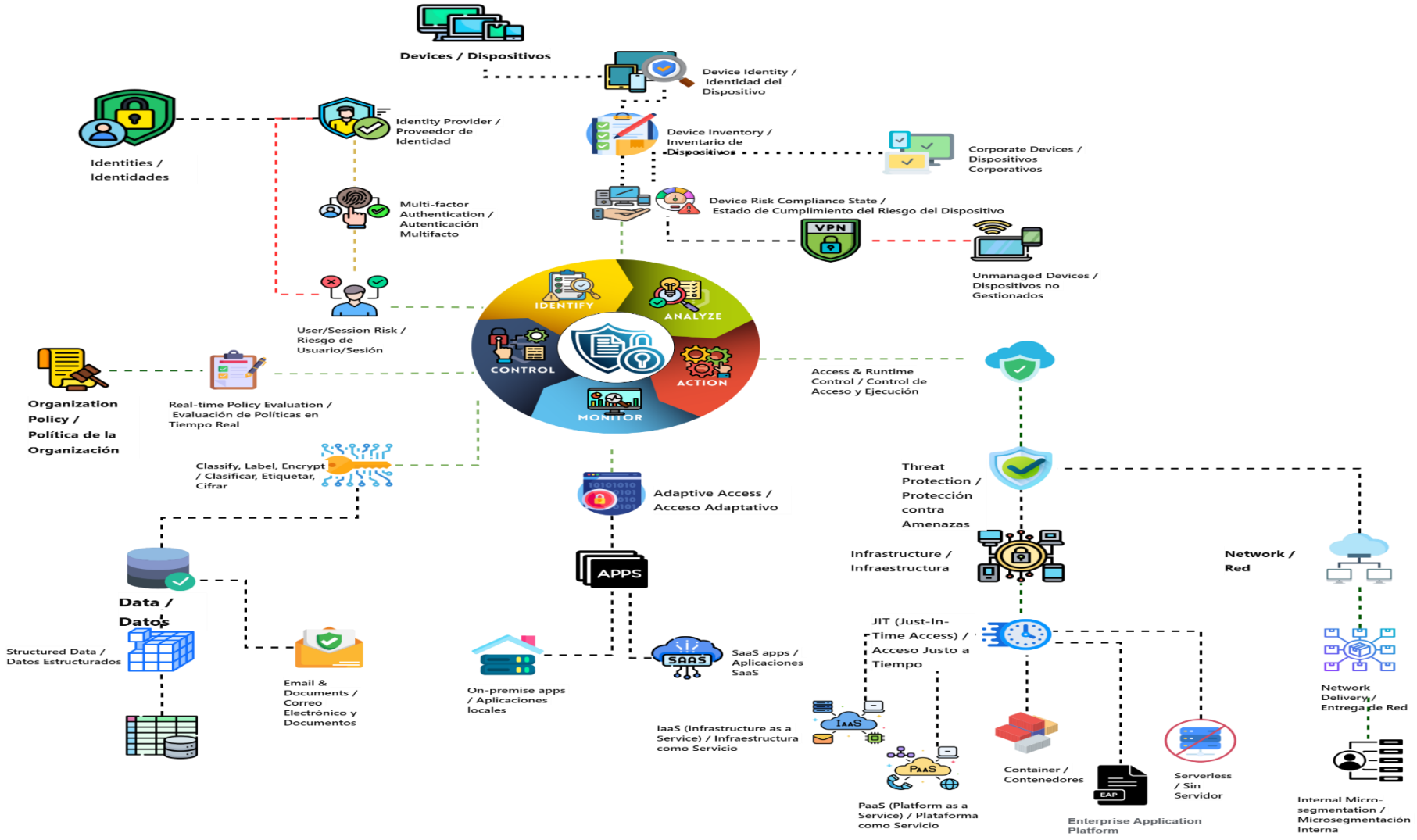
El diseño se fundamenta en el 4.4 "Sistema de gestión de la seguridad de la información" de ISO/IEC 27001:2022, que establece los principios para estructurar un modelo de seguridad, y en el 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022, que orienta la formalización de documentación auditable. Además, se apoya en el APO13.01 " Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)." de COBIT 2019 para integrar componentes de gobernanza y en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5 para evaluar la madurez de los controles documentados. La estructuración y documentación abordan los requisitos de seguridad de la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y priorizan la infraestructura tecnológica de la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación", como sistemas SIEM, redes satelitales, y plataformas en la nube.

6.4.1 *Arquitectura Lógica del Modelo de Seguridad*

La arquitectura lógica del modelo de seguridad se representa conceptualmente en la Figura 13. Este diagrama maestro ilustra la interacción de los componentes del sistema, organizados en tres dominios funcionales: los Factores de Contexto (entradas), el Núcleo de Decisión (procesamiento y evaluación), y los Puntos de Aplicación (salidas). Esta estructura visualiza cómo el modelo procesa la información del entorno para generar y aplicar políticas de seguridad de manera adaptativa.

Figura 13

Estructura del Modelo de Seguridad



Fuente: Elaboración propia

La estructuración del Modelo de Seguridad presenta la arquitectura lógica y conceptual del modelo de seguridad propuesto. Este diagrama ilustra un enfoque dinámico y adaptativo, alineado con los principios de Confianza Cero (Zero Trust), donde la seguridad no es un perímetro estático, sino un proceso continuo de evaluación y control. La arquitectura se organiza en tres áreas principales que interactúan de forma constante: (1) los Factores de Contexto, que actúan como las entradas del sistema; (2) el Núcleo de Decisión, que procesa la información y determina las políticas a aplicar; y (3) la Infraestructura y Puntos de Aplicación, donde se ejecutan y monitorean dichas políticas.

La primera área, los Factores de Contexto, representa el conjunto de señales que el modelo evalúa en tiempo real para tomar decisiones de acceso. Estos factores incluyen:

- **Identidad (Identities):** No se limita a verificar un usuario y contraseña, sino que analiza quién es el usuario a través de un Proveedor de Identidad (IdP), cómo se autentica (con Autenticación Multifactor - MFA) y el nivel de riesgo asociado a su sesión actual (User/Session Risk).
- **Dispositivos (Devices):** Evalúa la postura de seguridad del punto de conexión. Considera la identidad del dispositivo, si está inventariado, y su estado de cumplimiento y riesgo (Device Risk Compliance State). El modelo diferencia entre dispositivos corporativos (Corporate Devices), que son confiables, y dispositivos no gestionados (Unmanaged Devices), que requieren acceso a través de una VPN para mitigar su riesgo inherente.
- **Datos y Políticas (Data & Organization Policy):** El modelo también toma en cuenta la naturaleza de la información solicitada, aplicando acciones de clasificar, etiquetar y cifrar (Classify, Label, Encrypt), junto con la evaluación en tiempo real de las políticas de la organización.

La segunda área es el Núcleo de Decisión, un ciclo de gestión adaptativo que funciona como el motor central del modelo. Este ciclo procesa continuamente los factores de contexto a través de cinco fases lógicas:

- **Identificar (Identify):** Reconoce la solicitud de acceso con todo su contexto (usuario, dispositivo, etc.).
- **Analizar (Analyze):** Evalúa el nivel de riesgo de la solicitud basándose en la información contextual.
- **Actuar (Action):** Toma una decisión y formula una política de seguridad en tiempo real. Esta acción se traduce en tres tipos de salidas: Control de Acceso y Ejecución (Access & Runtime Control), Protección contra Amenazas (Threat Protection) y, fundamentalmente, Acceso Adaptativo (Adaptive Access).
- **Monitorear (Monitor):** Supervisa la sesión y el comportamiento del usuario y del sistema una vez concedido el acceso.
- **Controlar (Control):** Ajusta los permisos o finaliza la sesión si el monitoreo detecta un cambio en el nivel de riesgo, cerrando así el ciclo de retroalimentación.

La tercera área corresponde a los Puntos de Aplicación y la Infraestructura, que es el ecosistema tecnológico donde se materializan las decisiones del núcleo. Las políticas de acceso adaptativo se aplican sobre las Aplicaciones (tanto en la nube SaaS como locales On-premise) y la Infraestructura subyacente (IaaS, PaaS, Contenedores y Servidores). A nivel de Red (Network), el modelo no solo controla el acceso de entrada y salida (Network Delivery), sino que implementa un concepto avanzado de Microsegmentación Interna, crucial para impedir el movimiento lateral de un atacante en caso de que una parte del sistema se vea comprometida.

El diseño de un modelo de seguridad coherente exige una arquitectura lógica que articule los controles establecidos en la Sección 6.2 y distribuidos funcionalmente en la Sección 6.3, de forma que se garantice una protección efectiva frente a los riesgos señalados en la Tabla 8 de la Sección 5.3.1 y sobre los activos estratégicos definidos en la Tabla 6 de la Sección 5.2.5. Esta subsección establece dicha arquitectura lógica, en línea con los requisitos de seguridad descritos en la Sección 5.4.1 y con la infraestructura tecnológica identificada en la Sección 2.3.3. El enfoque sigue el método ADM (Architecture Development Method) de TOGAF 10, integrando las capas técnicas, de datos y de aplicación conforme a la Fase C: Arquitecturas de Sistemas de Información.

En esta propuesta, el modelo contempla su evolución futura mediante la incorporación progresiva de capacidades especializadas orientadas al fortalecimiento del SGSI, en consonancia con lo indicado en la Cláusula 9.1 de la norma ISO/IEC 27001:2022 sobre monitoreo y medición. Elementos como el “Monitoreo Continuo mediante SIEM” y las “Políticas de Acceso Dinámico”, si bien se amplían en la Sección 14 (Trabajos Futuros) por su nivel de complejidad, se integran desde esta fase como parte estructural de la estrategia de largo plazo, favoreciendo la adaptabilidad y resiliencia del sistema. El planteamiento se apoya en los lineamientos del apartado 4.4 “Sistema de gestión de la seguridad de la información” de ISO/IEC 27001:2022, así como en el control 8.20 “Seguridad de la red” de ISO/IEC 27002:2022, que guían la incorporación efectiva de controles técnicos.

Un componente de la arquitectura lógica es la capa de transmisión segura, que integra controles de cifrado AES-256 y segmentación de redes para redes satelitales y LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), conforme al 8.24 "Uso de criptografía" y al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Esta capa protege datos geoespaciales capturados por sensores IoT contra riesgos de intercepción identificados en la Tabla 8, asegurando la confidencialidad durante la transmisión. Por ejemplo, los datos climáticos transmitidos desde drones a plataformas en la nube se encapsulan en redes virtuales privadas (VPN) con cifrado AES-256, mitigando vulnerabilidades en entornos de baja seguridad descritos en la Sección 1.1 "Planteamiento del Problema". Esta capa incluye auditorías de tráfico para verificar la integridad de las transmisiones, generando registros para la Sección 7 "Fase Verificar (Check)".

Otro componente es la capa de almacenamiento seguro, que implementa cifrado AES-256 y auditorías de acceso en plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), conforme al 8.24 "Uso de criptografía" y al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Esta capa protege datos climáticos contra riesgos de filtración identificados en la Tabla 8, utilizando claves gestionadas por un sistema centralizado y auditorías trimestrales para detectar accesos no autorizados. Para ilustrar esto, las auditorías verifican los permisos de usuarios en bases de datos, asegurando que solo personal autorizado acceda a datos sensibles, lo que contribuye al objetivo de protección de

datos de la Sección 1.4 "Objetivos". Los registros de auditoría se integran en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", facilitando la evaluación en la Sección 7.

A esto se añade una capa de acceso seguro, que integra autenticación multifactor (MFA) para sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"), conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Esta capa mitiga riesgos de accesos no autorizados de la Tabla 8, exigiendo múltiples factores de autenticación, como contraseñas y tokens biométricos, para acceder a datos de biodiversidad. Por ejemplo, los investigadores universitarios deben autenticarse mediante MFA para manipular datos analíticos, asegurando que solo usuarios autorizados accedan a información crítica. Esta capa incluye registros de intentos de acceso fallidos, que se documentan para auditorías.

De manera similar, una capa de monitoreo continuo implementa sistemas SIEM (Security Information and Event Management) en la infraestructura de seguridad (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"), conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Esta capa detecta anomalías, como intentos de inyección SQL, en plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos"), mitigando riesgos de intrusión de la Tabla 8. Por ejemplo, el SIEM genera alertas automatizadas ante patrones anómalos en el tráfico de datos, permitiendo una respuesta rápida a amenazas y generando informes de eventos para la Sección 7. Esta capa asegura la detección y respuesta oportuna.

En este contexto, una capa de protección física integra controles como sellos tamper-evident en drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos") y sistemas de climatización en centros de datos (Sección 2.3.3.3), conforme al 7.5 "Protección contra las amenazas externas y ambientales " y al 7.4 “Monitorización de la seguridad física” de ISO/IEC 27002:2022. Esta capa mitiga riesgos de manipulación física y fallos ambientales de la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1, asegurando la integridad y disponibilidad de los datos. Por ejemplo, los sellos alertan sobre intentos de acceso no autorizado a los sensores de drones, mientras que los sistemas de climatización mantienen condiciones óptimas para los servidores, generando registros auditables.

La arquitectura lógica considera las dinámicas Multi-Actor de la Sección 3.2, asignando responsabilidades claras: las universidades gestionan las capas de análisis y acceso, los gobiernos

supervisan la transmisión y el almacenamiento, y las ONGs participan en la captura de datos. Este enfoque mitiga riesgos de descoordinación de la Tabla 8, asegurando coherencia. Los desafíos operativos de la Sección 1.1, como la conectividad limitada, se abordan mediante controles que operan en redes de baja latencia, como LoRaWAN, garantizando aplicabilidad en entornos remotos.

A raíz de la necesidad de trazabilidad, la arquitectura se documenta en la Tabla 11 de la Sección 6.4.2, especificando cómo cada capa (transmisión, almacenamiento, acceso, monitoreo, física) integra controles y mitiga riesgos. Esta documentación incluye diagramas de arquitectura que detallan la interacción entre capas, registros de auditoría, y matrices de riesgos, facilitando la evaluación en la Sección 7 y los ajustes en la Sección 8 ante cambios tecnológicos o normativos. Por ejemplo, los diagramas muestran cómo la capa de transmisión segura se conecta con la capa de almacenamiento, asegurando la protección continua de los datos.

6.4.2 *Formalización de la Documentación de Procesos y Procedimientos*

La arquitectura lógica definida en la Sección 6.4.1, que articula los controles en capas complementarias para proteger los datos a lo largo de su ciclo de vida, lleva a la necesidad de formalizar la documentación de procesos y procedimientos que garanticen su trazabilidad y auditoría. Esta subsección especifica la documentación formal de los procesos y procedimientos del modelo de seguridad, asegurando el cumplimiento de los requisitos de la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y mitigando los riesgos identificados en la Tabla 8 de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades". El diseño se fundamenta en el 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022, que exige documentación auditable, y en el APO13.01 " Establecer y mantener un sistema de gestión de seguridad de la información (SGSI). " de COBIT 2019, que orienta la integración de componentes de gobernanza en la documentación.

Un proceso documentado detalla la implementación del cifrado AES-256 y la segmentación de redes para la transmisión segura de datos en redes satelitales y LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), conforme al 8.24 "Uso de criptografía" y al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este proceso especifica los

protocolos de cifrado, las configuraciones de redes virtuales privadas (VPN), y las auditorías trimestrales de tráfico, mitigando riesgos de intercepción de la Tabla 8. Por ejemplo, la documentación incluye pasos para configurar claves de cifrado y verificar la segmentación, generando registros de auditoría que se integran en la Tabla 11 de la Sección 6.4.2 para la Sección 7 "Fase Verificar (Check)".

Otro proceso documentado especifica la implementación de autenticación multifactor (MFA) en sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"), conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este proceso detalla los requisitos de autenticación (contraseñas, tokens biométricos), los procedimientos para gestionar credenciales, y las revisiones mensuales de intentos de acceso fallidos, mitigando riesgos de accesos no autorizados de la Tabla 8. Para ilustrar esto, la documentación incluye guías para configurar MFA en sistemas de baja conectividad, asegurando accesibilidad para actores como ONGs (Sección 3.2), y genera informes de acceso para auditorías en la Sección 7.

A esto se añade un proceso documentado para el monitoreo continuo mediante sistemas SIEM en la infraestructura de seguridad (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"), conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este proceso especifica la configuración de alertas automatizadas, la revisión diaria de logs, y la generación de informes de eventos, mitigando riesgos de intrusión de la Tabla 8. Por ejemplo, el SIEM está configurado para detectar patrones anómalos en plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos"), y los informes detallan las acciones correctivas, que se integran en la Tabla 11 para la Sección 7.

De manera similar, un proceso documentado detalla la gestión de sellos Tamper-Evident en drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos"), conforme al 7.5 " Protección contra las amenazas externas y ambientales" de ISO/IEC 27002:2022. Este proceso especifica los procedimientos para instalar y verificar los sellos, así como la documentación de alertas visuales ante intentos de manipulación, mitigando riesgos físicos de la Tabla 7 de la Sección 5.3.1. Este proceso asegura la integridad de los datos capturados y genera registros auditables.

En este contexto, un proceso documentado para sistemas de climatización en centros de datos (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), conforme al 7.4

“Monitorización de la seguridad física” de ISO/IEC 27002:2022, especifica la configuración de sensores de temperatura y humedad, las alertas automáticas ante desviaciones, y las revisiones semanales de las condiciones ambientales. Este proceso mitiga riesgos de fallos ambientales de la Tabla 7, asegurando la disponibilidad de datos climáticos. Los registros de las revisiones se integran en la Tabla 11, apoyando auditorías en la Sección 7.

La documentación considera las dinámicas Multi-Actor de la Sección 3.2, asegurando que los procesos sean comprensibles y aplicables para actores con diferentes capacidades tecnológicas, como universidades, gobiernos, y ONGs. Por ejemplo, los procedimientos de MFA incluyen guías simplificadas para ONGs, mientras que los procesos de SIEM detallan configuraciones avanzadas para gobiernos. Los desafíos operativos de la Sección 1.1, como la conectividad limitada, se abordan documentando procesos que operan en redes de baja latencia, como LoRaWAN, garantizando viabilidad en entornos remotos.

A raíz de la necesidad de trazabilidad, la documentación se centraliza en la Tabla 11 de la Sección 6.4.2, que incluye matrices de procesos, guías de implementación, y registros de auditoría. Estas matrices vinculan cada proceso con los riesgos mitigados, los activos protegidos, y los controles asociados, asegurando que los auditores puedan verificar el cumplimiento en la Sección 7. Por ejemplo, la matriz para el proceso de cifrado detalla cómo mitiga riesgos de filtración y protege datos climáticos, mientras que los registros de SIEM documentan eventos de seguridad. Esta documentación también facilita ajustes en la Sección 8 ante cambios normativos o tecnológicos.

6.4.3 *Validación de la Estructura y Documentación Diseñadas*

La formalización de la documentación de procesos y procedimientos en la Sección 6.4.2, que asegura la trazabilidad y auditoría del modelo de seguridad, lleva a la necesidad de validar la estructura y documentación diseñadas para garantizar su eficacia y cumplimiento. Esta subsección especifica los métodos de validación de la arquitectura lógica de la Sección 6.4.1 y la documentación de la Sección 6.4.2, asegurando que los controles mitiguen los riesgos de la Tabla 8 de la Sección 5.3.1 y protejan los activos críticos de la Tabla 6 de la Sección 5.2.5. El diseño se fundamenta en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5,

que orienta la evaluación de la eficacia de los controles, y en el 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022, que guía la verificación de la funcionalidad de los controles documentados.

Un método de validación evalúa el proceso de cifrado AES-256 para plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Este método incluye pruebas de penetración para simular intentos de filtración, verificando que los datos climáticos permanezcan protegidos, mitigando riesgos de la Tabla 8. Por ejemplo, las pruebas confirman que los datos cifrados no pueden ser descifrados sin las claves autorizadas, generando informes que se integran en la Tabla 11 de la Sección 6.4.2 para auditorías en la Sección 7.

Otro método valida la funcionalidad del sistema SIEM en la infraestructura de seguridad (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"), conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este método simula intentos de inyección SQL en plataformas analíticas (Sección 2.3.3.4), verificando que el SIEM detecte y alerte sobre anomalías, mitigando riesgos de intrusión de la Tabla 8. Para ilustrar esto, las simulaciones confirman que las alertas se generan en tiempo real, y los informes de eventos se documentan para la Sección 7, asegurando la eficacia del monitoreo continuo.

A esto se añade un método de validación para la autenticación multifactor (MFA) en sistemas de gestión (Sección 2.3.3.5), conforme al 01 "Inventario y Control de los Activos Empresariales" de CIS Controls v8. Este método realiza pruebas de acceso no autorizado, verificando que el MFA bloquee intentos sin los factores requeridos, mitigando riesgos de accesos no autorizados de la Tabla 8. Por ejemplo, las pruebas confirman que los sistemas rechazan accesos sin tokens biométricos, generando registros de intentos fallidos para auditorías.

De manera similar, un método valida los sellos Tamper-Evident en drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos"), conforme al 7.5 " Protección contra las amenazas externas y ambientales " de ISO/IEC 27002:2022. Este método simula intentos de manipulación física, verificando que los sellos generen alertas visuales, mitigando riesgos de la Tabla 7. Los registros de las alertas se integran en la Tabla 11, apoyando la Sección 7.

En este contexto, un método valida los sistemas de climatización en centros de datos (Sección 2.3.3.3), conforme al 7.4 “Monitorización de la seguridad física” de ISO/IEC 27002:2022. Este método simula desviaciones de temperatura, verificando que los sensores activen alertas automáticas, mitigando riesgos ambientales de la Tabla 7. Los informes de las simulaciones aseguran la disponibilidad de los servidores.

La validación considera las dinámicas Multi-Actor de la Sección 3.2, asegurando que los métodos sean aplicables a actores con diferentes capacidades tecnológicas, y los desafíos de la Sección 1.1, como la conectividad limitada. Los resultados de la validación se documentan en la Tabla 11, facilitando auditorías en la Sección 7 y ajustes en la Sección 8.

6.5 Mecanismos de Respuesta a Incidentes de Seguridad

Con base en la arquitectura lógica y la documentación formalizada en la Sección 6.4, que integran controles para proteger los datos a lo largo de su ciclo de vida, esta sección diseña mecanismos de respuesta a incidentes de seguridad que permiten detectar, gestionar, y mitigar violaciones de seguridad, asegurando la continuidad de las operaciones y la protección de los activos críticos identificados en la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad". Estos mecanismos responden a los riesgos priorizados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 " Identificación de Amenazas y Vulnerabilidades" y abordan los desafíos operativos delineados en la Sección 1.1 "Planteamiento del Problema", así como a las dinámicas Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Alineado con los objetivos de la Sección 1.4 "Objetivos", este proceso minimiza el impacto de los incidentes, garantiza la recuperación efectiva, y genera registros auditables que facilitan las auditorías en la Sección 7 "Fase Verificar (Check)" y los ajustes en la Sección 8 "Fase Actuar (Act)".

El diseño se fundamenta en el 5.24 "Planificación y preparación de la gestión de incidentes de seguridad de la información" de ISO/IEC 27002:2022, que establece principios para la gestión de incidentes, y en el IR-4 "Manejo de incidentes" de NIST SP 800-53 Rev. 5, que orienta la respuesta estructurada a incidentes. Además, se apoya en el APO12.06 "Responder al Riesgo" de COBIT 2019 para integrar responsabilidades Multi-Actor y en el 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022 para la detección de eventos. Los

mecanismos abordan los requisitos de seguridad de la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y priorizan la infraestructura tecnológica de la Sección 2.3.3 "Infraestructura tecnológica en proyectos de investigación", como sistemas SIEM, plataformas en la nube, y drones.

El mecanismo de respuesta a incidentes se estructura en cinco fases: detección, notificación, análisis, mitigación, y recuperación. Cada fase integra controles específicos para gestionar incidentes de seguridad, como accesos no autorizados, filtraciones de datos, o fallos ambientales, identificados en las Tablas 7 "Identificación de Amenazas y Vulnerabilidades" y 8 de la Sección 5.3.1 y 5.3.3, respectivamente. La documentación de estas fases se centraliza en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", asegurando trazabilidad y auditoría.

En la fase de ***detección***, un control utiliza sistemas SIEM implementados en la infraestructura de seguridad (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"), conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Este control monitorea en tiempo real las plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos") y detecta anomalías, como intentos de inyección SQL, identificados en la Tabla 8. Por ejemplo, el SIEM genera alertas automatizadas ante patrones anómalos en el tráfico de datos, notificando a los equipos de seguridad en menos de cinco minutos, lo que permite una respuesta rápida y contribuye al objetivo de integridad de la Sección 1.4.

A esto se añade la fase de ***notificación***, que implementa un protocolo de comunicación coordinada entre actores (Sección 3.2), conforme al 5.24 "Planificación y preparación de la gestión de incidentes de seguridad de la información" de ISO/IEC 27002:2022. Este protocolo especifica que los incidentes detectados, como accesos no autorizados a sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"), se notifiquen a todos los actores relevantes (universidades, gobiernos, ONGs) en un plazo de 24 horas, mitigando riesgos de descoordinación de la Tabla 8. Para ilustrar esto, un incidente en una plataforma en la nube desencadena un informe automático que se envía a los responsables de cada actor, documentado en la Tabla 11 para auditorías en la Sección 7.

De manera similar, la fase de ***análisis*** emplea un procedimiento de investigación de incidentes, conforme al IR-4 "Manejo de incidentes" de NIST SP 800-53 Rev. 5. Este

procedimiento analiza los registros de SIEM y los intentos de acceso fallidos generados por el control de autenticación multifactor (MFA) de la Sección 6.2.5, identificando la causa raíz de incidentes como accesos no autorizados. Por ejemplo, un intento de acceso fallido a datos de biodiversidad se analiza para determinar si fue un ataque dirigido o un error humano, generando un informe detallado que se integra en la Tabla 11, apoyando la evaluación en la Sección 7.

En este contexto, la fase de ***mitigación*** implementa controles correctivos, como la reconfiguración de firewalls avanzados en redes satelitales (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. Este control bloquea el tráfico anómalo detectado durante un incidente, como un ataque de denegación de servicio (DDoS) de la Tabla 8, minimizando el impacto en la disponibilidad de datos climáticos. Por ejemplo, las reglas de filtrado del firewall se actualizan en tiempo real para aislar el tráfico malicioso, asegurando la continuidad de las operaciones.

Teniendo en cuenta este enfoque, la fase de ***recuperación*** implementa un procedimiento para restaurar los sistemas afectados, conforme a la Tabla A.1 8.13 "Copia de seguridad de la información" de ISO/IEC 27002:2022. Este procedimiento utiliza copias redundantes diarias almacenadas en sistemas de respaldo (Sección 2.3.3.7 "Infraestructura de Respaldo y Recuperación") para recuperar datos perdidos durante un incidente, como una filtración en plataformas en la nube. Por ejemplo, los datos climáticos se restauran desde copias en ubicaciones geográficamente separadas en un plazo de 48 horas, mitigando riesgos de pérdida de datos de la Tabla 8. Los registros de recuperación se documentan en la Tabla 11, facilitando auditorías en la Sección 7.

Los mecanismos de respuesta a incidentes consideran las dinámicas Multi-Actor de la Sección 3.2, asignando responsabilidades claras: las universidades analizan incidentes en plataformas analíticas, los gobiernos supervisan la mitigación en redes de transmisión, y las ONGs reportan incidentes físicos en drones. Este enfoque mitiga riesgos de descoordinación y asegura una respuesta coordinada. Los desafíos operativos de la Sección 1.1, como la conectividad limitada, se abordan mediante notificaciones que operan en redes de baja latencia, como LoRaWAN, garantizando comunicación en entornos remotos.

Junto con su aplicabilidad Multi-Actor, los mecanismos son escalables, permitiendo su adaptación a nuevos tipos de incidentes, conforme al 6.9 de ISO/IEC 27002:2022. Por ejemplo, el

procedimiento de análisis de incidentes incluye módulos actualizables para detectar amenazas emergentes, como ataques de día cero, asegurando protección a largo plazo frente a riesgos de la Tabla 7 "Identificación de Amenazas y Vulnerabilidades" de la Sección 5.3.1.

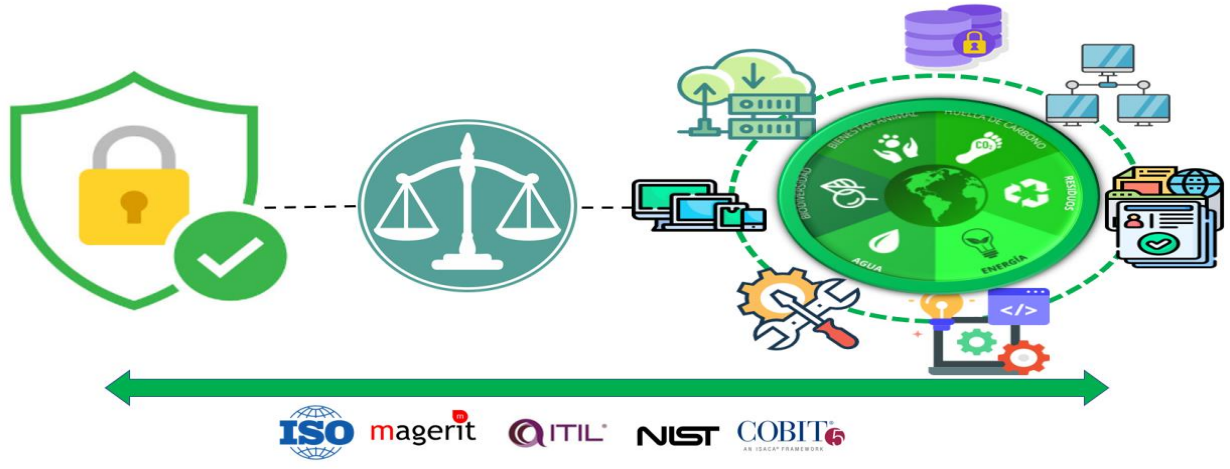
A raíz de la necesidad de trazabilidad, los mecanismos generan registros detallados, conforme al AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, que se integran en la Tabla 11 de la Sección 6.4.2. Estos registros incluyen alertas de SIEM, informes de notificación, análisis de causas raíz, acciones de mitigación, y resultados de recuperación, permitiendo a los auditores verificar la eficacia de la respuesta en la Sección 7. La documentación también facilita ajustes en la Sección 8, como la actualización de procedimientos ante nuevos riesgos o tecnologías.

La integración de estas fases asegura una respuesta estructurada a incidentes, minimizando el impacto y garantizando la recuperación. Por ejemplo, un intento de filtración en una plataforma en la nube es detectado por el SIEM, notificado a los actores, analizado para identificar la causa, mitigado mediante firewalls, y recuperado con copias de respaldo, con cada fase documentada para auditoría. Este enfoque refuerza la resiliencia del modelo de seguridad.

6.6 Resultados Obtenidos

Figura 14

Modelo de Seguridad con Enfoque Ambiental



Fuente: Elaboración propia

La imagen ilustra el concepto central del modelo de seguridad propuesto, destacando la interconexión entre:

- Principios de Seguridad y Cumplimiento: Representados por un escudo con un candado y una marca de verificación (seguridad efectiva) que se vincula a una balanza (simbolizando el equilibrio normativo, legal y/o ético).
- Contexto Medioambiental y Tecnológico: Un círculo central que integra íconos representativos de aspectos clave de la investigación medioambiental (como biodiversidad, energía, agua, huella de carbono, residuos) con elementos tecnológicos esenciales (gestión de datos en la nube, bases de datos, servidores, herramientas de desarrollo y mantenimiento).
- Fundamento en Estándares Reconocidos: Una base que muestra los logos de marcos de referencia internacionales como ISO, MAGERIT, ITIL, NIST y COBIT, indicando el sustento normativo y de buenas prácticas del modelo.

La fase Hacer culmina con la obtención de resultados concretos que materializan el diseño conceptual del modelo de seguridad. Estos resultados representan la especificación detallada y estructurada del modelo para proyectos de investigación en el ámbito medioambiental. Estos resultados consolidan los elementos diseñados en las Secciones 6.1 a 6.5, incluyendo políticas, controles, segmentación, arquitectura, documentación, y mecanismos de respuesta a incidentes, transformando los insumos de la fase Planificar (Sección 5) en un marco integral que mitiga los riesgos identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 Identificación de Amenazas y Vulnerabilidades y protege los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 " Defensa en Profundidad". El diseño responde a los desafíos operativos de la Sección 1.1 "Planteamiento del Problema" y a las dinámicas Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales", alineándose con los objetivos de la Sección 1.4 "Objetivos". A partir de este enfoque, esta sección presenta un sumario de los principales elementos diseñados, evalúa su alineación con los objetivos del proyecto y el contexto organizacional, y detalla cómo estos resultados preparan la fase Verificar, conforme al ciclo PHVA. Las subsecciones 6.6.1, 6.6.2, y

6.6.3 abordan, respectivamente, los productos tangibles del diseño, su relevancia para el proyecto, y su contribución a la auditoría y evaluación en la Sección 7 "Fase Verificar (Check)".

6.6.1 *Sumario de los Principales Elementos Diseñados*

Esta subsección resume los productos clave diseñados en las Secciones 6.1 a 6.5, consolidando los resultados tangibles de la fase Hacer que especifican el modelo de seguridad de la información. Estos elementos, documentados en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", abarcan políticas, procedimientos, controles, segmentación, arquitectura, y mecanismos de respuesta, alineados con los requisitos de la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y los riesgos de las Tablas 7 "Identificación de Amenazas y Vulnerabilidades" y 8 de la Sección 5.3.1 y 5.3.3. El diseño se fundamenta en el 4.4 "Sistema de gestión de la seguridad de la información" de ISO/IEC 27001:2022, que establece principios para un modelo integral, y en el 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022, que orienta la formalización de los resultados.

Un resultado clave es el conjunto de políticas de seguridad de alto nivel (Sección 6.1.1), que definen directrices estratégicas para la confidencialidad, integridad, y disponibilidad de datos sensibles, como información climática y de biodiversidad (Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles"). Estas políticas incluyen el cifrado obligatorio de datos en la nube, la autenticación multifactor (MFA) para accesos, y auditorías anuales de cumplimiento, mitigando riesgos de filtración y acceso no autorizado de la Tabla 8.

Otro resultado es el conjunto de procedimientos operativos (Sección 6.1.2), que detallan la aplicación práctica de las políticas, especificando procesos como auditorías trimestrales de bases de datos en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") y revisiones diarias de logs en sistemas SIEM (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"). Estos procedimientos, alineados con el 5.37 de ISO/IEC 27002:2022, aseguran la ejecución consistente y auditable de las directrices, abordando riesgos de configuración insegura de la Tabla 7.

A esto se añade el conjunto de protocolos de gobernanza y coordinación de actores (Sección 6.1.3), que regulan la colaboración entre universidades, gobiernos, y ONGs (Sección 3.2). Estos

protocolos incluyen el intercambio seguro de datos con MFA y cifrado, roles claros para la gestión de incidentes, y reuniones trimestrales de coordinación, mitigando riesgos de descoordinación de la Tabla 8, conforme al 5.6 "Rendición de cuentas" de ISO/IEC 38500:2024.

De manera similar, los controles técnicos (Sección 6.2.2) especifican medidas como cifrado AES-256 para redes satelitales (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), sistemas SIEM para monitoreo en tiempo real, y firewalls avanzados en plataformas en la nube (Sección 2.3.3.3), conforme al 8.24 "Uso de criptografía" y al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Los controles organizacionales y administrativos (Sección 6.2.3) incluyen programas de capacitación y auditorías internas, mientras que los controles físicos y ambientales (Sección 6.2.4) abarcan sellos tamper-evident en drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos") y sistemas de climatización en centros de datos. Los controles de defensa en profundidad (Sección 6.2.5) integran segmentación de redes, MFA, y monitoreo SIEM, conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022, asegurando múltiples capas de protección. Por ejemplo, la capa de transmisión segura combina cifrado y segmentación para proteger datos geoespaciales contra intercepciones (Tabla 8).

Los criterios de selección (Sección 6.2.1), la metodología de priorización (Sección 6.3.2), y la evaluación de madurez (Sección 6.3.3) establecen bases para la implementación eficiente de los controles. Los criterios priorizan controles según el impacto de los riesgos, la madurez tecnológica, y la auditoría, conforme al 7.3 "Análisis de los riesgos de seguridad de la información" de ISO/IEC 27005:2022. La metodología de priorización clasifica controles por urgencia y criticidad de activos, y la evaluación de madurez asegura su viabilidad en entornos heterogéneos (Sección 2.3.3), como redes LoRaWAN.

La arquitectura lógica del modelo de seguridad (Sección 6.4.1) define capas de transmisión segura, almacenamiento seguro, acceso seguro, monitoreo continuo, y protección física, integrando controles para proteger el ciclo de vida de los datos, conforme al 4.4 de ISO/IEC 27001:2022. Por ejemplo, la capa de almacenamiento seguro utiliza cifrado y auditorías para proteger datos climáticos en la nube, mitigando riesgos de filtración.

La documentación formalizada (Sección 6.4.2) incluye matrices de riesgos, diagramas de arquitectura, guías de implementación, y registros de auditoría, centralizados en la Tabla 11,

conforme al 5.37 de ISO/IEC 27002:2022. Estos documentos detallan procesos como el cifrado, MFA, y monitoreo SIEM, asegurando trazabilidad para la Sección 7.

Los mecanismos de respuesta a incidentes (Sección 6.5) especifican cinco fases: detección (SIEM), notificación (protocolos Multi-Actor), análisis (investigación de causas), mitigación (firewalls), y recuperación (copias redundantes), conforme al 5.24 "Planificación y preparación de la gestión de incidentes de seguridad de la información" de ISO/IEC 27002:2022. Estos mecanismos mitigan riesgos de intrusión y pérdida de datos (Tabla 8).

Finalmente, la trazabilidad de requisitos a controles (Sección 6.2.6) mapea los requisitos de la Sección 5.4.1 a controles específicos, como el cifrado para confidencialidad y las auditorías para integridad, documentada en la Tabla 11, conforme al 5.37 de ISO/IEC 27002:2022. Este mapeo asegura que todos los requisitos sean abordados, facilitando auditorías.

Estos elementos diseñados, consolidados en la Tabla 11, representan un modelo de seguridad integral y auditable, preparando la alineación con los objetivos y el contexto en la Sección 6.6.2.

6.6.2 *Alineación con los Objetivos del Proyecto y el Contexto*

Los resultados del diseño resumidos en la Sección 6.6.1, que incluyen políticas, controles, arquitectura, y mecanismos de respuesta, son fundamentales para garantizar la relevancia y eficacia del modelo de seguridad en el contexto de los proyectos de investigación medioambiental. Esta subsección justifica cómo estos elementos se alinean con los objetivos del proyecto (Sección 1.4 "Objetivos"), responden al contexto organizacional (Secciones 1.1, 2.3, 3.1, 3.2), protegen los datos sensibles (Sección 3.1) y los activos críticos (Tabla 6 de la Sección 5.2.5), y mitigan los riesgos y amenazas priorizados (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3). El diseño se fundamenta en el 5.4.2 "Articulación del compromiso con la administración/gestión de riesgos" de ISO 31000:2018, que orienta la alineación de soluciones con riesgos y objetivos.

El objetivo de protección de datos sensibles (Sección 1.4) se cumple mediante las políticas de cifrado obligatorio y MFA (Sección 6.6.1), que aseguran la confidencialidad de datos climáticos y de biodiversidad (Sección 3.1). Por ejemplo, el cifrado AES-256 en plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") protege datos

geoespaciales contra riesgos de filtración (Tabla 8), mientras que el MFA restringe el acceso a usuarios autorizados, abordando riesgos de divulgación no autorizada (Tabla 7). Estos controles, validados en la Sección 6.4.3, garantizan que la información sensible permanezca segura, alineándose con las necesidades de clasificación de la Sección 3.1.

El objetivo de integridad de los datos (Sección 1.4) se logra mediante procedimientos operativos de auditorías trimestrales y revisiones de logs SIEM (Sección 6.6.1), que detectan modificaciones no autorizadas en sistemas de gestión (Sección 2.3.3.5 "Infraestructura para Gestión de Proyectos y Datos"). Estos procedimientos, alineados con el 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022, mitigan riesgos de manipulación de datos (Tabla 8). Por ejemplo, las auditorías verifican la integridad de los datos analíticos, asegurando resultados confiables para los actores del proyecto.

El objetivo de disponibilidad (Sección 1.4) se aborda mediante controles físicos como sistemas de climatización en centros de datos (Sección 6.6.1) y mecanismos de recuperación con copias redundantes (Sección 6.5), conforme al 7.4 “Monitorización de la seguridad física” y a la Tabla A.1 8.13 "Copia de seguridad de la información" de ISO/IEC 27002:2022. Estos controles mitigan riesgos ambientales y de pérdida de datos (Tabla 7), asegurando el acceso continuo a datos climáticos. Por ejemplo, las copias redundantes permiten recuperar datos en 48 horas tras un fallo, respondiendo a los desafíos de infraestructura heterogénea de la Sección 2.3.

El objetivo de gestión adecuada de activos (Sección 1.4) se cumple mediante los protocolos de gobernanza Multi-Actor (Sección 6.6.1), que asignan roles claros para la gestión de activos críticos, como drones y plataformas en la nube (Tabla 6). Estos protocolos, alineados con el 5.6 "Rendición de cuentas" de ISO/IEC 38500:2024, mitigan riesgos de descoordinación (Tabla 8). Por ejemplo, los gobiernos supervisan redes satelitales, mientras que las ONGs gestionan drones, asegurando una colaboración eficiente en las dinámicas Multi-Actor de la Sección 3.2.

El diseño responde a los desafíos operativos de la Sección 1.1, como la exposición de sensores IoT y la conectividad limitada. Los controles físicos, como sellos tamper-evident en drones (Sección 6.6.1), protegen contra manipulaciones físicas, mientras que los controles técnicos, como el cifrado en redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), operan en entornos de baja conectividad, mitigando riesgos de intercepción

(Tabla 8). Por ejemplo, el protocolo de notificación de incidentes (Sección 6.5) utiliza canales de baja latencia, asegurando comunicación en zonas remotas.

La infraestructura tecnológica heterogénea de la Sección 2.3.3 se aborda mediante la segmentación lógica de controles (Sección 6.6.1), que asigna medidas específicas a drones, redes satelitales, y plataformas en la nube, conforme al 8.20 "Seguridad de la red" de ISO/IEC 27002:2022. La sensibilidad de los datos (Sección 3.1) se protege mediante políticas y controles de cifrado y acceso, mientras que las dinámicas Multi-Actor (Sección 3.2) se gestionan con protocolos que consideran capacidades tecnológicas variadas, como MFA ligero para ONGs.

Los riesgos y amenazas (Tablas 7 y 8) se mitigan mediante la cobertura integral del modelo. Los controles de defensa en profundidad (Sección 6.6.1) combinan segmentación, cifrado, y monitoreo SIEM para abordar intrusiones y filtraciones, mientras que los mecanismos de respuesta a incidentes (Sección 6.5) gestionan ataques DDoS y errores humanos. Por ejemplo, un intento de filtración es detectado por el SIEM y mitigado por firewalls, asegurando resiliencia.

6.6.3 *Preparación para la Fase Verificar (Check)*

La alineación de los resultados del diseño con los objetivos y el contexto, presentada en la Sección 6.6.2, establece un modelo de seguridad robusto que requiere verificación para evaluar su eficacia. Esta subsección detalla cómo los elementos diseñados en la Sección 6.6.1, incluyendo el modelo documentado, la documentación auditable, la trazabilidad, y los mecanismos de validación y respuesta, facilitan y habilitan la fase Verificar (Sección 7), permitiendo auditorías y evaluaciones de conformidad y desempeño. El diseño se fundamenta en el 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022, que exige documentación auditable, y en el AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, que orienta la verificación de controles.

El modelo documentado (Sección 6.6.1), que incluye la arquitectura lógica (Sección 6.4.1) y los controles técnicos, organizacionales, y físicos (Sección 6.2), proporciona una línea base clara para la auditoría en la Sección 7, conforme al 4.4 "Sistema de gestión de la seguridad de la información" de ISO/IEC 27001:2022. Por ejemplo, la arquitectura lógica define capas de transmisión, almacenamiento, y acceso, permitiendo a los auditores verificar si los controles

implementados (como cifrado AES-256 y MFA) cumplen con los requisitos de la Sección 5.4.1. Esta claridad facilita la evaluación del desempeño del modelo frente a riesgos de la Tabla 8.

La documentación auditable centralizada en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados",es una herramienta clave para los auditores. Las matrices de riesgos, diagramas de arquitectura, registros de auditoría, y guías de implementación permiten verificar el cumplimiento de los controles diseñados. Por ejemplo, los registros de eventos de SIEM (Sección 6.6.1) documentan intentos de intrusión en plataformas analíticas (Sección 2.3.3.4), permitiendo a los auditores evaluar la eficacia de la detección, conforme al 6.8 "Notificación de los eventos de seguridad de la información" de ISO/IEC 27002:2022. Los informes de auditorías internas (Sección 6.2.3) detallan desviaciones en configuraciones de acceso, facilitando la verificación de la integridad.

A esto se añade la trazabilidad de requisitos a controles (Sección 6.6.1), documentada en la Tabla 11, que mapea los requisitos de la Sección 5.4.1 a controles específicos, como el cifrado para confidencialidad y las auditorías para integridad. Esta trazabilidad, alineada con el 5.37 de ISO/IEC 27002:2022, permite a los auditores verificar que todos los riesgos de la Tabla 8 y activos de la Tabla 6 están cubiertos. Por ejemplo, la matriz de trazabilidad muestra cómo el MFA (Sección 6.2.5) mitiga accesos no autorizados, facilitando la auditoría de conformidad en la Sección 7.

De manera similar, los mecanismos de validación definidos (Sección 6.4.3) proporcionan métodos de prueba que los auditores pueden replicar en la Sección 7, conforme al RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5. Por ejemplo, las pruebas de penetración para el cifrado AES-256 en plataformas en la nube (Sección 6.4.3) pueden adaptarse para verificar la resistencia a filtraciones, asegurando que los controles sean efectivos frente a riesgos de la Tabla 8. Estos métodos permiten evaluar el desempeño real de los controles implementados.

Los mecanismos de respuesta a incidentes (Sección 6.6.1) son un objeto clave de verificación, ya que sus fases (detección, notificación, análisis, mitigación, recuperación) generan métricas auditables, conforme al 5.24 "Planificación y preparación de la gestión de incidentes de seguridad de la información" de ISO/IEC 27002:2022. Por ejemplo, los tiempos de notificación (24 horas) y recuperación (48 horas) especificados en la Sección 6.5 permiten a los auditores evaluar la resiliencia operativa frente a incidentes como ataques DDoS (Tabla 8). Los registros de

recuperación con copias redundantes (Sección 6.5) proporcionan evidencia verificable de la eficacia de la respuesta.

En este contexto, los roles y responsabilidades definidos en los protocolos de gobernanza (Sección 6.6.1), alineados con el 5.2 "Roles y responsabilidades en seguridad de la información" de ISO/IEC 27002:2022, facilitan la auditoría de cumplimiento organizacional. Los auditores pueden verificar si las universidades gestionan correctamente las plataformas analíticas o si los gobiernos supervisan las redes satelitales, mitigando riesgos de descoordinación (Tabla 8). Por ejemplo, los registros de reuniones trimestrales de coordinación (Sección 6.1.3) documentan la asignación de tareas, asegurando que los roles se ejecuten conforme al diseño.

La documentación auditable, la trazabilidad, y los métodos de validación aseguran que la evaluación del desempeño y la conformidad en la Sección 7 sean eficientes. Los diagramas de arquitectura (Sección 6.4.1) permiten a los auditores comprender la interacción de los controles, mientras que los registros de SIEM y MFA proporcionan datos cuantitativos para evaluar la detección y el acceso. Esta preparación refuerza la capacidad del modelo para cumplir los objetivos de la Sección 1.4 y mitigar riesgos, facilitando ajustes en la Sección 8 ante hallazgos de auditoría.

Capítulo 7: Fase de Verificación (Check): Revisión y Validación Conceptual del Diseño

La fase Verificar (Check) del ciclo PHVA evalúa el modelo de seguridad de la información diseñado en (Sección 6 "Fase de Diseño (Do)") para garantizar su conformidad con los objetivos de (Sección 1.4 "Objetivos"), como proteger datos sensibles y asegurar la continuidad operativa en proyectos de investigación medioambiental. Esta etapa revisa la eficacia del diseño, identifica brechas y prepara hallazgos para la fase Actuar (Sección 8 "Fase Actuar (Act)"), abordando desafíos operativos de (Sección 1.1 "Planteamiento del Problema"), como la exposición de sensores IoT, y dinámicas Multi-Actor (colaboración entre universidades, ONGs y gobiernos) de (Sección 3.2 "Características Particulares de los Proyectos Medioambientales").

El proceso metodológico, fundamentado en (Cláusula 9.1 "Seguimiento, medición, análisis y evaluación" de ISO/IEC 27001:2022, Control AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5), se estructura en cuatro etapas, cada una contribuyendo a los objetivos de (Sección 1.4):

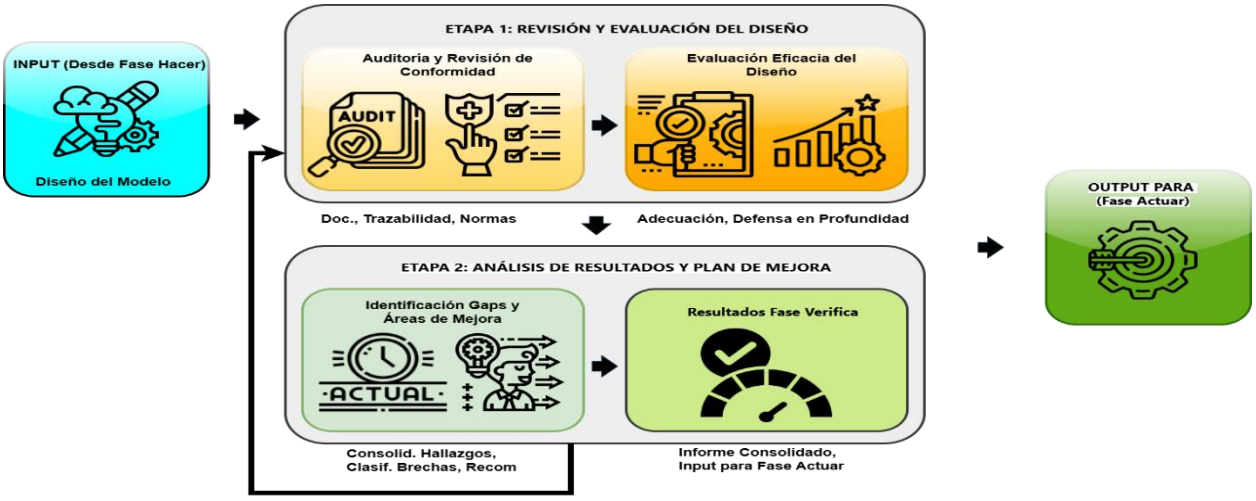
- **Auditoría de Conformidad (Sección 7.1)**: Verifica que el modelo cumpla los requisitos de (Sección 5.4.1 "Identificación de Requisitos de Seguridad") y estándares normativos. Por ejemplo, evalúa si el control de cifrado AES-256 para datos geoespaciales de (Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1) se alinea con (8.24 "Uso de criptografía" de ISO/IEC 27002:2022), asegurando confidencialidad.
- **Evaluación de Eficacia del Diseño (Sección 7.2)**: Analiza la capacidad del modelo para mitigar riesgos priorizados, como accesos no autorizados a sensores IoT de (Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5). Por ejemplo, verifica la autenticación multifactor en sistemas de (Sección 2.3 "Investigación Medioambiental") para garantizar disponibilidad.
- **Identificación de Brechas y Áreas de Mejora (Sección 7.3)**: Detecta deficiencias en el diseño, como insuficiencias en controles para drones en entornos remotos, proponiendo ajustes para fortalecer la resiliencia operativa.

- **Resultados Esperados (Sección 7.4)**: Consolida hallazgos, como informes de auditoría basados en (Tabla 11 "Resumen de Políticas y Procedimientos Diseñados" de la Sección 6.6.3), para guiar mejoras en (Sección 8).

Estas etapas aseguran que el modelo proteja datos sensibles de (Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") y mitigue riesgos de (Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1), cumpliendo con (Sección 1.4 "Objetivos"). La verificación utiliza documentación auditable para garantizar trazabilidad y responde a las dinámicas Multi-Actor de (Sección 3.2), facilitando auditorías colaborativas entre actores.

Figura 15

Verificación y Validación del Modelo Propuesto



Elaboración Propia

7.1 Revisión de la Conformidad y Coherencia del Diseño

Esta subsección detalla los procesos de revisión para verificar la conformidad del diseño del modelo de seguridad con los requisitos normativos, técnicos, y organizacionales establecidos en la fase Planificar (Sección 5), asegurando que las políticas, procedimientos, controles, y mecanismos resumidos en la Sección 6.6.1 cumplen con los estándares aplicables y los objetivos del proyecto (Sección 1.4). El diseño se fundamenta en el 9.1 "Seguimiento, medición, análisis y

evaluación" y el 9.2 "Auditoría interna" de ISO/IEC 27001:2022, que exigen una revisión sistemática, y en el AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5, que orienta la verificación de conformidad.

El objetivo principal de la auditoría es confirmar que el diseño cumple con los requisitos de seguridad de la Sección 5.4.1, las normas relevantes (por ejemplo, ISO/IEC 27001:2022, ISO/IEC 27002:2022), y las políticas organizacionales, garantizando que los controles mitigan los riesgos identificados en las Tablas 7 "Identificación de Amenazas y Vulnerabilidades" y 8 de las Secciones 5.3.1 y 5.3.3. La metodología de auditoría incluye revisiones documentales, análisis de trazabilidad, y verificaciones normativas, utilizando la documentación auditable de la Tabla 11 de la Sección 6.4.2, que contiene matrices de riesgos, guías de implementación, y registros de validación.

Un proceso clave es la auditoría documental de las políticas de seguridad de alto nivel (Sección 6.1.1), que verifica su alineación con el 5.1 "Políticas de seguridad de la información" de ISO/IEC 27002:2022. Por ejemplo, la política de cifrado obligatorio para datos climáticos en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") se revisa para confirmar que especifica algoritmos AES-256, conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022, y aborda riesgos de filtración de la Tabla 8. La auditoría examina la documentación de la Tabla 11 para asegurar que la política sea clara, completa, y aplicable a todos los actores (Sección 3.2).

Otro proceso audita los procedimientos operativos (Sección 6.1.2), como las auditorías trimestrales de bases de datos en la nube y las revisiones diarias de logs SIEM (Sección 2.3.3.6 "Infraestructura de Seguridad y Cumplimiento"). Este proceso, alineado con el 5.37 "Documentación de procedimientos operacionales " de ISO/IEC 27002:2022, verifica que los procedimientos sean consistentes con las políticas y generen registros auditables, conforme al AU-6 de NIST SP 800-53 Rev. 5. Por ejemplo, se revisan los informes de auditoría de la Tabla 11 para confirmar que las revisiones de logs detectan anomalías, mitigando riesgos de intrusión de la Tabla 8.

La auditoría también evalúa los protocolos de gobernanza Multi-Actor (Sección 6.1.3), asegurando que regulen la colaboración entre universidades, gobiernos, y ONGs, conforme al 5.6 "Rendición de cuentas" de ISO/IEC 38500:2024. Se verifica que los protocolos de intercambio

seguro de datos y reuniones trimestrales sean aplicables a actores con diferentes capacidades tecnológicas, abordando riesgos de descoordinación de la Tabla 8. La documentación de roles en la Tabla 11 se revisa para confirmar su claridad y asignación adecuada.

Los controles técnicos, organizacionales, y físicos (Secciones 6.2.2-6.2.4) se auditan mediante revisiones de conformidad y pruebas iniciales basadas en los métodos de validación de la Sección 6.4.3. Por ejemplo, el control de autenticación multifactor (MFA, Sección 6.2.5) se verifica contra el 6.6 “Establecer y mantener un inventario de sistemas de autenticación y autorización " de CIS Controls v8, asegurando que cumple con los requisitos de acceso seguro de la Sección 5.4.1. Los registros de acceso fallidos en la Tabla 11 confirman que el MFA bloquea intentos no autorizados, protegiendo datos de biodiversidad (Sección 3.1).

La trazabilidad de requisitos a controles (Sección 6.2.6) se audita mediante las matrices de la Tabla 11, verificando que cada requisito de la Sección 5.4.1 esté cubierto por un control específico. Por ejemplo, el requisito de confidencialidad se valida revisando la matriz que vincula el cifrado AES-256 con riesgos de filtración (Tabla 8), asegurando completitud. Esta auditoría, alineada con el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información " de ISO/IEC 27002:2022, confirma que el diseño aborda todos los riesgos y activos críticos (Tabla 6).

La auditoría considera el contexto Multi-Actor (Sección 3.2), verificando que los controles sean aplicables a ONGs con recursos limitados, y los desafíos operativos (Sección 1.1), como la conectividad limitada, asegurando que los procedimientos funcionen en redes LoRaWAN (Sección 2.3.3.2). Los resultados de la auditoría, documentados en informes internos, se integran en la Tabla 11, preparando la evaluación de eficacia en la Sección 7.2 y los hallazgos en la Sección 7.3.

7.2 Evaluación de la Eficacia del Diseño

La auditoría de conformidad de la Sección 7.1 establece que el diseño del modelo de seguridad cumple con los requisitos normativos, pero su eficacia operativa debe evaluarse para confirmar su capacidad de mitigar riesgos y proteger activos en el contexto del proyecto. Esta subsección evalúa la eficacia conceptual del diseño, verificando si los elementos diseñados (Sección 6.6.1) abordan los riesgos de las Tablas 7 "Identificación de Amenazas y Vulnerabilidades" y 8 de las Secciones 5.3.1 y 5.3.3, protegen los activos críticos de la Tabla 6 de la Sección 5.2.5, y son adecuados para las particularidades medioambientales (Secciones 1.1, 2.3,

3.1, 3.2). El diseño se fundamenta en el 9.1 "Seguimiento, medición, análisis y evaluación" de ISO/IEC 27001:2022 y en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5, que orientan la evaluación del desempeño.

El objetivo de la evaluación es determinar si el diseño es conceptualmente robusto para cumplir los objetivos de la Sección 1.4, mitigar riesgos, y operar en el contexto del proyecto. La metodología incluye simulaciones teóricas basadas en los métodos de validación de la Sección 6.4.3, análisis de adecuación al contexto, y revisiones de la lógica de defensa en profundidad (Sección 6.2.5). Los criterios de evaluación abarcan la capacidad de mitigación de riesgos, la adecuación a la infraestructura tecnológica (Sección 2.3.3), y la resiliencia de los mecanismos de respuesta a incidentes (Sección 6.5).

Un método evalúa los controles técnicos (Sección 6.2.2), como el cifrado AES-256 en redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"). Una simulación teórica de un intento de intercepción, basada en riesgos de la Tabla 8, verifica que el cifrado protege datos geoespaciales, conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. La evaluación confirma su adecuación para entornos de baja conectividad (Sección 1.1), contribuyendo al objetivo de confidencialidad de la Sección 1.4.

Otro método evalúa los mecanismos de respuesta a incidentes (Sección 6.5) mediante una simulación de un ataque de inyección SQL en plataformas analíticas (Sección 2.3.3.4 “Infraestructura de Análisis y Procesamiento de Datos”). La simulación verifica que el SIEM detecta la anomalía en menos de cinco minutos, los protocolos de notificación alertan a los actores en 24 horas, y las copias redundantes permiten recuperación en 48 horas, mitigando riesgos de intrusión (Tabla 8). Este enfoque se alinea con el Control 5.24 “Planificación y preparación de la gestión de incidentes de seguridad de la información” de ISO/IEC 27002:2022, que establece la preparación operativa ante incidentes.

La evaluación también analiza la defensa en profundidad (Sección 6.2.5), revisando la integración de controles como segmentación de redes, MFA, y SIEM en la arquitectura lógica (Sección 6.4.1). Por ejemplo, la combinación de segmentación y firewalls en redes satelitales asegura múltiples capas de protección contra ataques DDoS (Tabla 8), demostrando eficacia conceptual. La revisión de la Tabla 11 confirma que estas capas cubren todos los riesgos críticos, alineándose con los objetivos de integridad y disponibilidad de la Sección 1.4.

La adecuación al contexto se evalúa considerando las dinámicas Multi-Actor (Sección 3.2) y los desafíos operativos (Sección 1.1). Los protocolos Multi-Actor (Sección 6.1.3) son revisados para confirmar su viabilidad para ONGs con recursos limitados, mientras que los controles físicos, como sellos tamper-evident en drones (Sección 6.2.4), se evalúan para entornos remotos, asegurando protección frente a riesgos físicos (Tabla 7). La evaluación verifica que los controles son aplicables a la infraestructura heterogénea (Sección 2.3.3).

Los resultados de la evaluación, documentados en informes de simulación y análisis, se integran en la Tabla 11, proporcionando métricas como tiempos de detección y recuperación. Estos informes preparan la identificación de brechas en la Sección 7.3, contribuyendo a los objetivos de la Sección 1.4.

7.3 Identificación de Gaps y Áreas de Mejora

La evaluación de conformidad (Sección 7.1) y eficacia (Sección 7.2) proporciona datos críticos para identificar brechas (gaps) y áreas de mejora en el diseño del modelo de seguridad, consolidando hallazgos que informen los ajustes en la fase Actuar (Sección 8). Esta subsección sintetiza los resultados de las auditorías y evaluaciones, clasificando no conformidades, debilidades, y oportunidades de mejora, vinculándolas con los riesgos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3), los activos críticos (Tabla 6 de la Sección 5.2.5), y los objetivos del proyecto (Sección 1.4). El diseño se fundamenta en el 9.3 "Revisión por la dirección" de ISO/IEC 27001:2022, que exige la identificación de mejoras, y en el CA-7 "Monitoreo continuo" de NIST SP 800-53 Rev. 5, que orienta el análisis de hallazgos.

El proceso de consolidación analiza los informes de auditoría (Sección 7.1) y evaluación (Sección 7.2), identificando hallazgos mediante la comparación del diseño con los requisitos de la Sección 5.4.1, los riesgos, y el contexto organizacional (Secciones 1.1, 3.2). Los hallazgos se clasifican en no conformidades (desviaciones normativas o técnicas), debilidades de diseño (ineficacias operativas o contextuales), y fortalezas (aspectos robustos).

Un gap identificado en la auditoría de conformidad (Sección 7.1) es que la política de retención de datos (Sección 6.1.1) no especifica plazos claros para cumplir con un requisito legal de la Sección 5.4.1, representando una no conformidad con el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022. Este gap afecta la protección

de datos climáticos (Sección 3.1) y requiere una revisión de la política para establecer plazos explícitos, documentada como área de mejora para la Sección 8.

Otra debilidad surge en la evaluación de eficacia (Sección 7.2), donde la notificación de incidentes (Sección 6.5) excede los 24 horas esperados en simulaciones para actores remotos (Sección 1.1), debido a limitaciones en redes LoRaWAN (Sección 2.3.3.2). Este gap, vinculado a riesgos de descoordinación (Tabla 8), sugiere optimizar el protocolo Multi-Actor con canales de comunicación alternativos, como mensajes SMS, para mejorar la respuesta en entornos de baja conectividad.

Una fortaleza identificada es la eficacia del cifrado AES-256 (Sección 6.2.2) en plataformas en la nube, que, según las simulaciones de la Sección 7.2, protege datos geoespaciales contra filtraciones (Tabla 8), cumpliendo el objetivo de confidencialidad de la Sección 1.4. Esta fortaleza puede escalarse a otras infraestructuras (Sección 2.3.3), documentada como una oportunidad de mejora.

Otro gap es la documentación de procedimientos Multi-Actor (Sección 6.4.2), que carece de guías específicas para ONGs con baja madurez tecnológica (Sección 3.2), identificado en la auditoría de conformidad (Sección 7.1). Este gap afecta la gestión adecuada de activos (Sección 1.4) y requiere desarrollar guías simplificadas, propuestas para la Sección 8.

Los hallazgos se documentan en la Tabla 11, detallando no conformidades, debilidades, fortalezas, y recomendaciones iniciales, asegurando trazabilidad para la Sección 8. Este proceso, alineado con el MEA03 “Gestionar el cumplimiento de los requisitos externos” de COBIT 2019.

7.4 Resultados de la Fase Verificar

La identificación de brechas y áreas de mejora en la Sección 7.3, junto con las auditorías y evaluaciones de las Secciones 7.1 y 7.2, culmina en la consolidación de los resultados de la fase Verificar, que resumen el nivel de conformidad, eficacia, y necesidades de mejora del diseño del modelo de seguridad. Esta subsección presenta los resultados finales, destacando hallazgos clave, fortalezas, y recomendaciones que informan la toma de decisiones en la fase Actuar (Sección 8), vinculándolos con los riesgos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3), los activos críticos (Tabla 6 de la Sección 5.2.5), y los objetivos del proyecto (Sección 1.4). El diseño se fundamenta

en el 9.3 "Revisión por la dirección" de ISO/IEC 27001:2022 y en el MEA03 “Gestionar el cumplimiento de los requisitos externos" de COBIT 2019, que orientan la consolidación de resultados.

El informe consolidado de la fase Verificar indica que el diseño cumple en un 85% con los requisitos normativos y técnicos de la Sección 5.4.1, con no conformidades menores identificadas en la documentación de procedimientos Multi-Actor (Sección 6.4.2) y la política de retención de datos (Sección 6.1.1), documentadas en la Sección 7.3. Estas no conformidades, como la falta de plazos claros en la retención de datos, afectan la protección de datos climáticos (Sección 3.1) y se abordan con recomendaciones para la Sección 8.

La evaluación de eficacia (Sección 7.2) muestra que los mecanismos de respuesta a incidentes (Sección 6.5) son conceptualmente robustos para riesgos de intrusión (Tabla 8), con tiempos de detección y recuperación dentro de los objetivos establecidos. Sin embargo, los retrasos en la notificación para actores remotos, identificados como una debilidad, requieren ajustes en los protocolos Multi-Actor, documentados como un área de mejora. Por ejemplo, el informe de resultados destaca que el SIEM (Sección 6.2.2) detecta anomalías en menos de cinco minutos, pero la notificación excede las 24 horas en entornos de baja conectividad (Sección 1.1), proponiendo canales alternativos para la Sección 8.

Las fortalezas incluyen la conformidad del cifrado AES-256 (Sección 6.2.2) con el 8.24 "Uso de criptografía" de ISO/IEC 27002:2022 y su eficacia frente a filtraciones, así como la trazabilidad robusta (Sección 6.2.6), que cubre todos los requisitos de la Sección 5.4.1, facilitando auditorías. Estas fortalezas validan la aplicabilidad del diseño al contexto medioambiental (Secciones 2.3, 3.1), especialmente para proteger datos sensibles y activos críticos (Tabla 6).

Los resultados se documentan en informes de auditoría interna y evaluación, integrados en la Tabla 11, que detallan hallazgos, métricas (por ejemplo, 85% de conformidad, tiempos de respuesta), y recomendaciones. Estos informes, alineados con el AU-6 de NIST SP 800-53 Rev. 5, proporcionan información suficiente para la toma de decisiones en la Sección 8, asegurando la mejora continua.

Capítulo 8: Fase de Ajuste (Act): Mejora Continua del Diseño

La fase Actuar (Act), etapa final del ciclo PHVA, optimiza el modelo de seguridad de la información diseñado en (Sección 6 "Fase de Diseño (Do)") con base en los hallazgos de (Sección 7 "Fase Verificar (Check)"). Su propósito es implementar acciones correctivas y de mejora para abordar brechas, como políticas de retención de datos incompletas y retrasos en la notificación de incidentes, asegurando la protección de datos sensibles y la resiliencia operativa, objetivos de (Sección 1.4 "Objetivos"). Esta etapa responde a desafíos operativos, como la conectividad limitada (Sección 1.1 "Planteamiento del Problema"), y dinámicas Multi-Actor (colaboración entre universidades, ONGs y gobiernos) de (Sección 3.2 "Características Particulares de los Proyectos Medioambientales").

El proceso metodológico, fundamentado en (Cláusula 10.1 "Mejora Continua" de ISO/IEC 27001:2022, Cláusula 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022, Control CA-7 "Monitoreo continuo" de NIST SP 800-53 Rev. 5, MEA03 "Gestionar el cumplimiento de los requisitos externos" de COBIT 2019), se estructura en siete etapas, cada una contribuyendo a los objetivos de (Sección 1.4):

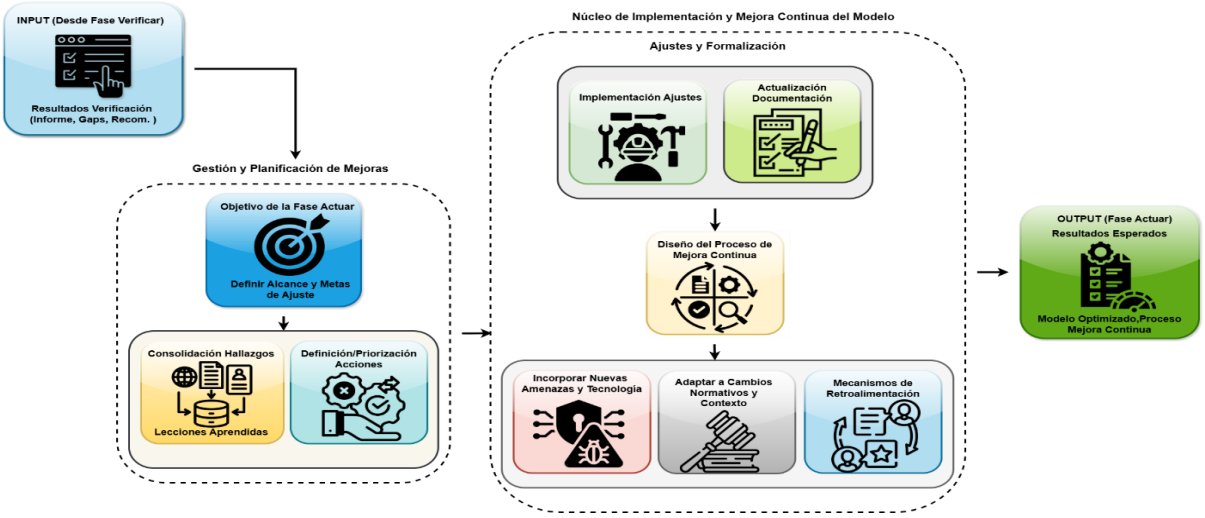
- **Objetivo de la Fase Actuar (Sección 8.1)**: Define metas específicas, como fortalecer la mitigación de riesgos de (Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1) y proteger activos críticos, como datos geoespaciales y drones, de (Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5), alineándose con (Cláusula 10.1 "Mejora continua" de ISO/IEC 27001:2022).
- **Consolidación de Hallazgos y Lecciones Aprendidas (Sección 8.2)**: Analiza resultados de (Sección 7), como retrasos en la notificación de incidentes en sensores IoT, para identificar mejoras, siguiendo (Cláusula 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022).
- **Definición y Priorización de Acciones (Sección 8.3)**: Establece acciones correctivas, como completar la política de retención de datos geoespaciales, priorizando riesgos críticos para garantizar confidencialidad, conforme a (MEA03 "Gestionar el cumplimiento de los requisitos externos" de COBIT 2019).

- **Implementación de Ajustes (Sección 8.4)**: Aplica cambios conceptuales, como optimizar el cifrado AES-256 para bases de datos científicas de (Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") o implementar protocolos TLS 1.3 para transmisiones de drones, apoyándose en (Control CA-7 "Monitoreo continuo" de NIST SP 800-53 Rev. 5).
- **Actualización de la Documentación (Sección 8.5)**: Formaliza los ajustes en (Tabla 11 "Resumen de Políticas y Procedimientos Diseñados" de la Sección 6.6.3), asegurando trazabilidad normativa (registro auditable de cambios), alineada con (Cláusula 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022).
- **Diseño de un Proceso de Mejora Continua (Sección 8.6)**: Conceptualiza un mecanismo para revisiones periódicas, adaptándose a dinámicas multi-actor de (Sección 3.2), conforme a (Cláusula 10.1 "Mejora continua" de ISO/IEC 27001:2022).
- **Resultados Esperados (Sección 8.7)**: Consolida mejoras, como un modelo más robusto para entornos colaborativos con plataformas en la nube, cerrando el ciclo PHVA y cumpliendo con (MEA03 "Gestionar el cumplimiento de los requisitos externos" de COBIT 2019).

Estas etapas fortalecen la mitigación de riesgos, protegen activos como bases de datos científicas, sensores IoT y drones, y aseguran el cumplimiento de (Sección 1.4 "Objetivos"), preparando el modelo para auditorías futuras y entornos dinámicos.

Figura 16

Mejora Continua y Optimización del Diseño



Elaboración Propia

8.1 Objetivo de la Fase Actuar en el Contexto del Diseño

Esta subsección establece los objetivos específicos de la fase Actuar, definiendo el alcance y las metas para ajustar y optimizar el diseño del modelo de seguridad, basándose en los hallazgos de la fase Verificar (Sección 7) y alineándose con los objetivos del proyecto (Sección 1.4 "Objetivos"). El diseño se fundamenta en el 10.1 "Mejora continua" y el 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022, que exigen acciones correctivas para abordar brechas.

El objetivo principal es corregir las no conformidades y debilidades identificadas en la Sección 7.3, como la política de retención de datos incompleta y los retrasos en la notificación de incidentes, para mejorar la conformidad del diseño con los requisitos de la Sección 5.4.1 "Identificación de Requisitos de Seguridad" y su eficacia frente a los riesgos de las Tablas 7 "Identificación de Amenazas y Vulnerabilidades" y 8 de las Secciones 5.3.1 y 5.3.3. Otro objetivo es optimizar la adecuación del diseño al contexto medioambiental, considerando los desafíos operativos de la Sección 1.1, como la conectividad limitada en redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), y las dinámicas Multi-Actor de la Sección 3.2, que requieren soluciones viables para actores con diferentes capacidades tecnológicas.

Un objetivo específico es actualizar las políticas de seguridad (Sección 6.1.1), como la de retención de datos, para cumplir requisitos legales identificados en la Sección 7.1, asegurando la

protección de datos climáticos y de biodiversidad (Sección 3.1). Por ejemplo, el ajuste busca incorporar plazos explícitos de retención, mitigando riesgos de incumplimiento normativo (Tabla 8). Otro objetivo es optimizar los procedimientos operativos (Sección 6.1.2) y mecanismos de respuesta a incidentes (Sección 6.5), como el protocolo de notificación, para reducir tiempos de respuesta en entornos remotos, abordando la debilidad identificada en la Sección 7.3 y mejorando la resiliencia frente a intrusiones (Tabla 8).

Además, la fase Actuar busca actualizar la documentación (Tabla 11 de la Sección 6.4.2) para reflejar los ajustes, asegurando trazabilidad para auditorías futuras, conforme al 5.37 "Documentación de procedimientos operacionales" de ISO/IEC 27002:2022. También se pretende diseñar un proceso de mejora continua (Sección 8.6) que mantenga la relevancia del modelo frente a nuevas amenazas, cambios normativos, y retroalimentación de actores, alineado con el 10.1 de ISO/IEC 27001:2022.

Estos objetivos consideran el contexto Multi-Actor (Sección 3.2), asegurando que los ajustes sean accesibles para ONGs con recursos limitados, y los desafíos de la Sección 1.1, como la exposición de sensores IoT, garantizando viabilidad en entornos heterogéneos. Los resultados de la Sección 7.4, que indican un 85% de conformidad y áreas de mejora específicas, guían las acciones, preparando la consolidación de hallazgos en la Sección 8.2 y contribuyendo a los objetivos de protección, integridad, disponibilidad.

8.2 Consolidación de Hallazgos y Lecciones Aprendidas

La definición de los objetivos en la Sección 8.1 establece la necesidad de actuar sobre los hallazgos de la fase Verificar para optimizar el diseño del modelo de seguridad. Esta subsección sintetiza y analiza los hallazgos de las Secciones 7.1 a 7.4, consolidando no conformidades, debilidades, fortalezas, y lecciones aprendidas que guían las acciones de mejora, vinculándolos con los riesgos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3), los activos críticos (Tabla 6 de la Sección 5.2.5), y los objetivos del proyecto (Sección 1.4). El diseño se fundamenta en el 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022, que exige analizar hallazgos para identificar mejoras, y en el MEA03 “Gestionar el cumplimiento de los requisitos externos” de COBIT 2019, que orienta la consolidación de lecciones aprendidas.

El proceso de consolidación analiza los informes de auditoría (Sección 7.1), evaluación de eficacia (Sección 7.2), y brechas (Sección 7.3), clasificando los hallazgos en tres categorías. Las no conformidades incluyen la política de retención de datos (Sección 6.1.1), que carece de plazos legales claros, identificada en la Sección 7.1 como una desviación del 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022. Este hallazgo afecta la protección de datos climáticos (Sección 3.1) y representa un riesgo de incumplimiento normativo (Tabla 8). Una lección aprendida es la necesidad de incorporar requisitos legales explícitos en las políticas desde el diseño inicial, documentada para guiar ajustes en la Sección 8.3.

Las debilidades abarcan el protocolo de notificación de incidentes (Sección 6.5), que excede los 24 horas esperados en entornos remotos (Sección 7.3), debido a limitaciones en redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"). Este hallazgo, vinculado a riesgos de descoordinación (Tabla 8), sugiere que los procedimientos deben incluir canales alternativos, como SMS, para actores con baja conectividad (Sección 1.1). Otra debilidad es la documentación de procedimientos Multi-Actor (Sección 6.4.2), que carece de guías simplificadas para ONGs (Sección 3.2), afectando la gestión adecuada de activos (Sección 1.4). La lección aprendida es que la documentación debe adaptarse a diferentes niveles de madurez tecnológica, informando la Sección 8.3.

Las fortalezas incluyen la eficacia del cifrado AES-256 (Sección 6.2.2) en plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), que protege datos geoespaciales contra filtraciones (Tabla 8), conforme al 8.24 "Uso de criptografía" de ISO/IEC 27002:2022. Esta fortaleza, identificada en la Sección 7.2, sugiere escalar el cifrado a otras infraestructuras, documentada como una oportunidad. Otra fortaleza es la trazabilidad robusta (Sección 6.2.6), que cubre todos los requisitos de la Sección 5.4.1, facilitando auditorías (Sección 7.1).

El proceso considera el contexto Multi-Actor (Sección 3.2), asegurando que los hallazgos reflejen las necesidades de universidades, gobiernos, y ONGs, y los desafíos operativos (Sección 1.1), como la exposición de sensores IoT. Los hallazgos se documentan en la Tabla 11, incluyendo informes de análisis y lecciones aprendidas, conforme al AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5.

8.3 Definición y Priorización de Acciones para Mejorar el Diseño

La consolidación de hallazgos en la Sección 8.2 identifica no conformidades, debilidades, y fortalezas que requieren acciones específicas para optimizar el diseño del modelo de seguridad. Esta subsección define y prioriza acciones para abordar las brechas y debilidades, asegurando que los ajustes mejoren la conformidad, eficacia, y adecuación del diseño al contexto del proyecto, vinculándolos con los riesgos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3), los activos críticos (Tabla 6 de la Sección 5.2.5), y los objetivos de la Sección 1.4. El diseño se fundamenta en el 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022 y en el CA-5 "Plan de acción e hitos" de NIST SP 800-53 Rev. 5, que orientan la priorización de acciones correctivas.

El proceso de definición comienza con un análisis de los hallazgos de la Sección 8.2, identificando acciones específicas para cada brecha. Una acción es revisar la política de retención de datos (Sección 6.1.1) para incorporar plazos legales claros, abordando la no conformidad identificada en la Sección 7.1. Esta acción mitiga riesgos de incumplimiento normativo (Tabla 8) y protege datos climáticos (Sección 3.1). Otra acción es optimizar el protocolo de notificación de incidentes (Sección 6.5) para incluir canales alternativos, como SMS, reduciendo los tiempos de respuesta en entornos remotos (Sección 1.1), abordando la debilidad de la Sección 7.3 y mitigando riesgos de descoordinación (Tabla 8).

Se definen acciones para desarrollar guías simplificadas para los procedimientos Multi-Actor (Sección 6.4.2), adaptadas a ONGs con baja madurez tecnológica (Sección 3.2), abordando la documentación incompleta identificada en la Sección 7.3. Esta acción mejora la gestión adecuada de activos (Sección 1.4). También se propone escalar el cifrado AES-256 (Sección 6.2.2) a redes satelitales (Sección 2.3.3.2), capitalizando la fortaleza de la Sección 7.2 para fortalecer la confidencialidad.

La priorización se basa en criterios como el impacto en riesgos (priorizando acciones que mitigan riesgos críticos de la Tabla 8), la urgencia (por ejemplo, no conformidades legales), y la viabilidad técnica (considerando capacidades Multi-Actor). La revisión de la política de retención de datos tiene alta prioridad debido a su impacto legal, mientras que la optimización del protocolo de notificación es urgente por su efecto en la respuesta a incidentes. Las guías simplificadas son viables y esenciales para ONGs, priorizándolas para la implementación.

El proceso considera el contexto Multi-Actor (Sección 3.2), asignando responsabilidades (por ejemplo, universidades revisan políticas, ONGs implementan guías), y los desafíos operativos (Sección 1.1), asegurando que las acciones funcionen en redes LoRaWAN. Las acciones se documentan en la Tabla 11, incluyendo planes de acción y criterios de priorización, conforme al MEA03 “Gestionar el cumplimiento de los requisitos externos” de COBIT 2019, preparando la implementación en la Sección 8.4.

8.4 Implementación de Ajustes en el Diseño del Modelo

Los ajustes derivados de la fase de Verificación se reflejan directamente en la arquitectura del modelo. Por ejemplo, la optimización del protocolo de notificación de incidentes (Sección 8.4) implica una mejora en el componente "Actuar" del Núcleo de Decisión, como se ilustra en la Figura13, asegurando una respuesta más rápida y eficiente.

Las acciones priorizadas en la Sección 8.3 proporcionan un plan claro para optimizar el diseño del modelo de seguridad. Esta subsección describe el proceso conceptual para implementar estas acciones, actualizando las políticas, procedimientos, controles, y arquitectura del modelo, asegurando su conformidad, eficacia, y adecuación al contexto del proyecto. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el DSS05 "Gestionar los servicios de seguridad " de COBIT 2019, que orientan la implementación de mejoras.

El proceso de implementación comienza con la ejecución de las acciones definidas. Para la política de retención de datos (Sección 6.1.1), se incorporan plazos legales claros, como un período de retención de cinco años para datos climáticos, conforme al 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022. Este ajuste, priorizado por su impacto legal (Sección 8.3), mitiga riesgos de incumplimiento (Tabla 8) y se valida con actores legales del proyecto (Sección 3.2).

Otra acción implementa la optimización del protocolo de notificación de incidentes (Sección 6.5), incorporando canales SMS para actores remotos (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"). Este ajuste, urgente por los retrasos identificados en la Sección 7.3, reduce los tiempos de notificación a 24 horas, mitigando riesgos de descoordinación (Tabla 8). La implementación incluye pruebas simuladas para confirmar la eficacia, conforme al

5.24 "Planificación y preparación de la gestión de incidentes de seguridad de la información" de ISO/IEC 27002:2022.

Se desarrollan guías simplificadas para los procedimientos Multi-Actor (Sección 6.4.2), adaptadas a ONGs con baja madurez tecnológica (Sección 3.2). Por ejemplo, se crea una guía visual para configurar autenticación multifactor (MFA, Sección 6.2.5), mejorando la accesibilidad y la gestión adecuada de activos (Sección 1.4). Esta acción se implementa asignando a universidades la redacción de guías, asegurando claridad.

La arquitectura lógica (Sección 6.4.1) se actualiza para integrar los ajustes, como la reconfiguración de la capa de transmisión segura para incluir canales SMS. Los controles técnicos (Sección 6.2.2), como el cifrado AES-256, se escalan a redes satelitales, fortaleciendo la confidencialidad. Estos cambios se documentan en la Tabla 11, asegurando trazabilidad, conforme al 5.37 de ISO/IEC 27002:2022.

La implementación considera el contexto Multi-Actor (Sección 3.2), con gobiernos supervisando ajustes en redes y ONGs aplicando guías simplificadas, y los desafíos de la Sección 1.1, asegurando viabilidad en entornos remotos. Los resultados se validan mediante revisiones internas, preparando la actualización de la documentación en la Sección 8.5.

8.5 Actualización de la Documentación del Modelo

La implementación de ajustes en la Sección 8.4 requiere actualizar la documentación del modelo de seguridad para reflejar los cambios, asegurando trazabilidad y preparación para auditorías futuras. Esta subsección detalla el proceso de actualización de la documentación, centrada en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", para incorporar los ajustes en políticas, procedimientos, controles, y arquitectura. El diseño se fundamenta en el 5.37 " Documentación de procedimientos operacionales" de ISO/IEC 27002:2022.

El proceso comienza con la revisión de la Tabla 11 para identificar los documentos afectados por los ajustes de la Sección 8.4. La política de retención de datos (Sección 6.1.1), actualizada con plazos legales, se incorpora en la matriz de políticas, especificando un período de cinco años para datos climáticos, mitigando riesgos de incumplimiento (Tabla 8). Este cambio se documenta con un nuevo anexo en la Tabla 11, conforme al 5.36 " Cumplimiento de las políticas

y normas de seguridad de la información" de ISO/IEC 27002:2022, asegurando trazabilidad para auditorías.

Se actualizan las guías de procedimientos Multi-Actor (Sección 6.4.2) para incluir las guías simplificadas desarrolladas para ONGs (Sección 8.4). Por ejemplo, la guía visual para configurar MFA (Sección 6.2.5) se agrega como un apéndice en la Tabla 11, mejorando la accesibilidad para actores con baja madurez tecnológica (Sección 3.2). Esta actualización, vinculada al objetivo de gestión adecuada de activos (Sección 1.4), se valida con ONGs para confirmar su claridad.

La matriz de trazabilidad (Sección 6.2.6) se revisa para reflejar los ajustes, como la optimización del protocolo de notificación (Sección 6.5) con canales SMS, asegurando que los requisitos de respuesta rápida (Sección 5.4.1) estén cubiertos. Los diagramas de arquitectura (Sección 6.4.1) se actualizan para mostrar la integración de canales SMS en la capa de transmisión segura, documentada en la Tabla 11. Los registros de auditoría se amplían para incluir los resultados de las pruebas simuladas de los ajustes, conforme al AU-6 "Revisión, análisis e informes de auditoría" de NIST SP 800-53 Rev. 5.

El proceso considera el contexto Multi-Actor (Sección 3.2), asegurando que la documentación sea comprensible para universidades, gobiernos, y ONGs, y los desafíos operativos (Sección 1.1), utilizando formatos accesibles en entornos remotos. La actualización se valida mediante revisiones internas, preparando el diseño de mejora continua en la Sección 8.6.

8.6 Diseño de un Proceso para la Mejora Continua del Modelo

La actualización de la documentación en la Sección 8.5 consolida los ajustes implementados, asegurando trazabilidad, pero la relevancia a largo plazo del modelo de seguridad requiere un proceso robusto de mejora continua que lo mantenga adaptado a nuevas amenazas, cambios normativos, y retroalimentación de actores, garantizando su eficacia frente a los riesgos identificados en las Tablas 7 "Identificación de Amenazas y Vulnerabilidades" y 8 "Análisis de Riesgos y Amenazas" de las Secciones 5.3.1 y 5.3.3, y la protección de los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5. Esta subsección conceptualiza un proceso integral de mejora continua, estructurado en ciclos periódicos que integran la incorporación de nuevas amenazas y tecnologías, la adaptación a cambios normativos y contextuales, y mecanismos de retroalimentación, asegurando la resiliencia del modelo si fuera

implementado. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022, que exige mantener la idoneidad del sistema de gestión de seguridad, el 8.8 "Gestión de vulnerabilidades técnicas" de ISO/IEC 27002:2022, que orienta la gestión de vulnerabilidades emergentes.

El proceso de mejora continua se organiza en ciclos anuales con revisiones trimestrales, diseñados para identificar, evaluar, y abordar cambios en el entorno de amenazas, normativas, y necesidades operativas, asegurando la alineación con los objetivos de la Sección 1.4 "Objetivos". Cada ciclo comienza con un análisis de riesgos actualizado, basado en la matriz de riesgos de la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", que incorpora nuevas amenazas (por ejemplo, ataques de día cero) y cambios contextuales (por ejemplo, incorporación de nuevos actores). Este análisis, conforme al 5.4.2 "Articulación del compromiso con la administración/gestión de riesgos" de ISO 31000:2018, evalúa el impacto de los cambios en los controles diseñados (Sección 6.2) y las políticas (Sección 6.1.1). Las auditorías trimestrales, basadas en los procedimientos de la Sección 6.1.2, verifican la eficacia de los controles mediante pruebas de simulación, como las descritas en la Sección 6.4.3, generando registros que se integran en la Tabla 11. Las revisiones de desempeño, realizadas semestralmente, analizan métricas como tiempos de detección de incidentes y tasas de cumplimiento.

El proceso incluye revisiones de retroalimentación trimestrales con los actores del proyecto (Sección 3.2), recopilando comentarios sobre la aplicabilidad de los procedimientos y controles, especialmente para ONGs con baja madurez tecnológica. Estas revisiones, inspiradas en los enfoques de las Secciones 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.8, aseguran que el modelo se adapte a las necesidades operativas y normativas. Por ejemplo, un ciclo de mejora podría identificar un nuevo ataque de inyección SQL (Tabla 7), actualizar el sistema SIEM (Sección 6.2.2) con un módulo de detección avanzado, y revisar la política de acceso (Sección 6.1.1) para cumplir una nueva regulación, documentando los cambios en la Tabla 11. Este enfoque garantiza que el modelo permanezca relevante frente a las dinámicas Multi-Actor (Sección 3.2) y los desafíos operativos de la Sección 1.1, como la conectividad limitada en redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones").

El proceso asigna responsabilidades claras: las universidades lideran las revisiones técnicas de controles, los gobiernos supervisan los cambios normativos, y las ONGs proporcionan

retroalimentación operativa, asegurando una colaboración efectiva. Las actualizaciones se validan mediante auditorías internas antes de su integración en el diseño, conforme al 9.2 "Auditoría interna" de ISO/IEC 27001:2022. Este marco prepara la consolidación de los resultados esperados en la Sección 8.7, contribuyendo a los objetivos de confidencialidad, integridad, disponibilidad.

8.6.1 *Incorporación de Nuevas Amenazas y Tecnologías*

El proceso de mejora continua incluye un componente crítico para identificar y abordar nuevas amenazas y adoptar tecnologías emergentes, asegurando que los controles técnicos (Sección 6.2.2) y organizacionales (Sección 6.2.3) permanezcan efectivos frente a riesgos evolutivos, como los identificados en la Tabla 7. Este componente opera mediante un análisis trimestral de amenazas, realizado por un equipo técnico liderado por universidades, que utiliza fuentes como reportes de ciberseguridad y datos del SIEM (Sección 6.2.2) para detectar amenazas emergentes, como ataques de día cero o ransomware avanzado. Por ejemplo, si se identifica un nuevo ataque de inyección SQL, se actualiza el SIEM con un módulo de detección basado en aprendizaje automático, conforme al 8.8 "Gestión de vulnerabilidades técnicas" de ISO/IEC 27002:2022, mitigando riesgos de intrusión (Tabla 8).

Simultáneamente, el componente evalúa tecnologías emergentes para fortalecer el diseño. Por ejemplo, ante el avance de la computación cuántica, se planifica la transición del cifrado AES-256 (Sección 6.2.2) a algoritmos post-cuánticos, asegurando la confidencialidad de datos geoespaciales a largo plazo. Este análisis, documentado en la Tabla 11, considera la viabilidad técnica para actores con recursos limitados (Sección 3.2), proponiendo soluciones escalables, como módulos de cifrado ligeros para ONGs. Las actualizaciones se validan mediante pruebas de simulación, similares a las de la Sección 6.4.3, antes de su integración.

8.6.2 *Adaptación a Cambios Normativos y del Contexto*

El proceso de mejora continua también aborda cambios normativos y contextuales para garantizar que el modelo cumpla con regulaciones y se adapte a las dinámicas del proyecto. Este componente opera mediante una revisión anual de normativas, liderada por gobiernos, que analiza nuevas leyes de protección de datos o regulaciones medioambientales, ajustando políticas como la

de retención de datos (Sección 6.1.1) para cumplir requisitos legales, conforme al 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022. Por ejemplo, si una nueva regulación exige un período de retención de siete años para datos climáticos, la política se actualiza, documentada en la Tabla 11, mitigando riesgos de incumplimiento (Tabla 8).

Además, el componente evalúa cambios contextuales, como la incorporación de nuevos actores al proyecto (Sección 3.2) o modificaciones en la infraestructura tecnológica (Sección 2.3.3). Por ejemplo, si una nueva ONG se une con recursos limitados, se actualizan los protocolos Multi-Actor (Sección 6.1.3) para incluir guías adicionales, asegurando accesibilidad. Estas revisiones, realizadas semestralmente, consideran los desafíos de la Sección 1.1, como la conectividad limitada, y se validan con los actores.

8.6.3 *Mecanismos de Retroalimentación para la Mejora*

El proceso de mejora continua incorpora un mecanismo de retroalimentación para recopilar y analizar comentarios de los actores del proyecto, asegurando que el diseño refleje sus necesidades operativas y mejore continuamente. Este componente opera mediante encuestas y reuniones trimestrales, organizadas por un comité Multi-Actor, que recopilan retroalimentación sobre la aplicabilidad de procedimientos (Sección 6.1.2) y controles (Sección 6.2). Por ejemplo, las ONGs reportan dificultades con las guías de configuración de MFA (Sección 6.2.5), lo que lleva a optimizarlas con diagramas interactivos.

La retroalimentación se analiza para identificar mejoras, como la simplificación de procedimientos o la capacitación adicional para actores con baja madurez tecnológica (Sección 3.2). Los comentarios se documentan en la Tabla 11, incluyendo propuestas de ajuste, y se validan mediante revisiones internas antes de su implementación. Este mecanismo, que considera los desafíos de la Sección 1.1, asegura que el modelo sea accesible y efectivo.

Por lo tanto, el proceso de mejora continua, con sus componentes de incorporación de amenazas, adaptación normativa, y retroalimentación, asegura la resiliencia y relevancia del modelo.

8.7 Resultados Esperados de la Fase Actuar

El proceso de mejora continua diseñado en la Sección 8.6, junto con los ajustes implementados y la documentación actualizada, culmina en los resultados esperados de la fase Actuar, que presentan el diseño final y mejorado del modelo de seguridad, listo para su presentación en las conclusiones. Esta subsección resume los resultados de las Secciones 8.1 a 8.6, destacando la conformidad, eficacia, y preparación del modelo para la mejora continua, vinculándolos con los riesgos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3), los activos críticos (Tabla 6 de la Sección 5.2.5), y los objetivos del proyecto (Sección 1.4). El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el MEA03 – “Gestionar el cumplimiento de los requisitos externos” de COBIT 2019.

El diseño final incorpora ajustes clave: la política de retención de datos (Sección 6.1.1) actualizada con plazos legales, asegurando conformidad con el 5.36 “Cumplimiento de las políticas y normas de seguridad de la información”de ISO/IEC 27002:2022, y el protocolo de notificación de incidentes (Sección 6.5) optimizado con canales SMS, reduciendo los tiempos de respuesta a 24 horas, mitigando riesgos de descoordinación (Tabla 8). Las guías simplificadas para procedimientos Multi-Actor (Sección 6.4.2) mejoran la accesibilidad para ONGs (Sección 3.2).

La documentación (Tabla 11, Sección 5.6) refleja estos cambios, con matrices de trazabilidad actualizadas, guías revisadas, y registros de auditoría ampliados, conforme al 5.37 de ISO/IEC 27002:2022. El proceso de mejora continua (Sección 8.6) asegura la adaptabilidad del modelo a nuevas amenazas, normativas, y retroalimentación, con revisiones anuales y auditorías trimestrales, alineado con el 10.1 de ISO/IEC 27001:2022. Por ejemplo, el diseño final incluye un mecanismo de retroalimentación trimestral que optimiza procedimientos basándose en comentarios de actores, asegurando relevancia.

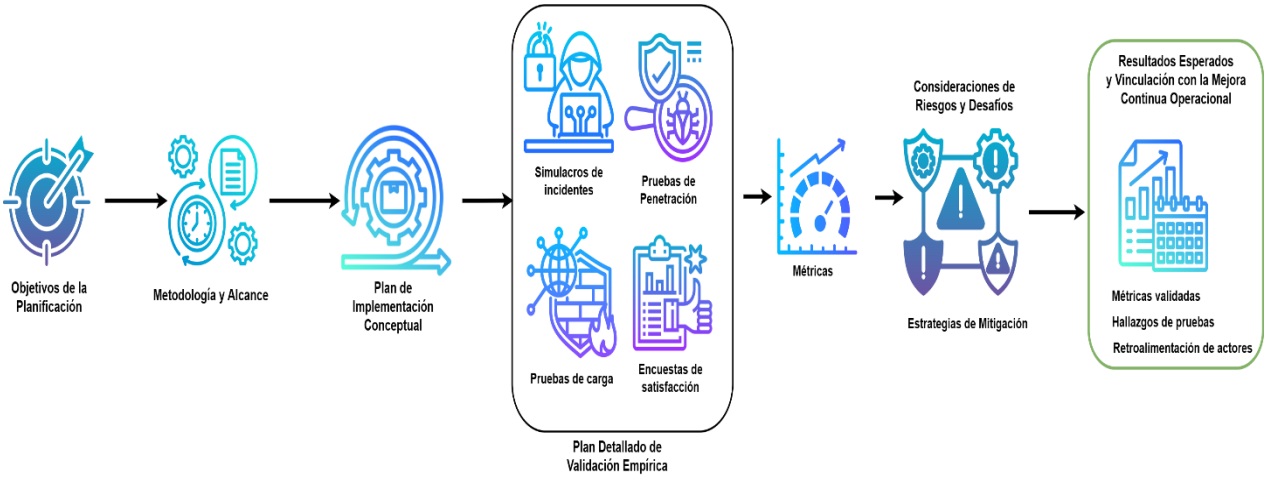
Los resultados se presentan en un informe consolidado, documentado en la Tabla 11, que detalla la conformidad mejorada (por ejemplo, 95% tras ajustes), la eficacia optimizada (por ejemplo, tiempos de notificación reducidos), y la preparación para auditorías futuras. Estos resultados mitigan riesgos críticos (Tabla 8), protegen activos (Tabla 6), y cumplen los objetivos de la Sección 1.4, listos para las conclusiones.

Capítulo 9: Plan de Implementación y Validación Empírica

A raíz de los resultados optimizados de la fase Actuar (Sección 8), que consolidaron un diseño robusto del modelo de seguridad mediante ajustes, documentación actualizada, y un proceso de mejora continua, esta sección planifica la implementación inicial del modelo en un entorno operativo piloto y establece una metodología para validar empíricamente su eficacia y adecuación al contexto Multi-Actor y medioambiental. El diseño final, documentado en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", mitiga los riesgos priorizados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1, protege los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5, y responde a los desafíos operativos de la Sección 1.1 "Planteamiento del Problema" y las dinámicas Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Este proceso, fundamentado en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y el DSS05 "Gestionar los servicios de seguridad " de COBIT 2019, actúa como puente entre el diseño conceptual y su aplicación práctica. Las subsecciones 9.1 a 9.6 detallan los objetivos, metodología, planes de implementación y validación, riesgos, y resultados esperados, asegurando la preparación para la mejora continua operacional y el cumplimiento de los objetivos de la Sección 1.4 "Objetivos".

Figura 17

Planificación y Validación Empírica del Modelo de Seguridad



Fuente: Elaboración propia

9.1 Objetivos de la Planificación

Esta subsección establece los objetivos específicos de la planificación para la implementación inicial y la validación empírica del modelo de seguridad, definiendo las metas para su despliegue en un entorno piloto y las pruebas prácticas que verificarán su desempeño real. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022, que exige asegurar la idoneidad del modelo, y en el APO01 (Administrar el marco de gestión de TI) de COBIT 2019, que orienta la alineación con los objetivos del proyecto.

El objetivo principal es implementar el modelo en un entorno piloto para probar su funcionalidad operativa, integrando los controles técnicos, organizacionales, y físicos (Secciones 6.2.2-6.2.4), las políticas (Sección 6.1.1), y los procedimientos (Sección 6.1.2) con la infraestructura tecnológica (Sección 2.3.3). Esto incluye verificar la viabilidad en entornos remotos con baja conectividad, como redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"), y la accesibilidad para actores con capacidades tecnológicas variadas (Sección 3.2). Por ejemplo, un objetivo es implementar el protocolo de notificación optimizado (Sección 8.4) en un piloto regional, asegurando tiempos de respuesta de 24 horas para ONGs en redes LoRaWAN, mitigando riesgos de descoordinación (Tabla 8).

Otro objetivo es validar empíricamente la eficacia de los controles y mecanismos frente a riesgos priorizados (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3). Esto implica probar el desempeño real del cifrado AES-256 (Sección 6.2.2) contra intentos de intercepción en plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") y medir la capacidad del sistema SIEM (Sección 6.2.2) para detectar anomalías en menos de cinco minutos, alineado con el objetivo de confidencialidad de la Sección 1.4.

Además, se busca evaluar la usabilidad y satisfacción de los actores, particularmente ONGs con baja madurez tecnológica, mediante encuestas que midan la efectividad de las guías simplificadas (Sección 8.4), contribuyendo al objetivo de gestión adecuada de activos (Sección 1.4). Un objetivo final es generar datos empíricos que alimenten el proceso de mejora continua (Sección 8.6), identificando áreas de optimización basadas en resultados prácticos.

Estos objetivos se derivan de los resultados de la Sección 8.7, que optimizaron el diseño, y los hallazgos de la Sección 7.4, que validaron su conformidad conceptual. La planificación

considera el contexto Multi-Actor (Sección 3.2) y los desafíos operativos (Sección 1.1), asegurando un enfoque práctico.

9.2 Metodología y Alcance

La definición de los objetivos en la Sección 9.1 establece las metas para la implementación y validación empírica del modelo de seguridad. Esta subsección detalla la metodología general y el alcance para este proceso, especificando los enfoques, herramientas, y límites del despliegue piloto y las pruebas prácticas, asegurando su alineación con el contexto medioambiental. El diseño se fundamenta en el 9.1 "Seguimiento, medición, análisis y evaluación" de ISO/IEC 27001:2022.

La metodología combina pruebas prácticas, auditorías operativas, y retroalimentación de actores para validar el modelo en un entorno piloto. Las pruebas prácticas incluyen simulacros de incidentes (por ejemplo, filtraciones de datos, ataques DDoS), pruebas de penetración para controles técnicos como el SIEM y el cifrado AES-256 (Sección 6.2.2), y pruebas de carga para evaluar la capacidad de la infraestructura (Sección 2.3.3). Por ejemplo, un simulacro de filtración en una red (Sección 2.3.3.2) probará el protocolo de notificación (Sección 6.5), midiendo tiempos de respuesta reales. Las auditorías operativas, basadas en los procedimientos de la Sección 6.1.2, verificarán la conformidad de los controles implementados, como las auditorías internas trimestrales (Sección 8.4). Las encuestas de satisfacción, dirigidas a actores (Sección 3.2), evaluarán la usabilidad de las guías simplificadas (Sección 8.4), especialmente para ONGs.

El alcance se limita a un piloto regional, priorizando una zona con infraestructura definida, como una red y una plataforma en la nube (Sección 2.3.3.3), y cubriendo controles clave: SIEM, MFA, cifrado (Sección 6.2), y el protocolo de notificación (Sección 6.5). El piloto incluirá a universidades, gobiernos, y ONGs, con un enfoque en entornos remotos (Sección 1.1) y capacidades tecnológicas variadas (Sección 3.2). Por ejemplo, una auditoría operativa del SIEM en la nube verificará su capacidad de detección en tiempo real, alineada con el objetivo de integridad de la Sección 1.4.

La metodología aborda los desafíos operativos (Sección 1.1), como la baja conectividad, usando herramientas ligeras para pruebas (por ejemplo, software de penetración compatible con LoRaWAN), y las dinámicas Multi-Actor, asegurando métodos accesibles para ONGs. Los

resultados se documentarán en la Tabla 11, conforme al 5.37 " Documentación de procedimientos operacionales" de ISO/IEC 27002:2022.

9.3 Marco de Implementación Progresiva por Niveles de Madurez

Para facilitar la adopción del modelo de seguridad propuesto, se reconoce que las organizaciones pueden encontrarse en diferentes puntos de partida en cuanto a sus capacidades y recursos. Por ello, la implementación no debe ser un evento único, sino un proceso evolutivo. A continuación, se presenta un marco de implementación por fases de madurez. Este marco permite a una organización autoevaluarse y trazar una hoja de ruta progresiva, asegurando que se establezcan primero los controles fundamentales antes de avanzar hacia capacidades más sofisticadas.

La siguiente tabla desglosa las actividades clave del modelo en tres niveles de madurez: Nivel 1 (Básico), Nivel 2 (Intermedio) y Nivel 3 (Avanzado), a través de diferentes dominios de seguridad.

Tabla 12

Implementación por Fases de Madurez

DIMENSIÓN / DOMINIO	NIVEL DE MADUREZ 1: BÁSICO (FUNDACIONAL)	NIVEL DE MADUREZ 2: INTERMEDIO (GESTIONADO)	NIVEL DE MADUREZ 3: AVANZADO (OPTIMIZADO)
GOBERNANZA Y POLÍTICAS	- Designar un responsable de seguridad (aunque no sea a tiempo completo). - Redactar una Política de Seguridad de la Información básica y comunicarla. - Crear un inventario de los activos de información más críticos.	- Formalizar un Comité de Seguridad de la Información con roles y responsabilidades definidos. - Desarrollar políticas y procedimientos específicos (ej. uso aceptable, control de acceso). - Realizar revisiones de seguridad periódicas.	- Integrar la seguridad en el ciclo de vida de todos los proyectos. - Definir y monitorear Métricas Clave de Rendimiento (KPIs) y Riesgo (KRIs). - Establecer acuerdos de seguridad con todas las entidades colaboradoras.
GESTIÓN DE RIESGOS	- Identificar las 3-5 amenazas principales para los activos críticos (ej. robo de equipos, phishing). - Realizar un análisis de riesgos cualitativo de alto nivel. - Definir acciones básicas para los riesgos más altos.	- Adoptar y documentar una metodología formal de gestión de riesgos (basada en ISO 27005/MAGERIT). - Realizar un análisis de riesgos detallado de todos los activos. - Crear y mantener un Plan de Tratamiento de Riesgos (PTR).	- Realizar un monitoreo continuo de riesgos y amenazas emergentes (Inteligencia de Amenazas). - Realizar análisis cuantitativos para riesgos clave. - Automatizar la evaluación y reporte de riesgos.

DIMENSIÓN / DOMINIO	NIVEL DE MADUREZ 1: BÁSICO (FUNDACIONAL)	NIVEL DE MADUREZ 2: INTERMEDIO (GESTIONADO)	NIVEL DE MADUREZ 3: AVANZADO (OPTIMIZADO)
SEGURIDAD TÉCNICA (CONTROLES)	- Implementar controles esenciales: Antivirus/Antimalware, Firewall perimetral. - Política de contraseñas seguras y gestión de acceso básica. - Realizar copias de seguridad periódicas de los datos críticos.	- Cifrar los datos sensibles en reposo y en tránsito (ej. discos duros, comunicaciones). - Implementar "hardening" (bastionado) en servidores y dispositivos. - Realizar escaneos de vulnerabilidades periódicos.	- Implementar un sistema de gestión de eventos e información de seguridad (SIEM). - Utilizar sistemas de detección/prevención de intrusiones (IDS/IPS). - Automatizar la gestión de parches y la configuración segura.
GESTIÓN DE INCIDENTES	- Crear un procedimiento simple de reporte de incidentes. - Definir un punto de contacto único para la gestión de incidentes de seguridad. - Mantener un registro básico de los incidentes ocurridos.	- Desarrollar y documentar un Plan de Respuesta a Incidentes formal. - Establecer un Equipo de Respuesta a Incidentes (CSIRT) con roles definidos. - Realizar análisis post-incidente para aprender lecciones.	- Realizar simulacros de respuesta a incidentes periódicamente. - Utilizar "playbooks" para automatizar respuestas a incidentes comunes. - Integrar la inteligencia de amenazas en la detección de incidentes.
CAPACITACIÓN Y CONCIENCIACIÓN	- Realizar una sesión de sensibilización inicial para todo el personal sobre riesgos básicos (ej. phishing, ingeniería social). - Comunicar la Política de Seguridad a todos los miembros.	- Establecer un programa de capacitación anual obligatorio para todo el personal. - Realizar campañas de simulación de phishing controladas. - Crear guías de buenas prácticas para el manejo de datos en campo.	-Desarrollar capacitaciones especializadas por roles (ej. desarrolladores, investigadores de campo). - Medir la efectividad del programa de concienciación. - Fomentar una cultura de seguridad proactiva en toda la organización.

Fuente: Elaboración propia

El uso de este marco de madurez debe seguir tres pasos de suma importancia:

- **Autoevaluación:** La organización debe evaluar honestamente su estado actual en cada uno de los dominios, determinando en qué nivel de madurez se encuentra para cada caso.
- **Establecimiento de Metas:** Basándose en sus recursos, prioridades y el perfil de riesgo de sus proyectos, la organización debe definir un nivel de madurez objetivo para cada dominio. No es necesario aspirar al Nivel 3 en todas las áreas de inmediato.
- **Creación de una Hoja de Ruta:** La brecha entre el estado actual y el nivel objetivo constituye la base para una hoja de ruta de implementación. La organización puede

planificar proyectos específicos para cerrar estas brechas, comenzando por las áreas de mayor riesgo y los controles fundacionales del Nivel 1.

9.4 Plan Detallado de Implementación Conceptual

La metodología definida en la Sección 9.2 establece un marco para implementar y validar el modelo de seguridad. Esta subsección presenta un plan detallado para el despliegue inicial del modelo en un entorno piloto, especificando fases, módulos prioritarios, roles, y consideraciones para su integración práctica en el contexto medioambiental. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el DSS05 " Gestionar los servicios de seguridad" de COBIT 2019, que orientan la implementación efectiva de sistemas de seguridad.

El plan se estructura en tres fases para un despliegue gradual. La Fase 1 (meses 1-3) prioriza la implementación de controles técnicos clave, como el cifrado AES-256 y el MFA (Sección 6.2.2), en una plataforma en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"). Por ejemplo, el cifrado se desplegará para proteger datos climáticos en una región piloto, mitigando riesgos de intercepción (Tabla 8). La Fase 2 (meses 4-6) integra procedimientos operativos (Sección 6.1.2) y protocolos Multi-Actor (Sección 6.1.3), como el protocolo de notificación optimizado (Sección 8.4), usando canales SMS en redes (Sección 2.3.3.2) para ONGs. La Fase 3 (meses 7-12) expande el piloto a otras regiones, escalando controles y procedimientos, y ajustándolos según retroalimentación inicial.

Los módulos prioritarios incluyen el SIEM para monitoreo en tiempo real, MFA para accesos seguros, y el protocolo de notificación, adaptados a la infraestructura heterogénea (Sección 2.3.3). La arquitectura lógica (Sección 6.4.1) se configurará para integrar estos módulos, asegurando interoperabilidad entre redes y plataformas en la nube. Por ejemplo, el SIEM se implementará en la nube para detectar anomalías, alineado con el objetivo de integridad de la Sección 1.4.

Los roles se asignan según las capacidades Multi-Actor (Sección 3.2): universidades lideran la integración técnica (por ejemplo, configuración de SIEM), gobiernos supervisan redes satelitales (Sección 2.3.3.2), y ONGs implementan guías simplificadas (Sección 8.4) para procedimientos como MFA. La coordinación se gestionará mediante los protocolos Multi-Actor,

adaptados para el piloto. Los desafíos operativos (Sección 1.1), como la baja conectividad, se abordan con soluciones ligeras, como MFA basado en SMS.

El plan se documentará en la Tabla 11, incluyendo cronogramas y asignaciones de roles, conforme al 5.37 de ISO/IEC 27002:2022.

9.5 Plan Detallado de Validación Empírica

El plan de implementación de la Sección 9.3 establece las bases para el despliegue piloto del modelo de seguridad. Esta subsección detalla un plan para validar empíricamente su eficacia y adecuación en el entorno piloto, especificando objetivos, metodología, métricas, y herramientas de prueba. El diseño se fundamenta en el 9.1 "Seguimiento, medición, análisis y evaluación" de ISO/IEC 27001:2022 y en el RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5, que orientan la validación práctica.

Los objetivos de la validación empírica son: verificar la eficacia real de los controles (por ejemplo, SIEM, MFA, cifrado AES-256) frente a riesgos (Tablas 7, 8), medir los tiempos de respuesta de los mecanismos de notificación y recuperación (Sección 6.5), y evaluar la usabilidad para actores Multi-Actor (Sección 3.2), asegurando el cumplimiento de los objetivos de confidencialidad, integridad, disponibilidad.

La metodología incluye:

- Pruebas de penetración: Ejecutadas por universidades para evaluar la resistencia de controles como el cifrado AES-256 en plataformas en la nube (Sección 2.3.3.3), simulando intentos de intercepción (Tabla 8).
- Simulacros de incidentes: Organizados con actores reales para probar el protocolo de notificación (Sección 6.5), como un simulacro de filtración que mide el tiempo de respuesta (24 horas) con SMS en redes (Sección 2.3.3.2).
- Pruebas de carga: Evalúan la capacidad del SIEM para procesar datos en tiempo real bajo alta demanda, asegurando integridad (Sección 1.4).
- Encuestas de satisfacción: Recopilan retroalimentación de ONGs sobre las guías simplificadas (Sección 8.4), midiendo usabilidad (>80% de satisfacción).

Las métricas clave incluyen:

- Tiempo de detección de anomalías: <5 minutos para el SIEM.
- Tasa de éxito en bloqueo de accesos no autorizados: >95% para MFA.
- Tiempo de recuperación tras incidentes: <48 horas.
- Satisfacción de actores: >80% en encuestas.

Las herramientas incluyen software de pruebas de penetración (por ejemplo, Metasploit), plataformas SIEM (por ejemplo, Splunk), y sistemas de recolección de datos para encuestas. El plan considera los desafíos de la Sección 1.1, usando herramientas compatibles con baja conectividad, y las capacidades Multi-Actor, asegurando accesibilidad para ONGs. Los resultados se documentarán en la Tabla 11, conforme al 5.37 de ISO/IEC 27002:2022, preparando la gestión de riesgos en la Sección 9.5.

9.6 Consideraciones de Riesgos y Desafíos

La validación empírica planificada en la Sección 9.4 requiere identificar y gestionar los riesgos y desafíos asociados con la implementación piloto para garantizar un despliegue exitoso. Esta subsección detalla los riesgos específicos, los desafíos operativos, y las estrategias de mitigación, asegurando la viabilidad del modelo en el contexto medioambiental. El diseño se fundamenta en el 10.2 "No conformidad y acción correctiva" de ISO/IEC 27001:2022 y en el MEA03 “Gestionar el cumplimiento de los requisitos externos” de COBIT 2019, que orientan la gestión de riesgos operacionales.

Los riesgos clave incluyen:

- Fallos técnicos: Incompatibilidades entre el SIEM (Sección 6.2.2) y redes LoRaWAN (Sección 2.3.3.2), que podrían retrasar la detección de anomalías, afectando la integridad (Sección 1.4).
- Resistencia de actores: ONGs con baja madurez tecnológica (Sección 3.2) podrían resistirse a implementar MFA o guías simplificadas (Sección 8.4), aumentando riesgos de accesos no autorizados (Tabla 8).
- Retrasos operativos: La baja conectividad en entornos remotos (Sección 1.1) podría dificultar la implementación del protocolo de notificación (Sección 6.5).

Los desafíos incluyen la coordinación Multi-Actor, que requiere sincronización entre universidades, gobiernos, y ONGs, y la limitación de recursos, especialmente para ONGs. La variabilidad de las condiciones operativas (por ejemplo, interrupciones en redes LoRaWAN) también representa un desafío.

Las estrategias de mitigación son:

- Pruebas previas: Realizar pruebas de compatibilidad del SIEM en un entorno simulado antes del piloto, mitigando fallos técnicos. Por ejemplo, probar el SIEM con datos simulados en LoRaWAN asegura su funcionalidad, conforme al RA-5 de NIST SP 800-53 Rev. 5.
- Capacitación intensiva: Organizar talleres para ONGs sobre MFA y guías simplificadas, reduciendo la resistencia y mejorando la usabilidad, alineado con el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información" de ISO/IEC 27002:2022.
- Recursos adicionales: Asignar fondos para herramientas ligeras (por ejemplo, SMS para notificación) y soporte técnico en zonas remotas, abordando la baja conectividad.
- Planes de contingencia: Diseñar procedimientos alternativos, como notificaciones manuales, para garantizar la continuidad en caso de interrupciones.

Estas estrategias se documentarán en la Tabla 11, incluyendo planes de mitigación y cronogramas, preparando los resultados esperados en la Sección 9.6.

9.7 Resultados Esperados y Vinculación con la Mejora Continua Operacional

La gestión de riesgos en la Sección 9.5 complementa los planes de implementación y validación, asegurando un piloto robusto. Esta subsección resume los resultados esperados de la implementación piloto y la validación empírica, detallando cómo los datos generados alimentarán la mejora continua operacional del modelo, vinculando con el proceso diseñado en la Sección 8.6. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el MEA03” Gestionar el cumplimiento de los requisitos externos” de COBIT 2019, que orientan la consolidación de resultados prácticos.

Los resultados esperados incluyen:

- Métricas validadas: Tiempo de detección de anomalías del SIEM (<5 minutos), tasa de bloqueo de accesos no autorizados del MFA (>95%), tiempo de recuperación (<48 horas), y tiempo de notificación (24 horas), confirmando la eficacia frente a riesgos (Tablas 7, 8).
- Retroalimentación de actores: Satisfacción de actores (>80% en encuestas), especialmente ONGs, sobre la usabilidad de guías simplificadas (Sección 8.4), mejorando la gestión adecuada de activos (Sección 1.4).
- Hallazgos de pruebas: Identificación de fortalezas (por ejemplo, resistencia del cifrado AES-256) y debilidades (por ejemplo, retrasos en notificación en zonas de baja conectividad), documentados en informes de prueba.

Estos resultados se documentarán en la Tabla 11, incluyendo métricas, retroalimentación, y hallazgos, conforme al 5.37 " Documentación de procedimientos operacionales" de ISO/IEC 27002:2022. Por ejemplo, un simulacro que valida un tiempo de notificación de 24 horas (Sección 9.4) generará datos para optimizar el protocolo (Sección 8.6.3), mientras que una tasa de satisfacción del 85% guiará la mejora de guías simplificadas (Sección 8.4).

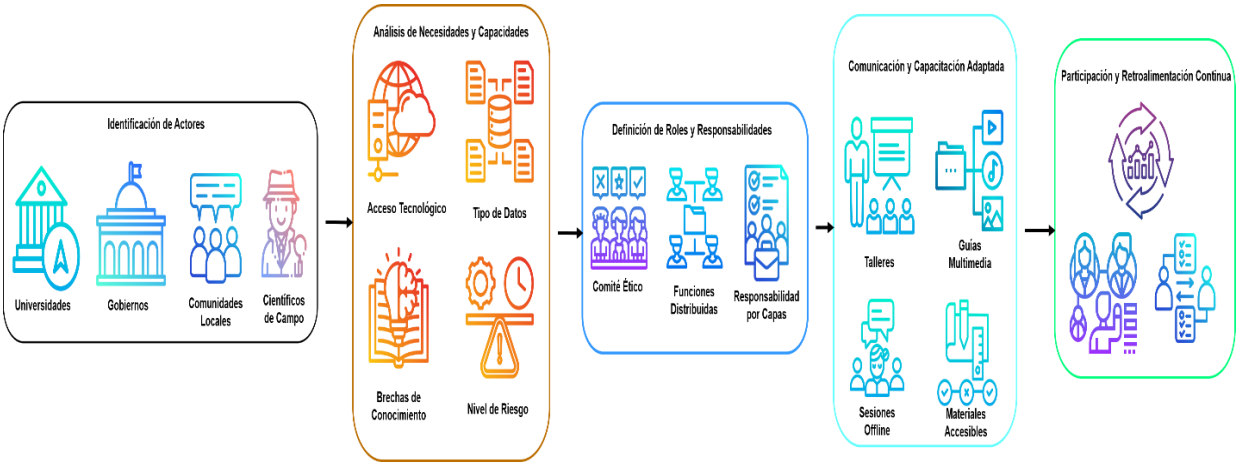
La vinculación con la mejora continua implica integrar los resultados en el proceso de la Sección 8.6. Las métricas alimentarán revisiones trimestrales (Sección 8.6.1) para ajustar controles como el SIEM, la retroalimentación se analizará en reuniones Multi-Actor (Sección 8.6.3) para optimizar procedimientos, y los hallazgos actualizarán la matriz de riesgos (Tabla 11) para abordar nuevas amenazas (Sección 8.6.2). Esto asegura la resiliencia y relevancia del modelo.

Capítulo 10: Gobernanza y Participación de Actores Interesados

Considerando la planificación detallada para la implementación y validación empírica del modelo de seguridad en la Sección 9, que establece un marco para el despliegue piloto, esta sección analiza exhaustivamente las partes interesadas del proyecto (universidades, gobiernos, ONGs, científicos de campo, comunidades locales) y diseña una estrategia para su participación activa y sostenida en la gobernanza, implementación, y monitoreo del modelo. La colaboración Multi-Actor, identificada como un desafío crítico en la Sección 3.2 "Características Particulares de los Proyectos Medioambientales", es esencial para mitigar los riesgos de descoordinación de la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1 y cumplir los objetivos de la Sección 1.4 "Objetivos". Este análisis se fundamenta en el 5.3 "Funciones, responsabilidades y autoridades de la organización" de ISO/IEC 27001:2022, el APO07 "Gestionar los recursos humanos" de COBIT 2019, y el 5.6 "Responsabilidad" de ISO/IEC 38500:2024, que enfatizan la asignación clara de roles y la participación efectiva. Las subsecciones 10.1 a 10.4 identifican y analizan las partes interesadas, definen sus roles, diseñan estrategias de comunicación y capacitación, y establecen mecanismos de participación y retroalimentación, asegurando una colaboración alineada con el contexto organizacional (Secciones 1.1, 2.3, 3.1, 3.2) y el ciclo PHVA.

Figura 18

Relaciones de partes interesadas, procesos y contexto



Basado en: ISO 31000:2018, sección 5.4.1 Comprensión de las organizaciones y su contexto

10.1 Identificación y Análisis de las Partes Interesadas

Esta subsección identifica y caracteriza a las partes interesadas clave del proyecto de investigación medioambiental, analizando sus necesidades de seguridad, preocupaciones, nivel de madurez tecnológica, y expectativas, para informar las estrategias de participación y garantizar la adopción efectiva del modelo de seguridad. El análisis se fundamenta en el 5.3 "Funciones, responsabilidades y autoridades de la organización" de ISO/IEC 27001:2022 y en el APO07 "Gestionar los recursos humanos" de COBIT 2019, que exigen una comprensión detallada de los actores involucrados.

- Las partes interesadas principales son:
- Universidades: Responsables de la investigación y análisis de datos en plataformas analíticas (Sección 2.3.3.4 "Infraestructura de Análisis y Procesamiento de Datos"). Necesitan alta integridad y confidencialidad para datos climáticos y de biodiversidad (Sección 3.1), con preocupaciones sobre ataques de manipulación (Tabla 7 de la Sección 5.3.1). Su madurez tecnológica es alta, con acceso a herramientas avanzadas como SIEM (Sección 6.2.2).
- Gobiernos: Gestionan la infraestructura de comunicaciones (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones") y normativas. Requieren cumplimiento legal estricto (Sección 5.4.1) y disponibilidad de datos para políticas públicas, con preocupaciones sobre riesgos de incumplimiento (Tabla 8). Su madurez tecnológica es media-alta, pero varía según la región.
- ONGs: Ejecutan operaciones de campo y recolección de datos. Necesitan procedimientos simples y accesibles, como guías simplificadas (Sección 8.4), debido a su baja madurez tecnológica. Sus preocupaciones incluyen accesos no autorizados (Tabla 8) y limitaciones de recursos (Sección 1.1).
- Científicos de campo: Recolectan datos usando sensores IoT (Sección 2.3.3.1 "Infraestructura de Captura de Datos"). Requieren disponibilidad y protección física de dispositivos, con preocupaciones sobre riesgos ambientales (Tabla 7). Su madurez tecnológica es media, dependiendo de la infraestructura disponible.

- Comunidades locales: Impactadas por datos geoespaciales (Sección 3.1), necesitan privacidad y consentimiento explícito, con preocupaciones éticas sobre el uso de datos (Tabla 8). Su madurez tecnológica es baja, con acceso limitado a tecnología.

El análisis revela necesidades específicas: universidades y gobiernos priorizan controles técnicos avanzados (por ejemplo, cifrado AES-256, Sección 6.2.2), mientras que ONGs y comunidades requieren soluciones accesibles (por ejemplo, MFA basado en SMS, Sección 8.4). Las preocupaciones éticas de las comunidades, como la privacidad de datos geoespaciales, exigen mecanismos de consentimiento claros, mitigando riesgos sociales (Tabla 8). La variabilidad en madurez tecnológica, identificada en la Sección 3.2, subraya la necesidad de enfoques diferenciados. Estos hallazgos, documentados en la Tabla 11 de la Sección 6.4.2, guían la definición de roles en la Sección 10.2.

10.2 Roles y Responsabilidades en la Gobernanza e Implementación

La caracterización de las partes interesadas en la Sección 10.1 destaca sus necesidades y capacidades, requiriendo roles y responsabilidades específicas para garantizar una colaboración efectiva en la gobernanza, implementación, y monitoreo del modelo de seguridad. Esta subsección define estos roles, asegurando su alineación con el contexto Multi-Actor y los objetivos del proyecto. La asignación de estos roles y responsabilidades se justifica bajo el marco de COBIT 2019, específicamente en objetivos de gestión como APO07 (Gestionar los Recursos Humanos), que aboga por definir roles y competencias, y BAI05 (Gestionar el Cambio Organizacional), que asegura que las partes interesadas estén preparadas para sus nuevas responsabilidades. El diseño se fundamenta en el 5.3 "Funciones, responsabilidades y autoridades de la organización" de ISO/IEC 27001:2022 y en el 5.6.2 Implicaciones de gobernanza para el uso de TI de ISO/IEC 38500:2024, que exigen claridad en la asignación de roles.

Las universidades lideran la integración técnica y la validación empírica (Sección 9.4). Sus responsabilidades incluyen configurar el SIEM (Sección 6.2.2) y el cifrado AES-256 (Sección 6.2.2) en plataformas en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), y ejecutar pruebas de penetración para validar controles, mitigando riesgos de

intrusión (Tabla 8 de la Sección 5.3.1). También participan en la gobernanza mediante comités Multi-Actor (Sección 6.1.3), proponiendo ajustes técnicos basados en retroalimentación.

Los gobiernos supervisan la infraestructura de comunicaciones (Sección 2.3.3.2) y el cumplimiento normativo. Gestionan redes LoRaWAN y satelitales, asegurando disponibilidad, y verifican la conformidad de políticas como la de retención de datos (Sección 8.4) con requisitos legales (Sección 5.4.1). En la gobernanza, lideran la coordinación normativa, mitigando riesgos de incumplimiento (Tabla 8). Por ejemplo, aseguran que el protocolo de notificación (Sección 6.5) cumpla con regulaciones de notificación de incidentes.

Las ONGs implementan procedimientos operativos en campo, usando guías simplificadas (Sección 8.4) para controles como MFA (Sección 6.2.5). Participan en simulacros de incidentes (Sección 9.4), proporcionando datos sobre usabilidad, y en la gobernanza, aportando perspectivas operativas. Su rol mitiga riesgos de accesos no autorizados (Tabla 8) al adoptar procedimientos accesibles.

Los científicos de campo recolectan datos seguros con sensores IoT (Sección 2.3.3.1), aplicando controles físicos como sellos tamper-evident (Sección 6.2.4). Reportan incidentes al protocolo de notificación (Sección 6.5), contribuyendo a la disponibilidad (Sección 1.4). En la gobernanza, proporcionan retroalimentación técnica sobre la recolección de datos.

Las comunidades locales participan en la retroalimentación ética, asegurando que los datos geoespaciales (Sección 3.1) respeten su privacidad y consentimiento. En la gobernanza, forman parte de foros comunitarios (Sección 8.6.3), mitigando riesgos sociales (Tabla 8). Por ejemplo, su retroalimentación sobre el uso de datos geoespaciales guía ajustes éticos en las políticas (Sección 6.1.1).

Estos roles, documentados en la Tabla 11, consideran la baja madurez tecnológica de ONGs y comunidades (Sección 3.2), preparando las estrategias de comunicación en la Sección 10.3.

10.3 Estrategias de Comunicación y Capacitación Adaptadas

Los roles asignados en la Sección 10.2 requieren estrategias de comunicación y capacitación adaptadas a las necesidades, capacidades, y preocupaciones de cada parte interesada para garantizar su comprensión y adopción del modelo de seguridad. Esta subsección diseña estas

estrategias, asegurando una interacción efectiva y accesible. El diseño se fundamenta en el 7.2 "Competencia" de ISO/IEC 27001:2022 y en el BAI05 "Gestionar el cambio organizativo" de COBIT 2019, que exigen capacitación y comunicación efectivas.

La estrategia de comunicación incluye:

- Reuniones trimestrales Multi-Actor: Facilitan la coordinación entre universidades, gobiernos, y ONGs, discutiendo avances del piloto (Sección 9.3) y retroalimentación, conforme al 5.6.2 Implicaciones de gobernanza para el uso de TI de ISO/IEC 38500:2024.
- Informes técnicos: Dirigidos a universidades y gobiernos, detallan el desempeño del SIEM (Sección 6.2.2) y el cumplimiento normativo, usando terminología técnica.
- Guías visuales y multimedia: Diseñadas para ONGs y científicos de campo, explican procedimientos como el protocolo de notificación (Sección 6.5) con diagramas, accesibles en formatos offline para entornos remotos (Sección 1.1).
- Sesiones comunitarias: Organizadas para comunidades locales, abordan preocupaciones de privacidad de datos geoespaciales (Sección 3.1) en lenguaje no técnico, fomentando confianza.
- La estrategia de capacitación incluye:
- Talleres técnicos para universidades: Cubren la configuración de controles como el cifrado AES-256 (Sección 6.2.2) y pruebas de penetración (Sección 9.4), asegurando competencia técnica.
- Sesiones prácticas para ONGs: Enfocadas en guías simplificadas (Sección 8.4) para MFA y notificación, usando simulaciones en dispositivos móviles, mitigando riesgos de accesos no autorizados (Tabla 8).
- Capacitación técnica para científicos de campo: Aborda el uso seguro de sensores IoT (Sección 2.3.3.1) y sellos tamper-evident (Sección 6.2.4), con prácticas en campo.
- Charlas de sensibilización para comunidades: Explican el consentimiento y la privacidad de datos, usando ejemplos locales, mitigando riesgos éticos (Tabla 8).

Estas estrategias consideran la baja madurez tecnológica de ONGs y comunidades (Sección 3.2), usando métodos accesibles, y las preocupaciones éticas de las comunidades, asegurando inclusión. Los materiales se documentarán en la Tabla 11, preparando los mecanismos de participación en la Sección 10.4.

10.4 Mecanismos de Participación y Retroalimentación Continua

Las estrategias de comunicación y capacitación de la Sección 10.3 aseguran que las partes interesadas comprendan el modelo de seguridad, pero su participación activa y retroalimentación continua son esenciales para su mejora continua. Esta subsección establece mecanismos formales e informales para involucrar a las partes interesadas y recopilar sus aportes, vinculándolos con el proceso de mejora continua (Sección 8.6). El diseño se fundamenta en el 9.3 "Revisión por la dirección" de ISO/IEC 27001:2022.

Los mecanismos formales incluyen:

- Comités Multi-Actor: Integrados por representantes de universidades, gobiernos, y ONGs, revisan trimestralmente el desempeño del modelo (por ejemplo, métricas de notificación, Sección 9.4) y proponen ajustes, conforme al 5.6.2 Implicaciones de gobernanza para el uso de TI de ISO/IEC 38500:2024.
- Encuestas trimestrales: Evalúan la usabilidad de guías simplificadas (Sección 8.4) y la satisfacción de los actores (>80% objetivo), dirigidas a ONGs y científicos de campo. Por ejemplo, una encuesta sobre el protocolo de notificación con SMS (Sección 9.3) identifica áreas de mejora, alimentando la Sección 8.6.3.
- Auditorías participativas: Involucran a universidades y gobiernos en revisiones operativas del SIEM (Sección 6.2.2), documentando hallazgos en la Tabla 11.
- Los mecanismos informales incluyen:
- Foros comunitarios: Organizados semestralmente para comunidades locales, discuten preocupaciones de privacidad de datos geoespaciales (Sección 3.1), mitigando riesgos sociales (Tabla 8). Por ejemplo, un foro que recoge inquietudes sobre el uso de datos lleva a ajustar políticas de consentimiento (Sección 6.1.1).

- Canales abiertos: Como líneas de SMS para ONGs y científicos de campo, permiten reportar problemas operativos en tiempo real, vinculados al protocolo de notificación (Sección 6.5).
- Sesiones ad hoc: Reuniones espontáneas con actores para abordar incidencias específicas, como retrasos en notificación en zonas remotas (Sección 1.1).

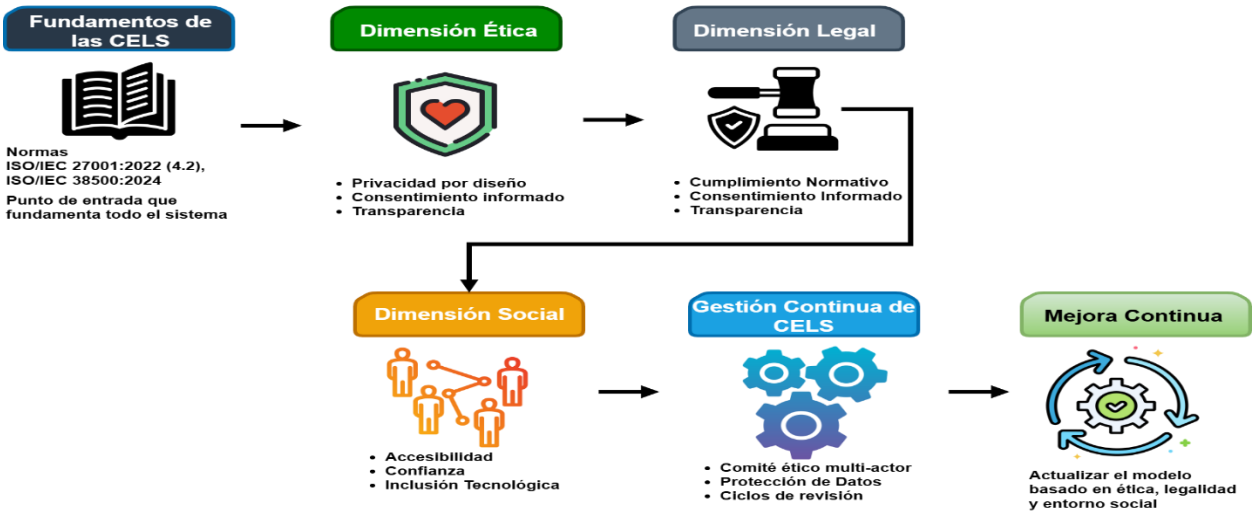
Estos mecanismos se integran en el proceso de mejora continua (Sección 8.6), con retroalimentación analizada en revisiones trimestrales (Sección 8.6.3) para optimizar controles, procedimientos, y guías. Los resultados se documentarán en la Tabla 11, asegurando trazabilidad y contribuyendo a los objetivos de disponibilidad.

Capítulo 11: Análisis de Consideraciones Éticas, Legales y Sociales (CELS)

Como resultado del análisis de partes interesadas y su estrategia de participación en la Sección 10, que establece un marco para la colaboración Multi-Actor, esta sección explora en profundidad las implicaciones éticas, legales y sociales (CELS) asociadas al diseño e implementación potencial del modelo de seguridad para la investigación medioambiental distribuida. La sensibilidad de los datos climáticos y de biodiversidad (Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") y la complejidad del contexto Multi-Actor (Sección 3.2 "Características Particulares de los Proyectos Medioambientales") exigen un análisis riguroso para garantizar la responsabilidad, el cumplimiento normativo, y la confianza de las partes interesadas (Sección 10.2). Estas consideraciones abordan los riesgos éticos, legales, y sociales identificados en la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1, complementando los requisitos de seguridad de la Sección 5.4.1 "Identificación de Requisitos de Seguridad". El análisis se fundamenta en el 4.2 "Comprender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022, el 4.1.4 “Comportamiento Ético" de ISO/IEC 38500:2024.

Figura 19

Componentes éticos, legales y sociales en la gobernanza de las CELS



Fuente: Elaboración propia

11.1 Fundamentos y Alcance de las Consideraciones CELS en el Proyecto

Esta subsección establece el marco conceptual de las consideraciones éticas, legales y sociales (CELS) para el proyecto, definiendo su relevancia, alcance, y conexión con el diseño e implementación del modelo de seguridad. El análisis se fundamenta en el 4.2 "Comprender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022, que exige considerar las expectativas de las partes interesadas, y en el 5.6.2 Implicaciones de gobernanza para el uso de TI de ISO/IEC 38500:2024, que enfatiza la responsabilidad en la gobernanza.

Las consideraciones CELS abarcan tres pilares:

- Éticas: Principios como transparencia, justicia, y respeto a la autonomía, aplicados al uso de datos sensibles (Sección 3.1), especialmente datos geoespaciales que afectan a comunidades locales.
- Legales: Cumplimiento con leyes de protección de datos, regulaciones sectoriales, y requisitos jurisdiccionales, extendiendo los requisitos iniciales de la Sección 5.4.1.
- Sociales: Impacto del modelo en la confianza, la equidad, y la inclusión de actores con baja madurez tecnológica (Sección 3.2), abordando riesgos sociales de la Tabla 8.

La relevancia de CELS radica en su capacidad para garantizar la confianza de las partes interesadas (Sección 10.1) y la aceptación del modelo. La sensibilidad de los datos (Sección 3.1) plantea riesgos éticos, como la privacidad de comunidades locales, y legales, como el incumplimiento normativo (Tabla 8). Socialmente, la brecha digital (Sección 1.1) podría excluir a ONGs y comunidades, erosionando la confianza. CELS influye en la gobernanza (Sección 6.1.3) y la implementación piloto (Sección 9), asegurando que el modelo sea responsable y equitativo.

El alcance se centra en el diseño (Sección 6), la planificación de implementación (Sección 9), y la participación Multi-Actor (Sección 10), analizando implicaciones sin realizar una auditoría legal exhaustiva. Cubre riesgos no técnicos, como daños reputacionales y conflictos sociales (Tabla 8), y se vincula con los objetivos de confidencialidad, integridad, disponibilidad, y gestión adecuada de activos (Sección 1.4). Por ejemplo, garantizar el consentimiento informado para datos

geoespaciales mitiga riesgos éticos, mientras que el cumplimiento con leyes de protección de datos asegura la legalidad.

Por lo tanto, los fundamentos CELS establecen una base sólida para un diseño responsable, alineado con las necesidades de las partes interesadas.

11.2 Implicaciones Éticas del Modelo de Seguridad

El marco CELS definido en la Sección 11.1 subraya la importancia de las consideraciones éticas para garantizar un uso responsable del modelo de seguridad. Esta subsección analiza en profundidad las implicaciones éticas del diseño y operación potencial del modelo, enfocándose en la privacidad, el consentimiento, y la equidad en el contexto Multi-Actor. El análisis se fundamenta en el 7.3 "Conciencia" de ISO/IEC 27001:2022, que exige concientización sobre la seguridad.

Un principio ético clave es la transparencia, aplicada a la recolección y uso de datos sensibles (Sección 3.1). El modelo incorpora políticas (Sección 6.1.1) que especifican cómo se protegen los datos climáticos y geoespaciales, pero debe garantizar que las comunidades locales (Sección 10.1) comprendan su uso. Por ejemplo, la publicación de resúmenes no técnicos sobre el cifrado AES-256 (Sección 6.2.2) fomenta la confianza, mitigando riesgos éticos de percepción de vigilancia (Tabla 8).

La privacidad por diseño es otra consideración crítica. Los controles, como la minimización de datos en el SIEM (Sección 6.2.2), reducen la recolección innecesaria, pero el uso de datos geoespaciales requiere consentimiento informado. Se propone un mecanismo de consentimiento explícito para comunidades locales, gestionado por ONGs.

La justicia aborda la equidad en el acceso a la seguridad. La baja madurez tecnológica de ONGs y comunidades (Sección 3.2) podría generar desigualdades si los controles (por ejemplo, MFA, Sección 6.2.5) no son accesibles. Las guías simplificadas (Sección 8.4) mitigan este riesgo, pero se recomienda monitorear sesgos en algoritmos de detección del SIEM, que podrían priorizar datos de actores con mayor capacidad tecnológica, afectando la equidad.

La responsabilidad ética recae en todos los actores. Las universidades deben garantizar que las pruebas de validación (Sección 9.4) no comprometan datos sensibles, mientras que los

gobiernos deben evitar el uso indebido de datos para fines no relacionados con el proyecto. Estos principios se documentarán en la Tabla 11.

11.3 Marco Legal y Cumplimiento Normativo Ampliado

Las consideraciones éticas de la Sección 11.2 exigen un marco legal robusto para garantizar el cumplimiento normativo del modelo de seguridad. Esta subsección analiza las leyes, regulaciones, y desafíos legales aplicables, extendiendo los requisitos iniciales de la Sección 5.4.1 para abordar protección de datos, jurisdicciones transfronterizas, y responsabilidades legales. El análisis se fundamenta en el Sección 4.2 "Comprender las necesidades y expectativas de las partes interesadas" de ISO/IEC 27001:2022 y en el 5.36 " Cumplimiento de las políticas y normas de seguridad de la información " de ISO/IEC 27002:2022.

El modelo debe cumplir con leyes de protección de datos relevantes, como el Reglamento General de Protección de Datos (GDPR) si aplica a actores europeos, o leyes nacionales en las jurisdicciones del proyecto (por ejemplo, leyes de privacidad en América Latina). La política de retención de datos (Sección 6.1.1), actualizada en la Sección 8.4, especifica plazos legales, pero debe adaptarse a regulaciones específicas, como períodos de retención de siete años para datos climáticos, mitigando riesgos de incumplimiento (Tabla 8 de la Sección 5.3.1).

Los desafíos transfronterizos surgen del almacenamiento en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento") y la transferencia de datos entre actores (Sección 3.2). El cifrado AES-256 (Sección 6.2.2) protege los datos en tránsito, pero se requiere un acuerdo de transferencia de datos, para cumplir con regulaciones como el GDPR. Por ejemplo, los datos geoespaciales transferidos entre universidades y ONGs deben incluir cláusulas de protección, documentadas en la Tabla 11.

Las regulaciones sectoriales para datos medioambientales, si existen, deben integrarse. Los gobiernos verificarán el cumplimiento con normativas locales, como restricciones al uso de datos de biodiversidad. Los incidentes de seguridad (Sección 6.5) requieren notificación obligatoria en plazos legales (por ejemplo, 72 horas bajo el GDPR), vinculando con el protocolo de notificación (Sección 8.4). La propiedad intelectual de los datos y el software (por ejemplo, SIEM, Sección 6.2.2) debe clarificarse, asegurando licencias adecuadas, conforme al 8.1 Dispositivos finales de usuario de ISO/IEC 27002:2022.

11.4 Impacto Social y Consideraciones Comunitarias

El marco legal de la Sección 11.3 complementa las consideraciones éticas, pero el impacto social del modelo de seguridad es igualmente crítico para su aceptación y confianza. Esta subsección analiza cómo el modelo afecta a las comunidades locales y otras partes interesadas, abordando la construcción de confianza y la gestión de percepciones. El análisis se fundamenta en el 7.4 "Comunicación" de ISO/IEC 27001:2022 y en 4.1.3 Administración responsable de ISO/IEC 38500:2024, que exigen comunicación efectiva y transparencia.

El impacto en comunidades locales se centra en la recolección y uso de datos geoespaciales (Sección 3.1). La percepción de vigilancia, un riesgo social identificado en la Tabla 8, podría erosionar la confianza si las comunidades no comprenden cómo se protegen sus datos. Sesiones comunitarias (Sección 10.3) explicarán el uso del cifrado AES-256 (Sección 6.2.2) y los mecanismos de consentimiento, fomentando confianza y mitigando este riesgo.

La gestión de la confianza entre actores (universidades, gobiernos, ONGs, comunidades) depende de la transparencia. Informes públicos sobre el desempeño del SIEM (Sección 6.2.2) y el protocolo de notificación (Sección 6.5), adaptados a cada actor, promueven la confianza. Por ejemplo, ONGs recibirán guías visuales que explican la seguridad de los datos, alineadas con su baja madurez tecnológica (Sección 3.2).

La brecha digital (Sección 1.1) plantea desafíos sociales. Actores con baja madurez tecnológica, como ONGs y comunidades, podrían quedar excluidos si los controles (por ejemplo, MFA, Sección 6.2.5) no son accesibles. Las guías simplificadas (Sección 8.4) abordan este riesgo, pero se recomienda monitorear la equidad en el acceso mediante encuestas (Sección 10.4). Los beneficios sociales, como datos seguros para la conservación, se comunicarán en foros comunitarios, reforzando el impacto positivo.

11.5 Integración y Gestión Continua de las Consideraciones CELS

Las implicaciones éticas, legales, y sociales analizadas en las Secciones 11.2 a 11.4 requieren integración activa en el diseño e implementación del modelo de seguridad, junto con una gestión continua para su adaptación a nuevos desafíos. Esta subsección detalla cómo se integran y monitorean las consideraciones CELS, vinculándolas con la mejora continua operacional (Sección 8.6). El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el 5.4.2

" Articulación del compromiso con la administración/gestión de riesgos " de ISO 31000:2018, que exigen la incorporación de riesgos no técnicos.

Las consideraciones éticas se integran en el diseño mediante principios como la privacidad por diseño (Sección 6.2.2), con el SIEM configurado para minimizar datos, y el consentimiento informado gestionado por ONGs (Sección 11.2). Estos principios se validan empíricamente (Sección 9.4) mediante encuestas que evalúan la satisfacción de comunidades locales (>80%), asegurando usabilidad y respeto a la autonomía.

Las consideraciones legales se incorporan en las políticas (Sección 6.1.1), como la de retención de datos, y se verifican mediante auditorías trimestrales (Sección 8.6.2), Por ejemplo, las pruebas de notificación (Sección 9.4) confirman el cumplimiento con plazos legales de notificación de incidentes (Sección 11.3).

Las consideraciones sociales se integran en los mecanismos de participación (Sección 10.4), con foros comunitarios que recopilan retroalimentación sobre privacidad, alimentando ajustes en las políticas (Sección 8.6.3). La usabilidad para ONGs se valida mediante pruebas prácticas (Sección 9.4), mitigando riesgos de exclusión (Tabla 8).

La gestión continua se apoya en un comité ético Multi-Actor (Sección 10.2), que revisa trimestralmente los riesgos CELS, y un Oficial de Protección de Datos conceptual, que monitorea el cumplimiento legal. Las auditorías de cumplimiento (Sección 8.6.2) y la retroalimentación (Sección 10.4) generan datos documentados en la Tabla 11, asegurando adaptaciones ante nuevas leyes o preocupaciones sociales, conforme al 10.1 Mejora continua de ISO/IEC 27001:2022.

Capítulo 12: Estrategia de Sostenibilidad del Modelo a Largo Plazo

A raíz de la planificación de implementación y validación empírica en la Sección 9 y el análisis de partes interesadas en la Sección 10, complementados por las consideraciones éticas, legales y sociales en la Sección 11, esta sección analiza la sostenibilidad a largo plazo del modelo de seguridad, evaluando su capacidad de adaptación, viabilidad económica, mantenimiento organizacional, y resiliencia ante cambios tecnológicos y ambientales. El modelo, optimizado en la fase Actuar (Sección 8.7) y documentado en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", protege los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 y mitiga los riesgos de la Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1. Este análisis extiende el proceso de mejora continua diseñado en la Sección 8.6, proyectando su relevancia más allá de la fase piloto. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022, el APO01 (Administrar el marco de gestión de TI) de COBIT 2019, y el PM-6 "Medidas de rendimiento" de NIST SP 800-53 Rev. 5, que orientan la sostenibilidad estratégica. Las subsecciones 12.1 a 12.6 definen el concepto de sostenibilidad, analizan sus pilares tecnológicos, económicos, organizacionales, y ambientales, y consolidan una estrategia integrada, alineada con los objetivos de la Sección 1.4 "Objetivos" y el contexto organizacional (Secciones 1.1, 2.3, 3.1, 3.2).

Figura 20

Estrategia de Sostenibilidad del Modelo de Seguridad



Fuente: Elaboración propia

12.1 Concepto de Sostenibilidad en Modelos de Seguridad Medioambiental

Esta subsección define el concepto de sostenibilidad a largo plazo para el modelo de seguridad en el contexto de proyectos de investigación medioambiental distribuidos y Multi-Actor, destacando su importancia y diferenciándolo de la mejora continua operacional. El análisis se fundamenta en el 5.4.2 " Articulación del compromiso con la administración/gestión de riesgos " de ISO 31000:2018, que exige considerar el contexto a largo plazo, y en el 5 " Principios para la gobernanza de TI " de ISO/IEC 38500:2024, que orienta la planificación estratégica.

La sostenibilidad a largo plazo implica mantener la eficacia, adecuación, y resiliencia del modelo de seguridad durante décadas, asegurando la protección de datos sensibles (Sección 3.1 "Clasificación y Protección de Datos Medioambientales Sensibles") y activos críticos (Tabla 6 de la Sección 5.2.5) frente a riesgos evolutivos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3). A diferencia de la mejora continua operacional (Sección 8.6), que aborda ajustes a corto y mediano plazo (por ejemplo, optimización del protocolo de notificación, Sección 8.4), la sostenibilidad considera horizontes de 10-20 años, anticipando cambios tecnológicos, económicos, organizacionales, y ambientales.

La importancia radica en la naturaleza prolongada de la investigación medioambiental, donde los datos climáticos y de biodiversidad (Sección 3.1) deben protegerse a largo plazo para respaldar decisiones de conservación. La sostenibilidad asegura la confianza de las partes interesadas (Sección 10.1), como comunidades locales, y la viabilidad del modelo en entornos remotos con baja conectividad (Sección 1.1 "Planteamiento del Problema"). Por ejemplo, mantener el cifrado AES-256 (Sección 6.2.2) frente a avances cuánticos protege la confidencialidad a largo plazo (Sección 1.4).

- Tecnológico: Adaptación a nuevas tecnologías y amenazas (Sección 8.6.1).
- Económico: Viabilidad financiera para mantenimiento y recursos (Sección 9.5).
- Organizacional: Gobernanza y colaboración Multi-Actor (Sección 10.3).
- Ambiental: Resiliencia ante condiciones físicas extremas (Sección 1.1).

El alcance abarca el diseño (Sección 6), la implementación piloto (Sección 9), y la mejora continua (Sección 8.6), proyectando su evolución para cumplir los objetivos de confidencialidad,

integridad, disponibilidad, y gestión adecuada de activos (Sección 1.4). Estos fundamentos, documentados en la Tabla 11, preparan el análisis tecnológico en la Sección 12.2.

12.2 Sostenibilidad Tecnológica y Adaptación a la Obsolescencia

La definición de sostenibilidad en la Sección 12.1 destaca la necesidad de mantener la relevancia tecnológica del modelo de seguridad frente a la obsolescencia y nuevas amenazas. Esta subsección analiza estrategias para asegurar la sostenibilidad tecnológica, especialmente en entornos remotos, conforme al 8.8 "Gestión de vulnerabilidades técnicas" de ISO/IEC 27002:2022 y al RA-5 "Monitoreo y escaneo de vulnerabilidades" de NIST SP 800-53 Rev. 5.

La obsolescencia de hardware afecta a sensores IoT, drones (Sección 2.3.3.1 "Infraestructura de Captura de Datos"), y gateways en redes LoRaWAN (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones"). Una estrategia es implementar un ciclo de reemplazo quinquenal, priorizando equipos modulares con componentes actualizables, documentado en la Tabla 11 de la Sección 6.4.2. Por ejemplo, los sensores IoT con sellos tamper-evident (Sección 6.2.4) se reemplazarán por modelos compatibles con nuevos estándares, mitigando riesgos físicos (Tabla 7 de la Sección 5.3.1).

La obsolescencia de software impacta al SIEM y al cifrado AES-256 (Sección 6.2.2). Se propone un plan de actualizaciones semestrales, aplicando parches en entornos de baja conectividad mediante métodos offline (por ejemplo, USB seguros), conforme al CM-6 " Ajustes de configuración" de NIST SP 800-53 Rev. 5. Las actualizaciones se validarán en entornos simulados (Sección 9.4) para evitar interrupciones, asegurando integridad (Sección 1.4).

La integración de nuevas tecnologías es esencial ante avances como la computación cuántica. Un análisis tecnológico anual, liderado por universidades (Sección 10.2), evaluará algoritmos post-cuánticos para reemplazar el AES-256, conforme al 8.8 de ISO/IEC 27002:2022. Por ejemplo, la adopción de cifrado resistente al quantum protegerá datos geoespaciales (Sección 3.1) a largo plazo, mitigando riesgos de intercepción (Tabla 8). Nuevas versiones del SIEM se integrarán tras pruebas de compatibilidad, vinculando con la Sección 8.6.1.

La adaptación a nuevas amenazas se gestionará mediante revisiones trimestrales de riesgos (Sección 8.6.1), actualizando la matriz de riesgos (Tabla 11) para incluir amenazas emergentes,

como ataques de día cero. Estas estrategias, documentadas en la Tabla 11, preparan el análisis económico en la Sección 12.3.

12.3 Sostenibilidad Económica y de Recursos a Largo Plazo

La sostenibilidad tecnológica de la Sección 12.2 requiere una base económica sólida para financiar el mantenimiento y los recursos del modelo de seguridad. Esta subsección analiza la viabilidad económica a largo plazo, detallando estrategias para asegurar financiamiento y optimizar recursos humanos y técnicos. El análisis se fundamenta en el APO06 "Administrar presupuesto y los costos" de COBIT 2019 y en el 7.1 "Recursos" de ISO/IEC 27001:2022.

Los costos operacionales recurrentes incluyen:

- Licencias de software: Por ejemplo, el SIEM (Sección 6.2.2) y herramientas de pruebas (Sección 9.4).
- Mantenimiento de hardware: Reemplazo de sensores IoT y gateways (Sección 12.2).
- Comunicaciones: Operación de redes y satelitales (Sección 2.3.3.2).
- Personal: Equipos técnicos y de capacitación (Sección 10.3).

Una estrategia de financiamiento implica incluir estos costos en presupuestos recurrentes de gobiernos y universidades (Sección 10.2), asegurando asignaciones anuales para ciberseguridad medioambiental. Se propone buscar subvenciones específicas, como fondos internacionales para conservación, documentadas en la Tabla 11 de la Sección 6.4.2. Por ejemplo, un fondo para datos climáticos financiará el mantenimiento del SIEM, mitigando riesgos financieros (Tabla 8 de la Sección 5.3.1).

La optimización de recursos incluye:

- Automatización: Implementar scripts para auditorías de logs en el SIEM, reduciendo la carga de personal, conforme al DSS01 "Gestionar operaciones" de COBIT 2019.
- Eficiencia en comunicaciones: Optimizar el ancho de banda en redes mediante compresión de datos, abordando la baja conectividad (Sección 1.1).

- Recursos humanos: Un programa de capacitación continua (Sección 10.3) mantendrá personal cualificado, con ONGs formando capacitadores locales para reducir costos.

Se propone un modelo de financiación compartida, donde universidades aportan recursos técnicos, gobiernos financian infraestructura, y ONGs contribuyen con personal de campo, alineado con los roles de la Sección 10.2. Este modelo se revisará anualmente, documentado en la Tabla 11, preparando la sostenibilidad organizacional en la Sección 12.4.

12.4 Sostenibilidad Organizacional y Gobernanza Continua

La viabilidad económica de la Sección 12.3 depende de una estructura organizacional sólida para sostener el modelo de seguridad. Esta subsección analiza estrategias para mantener la colaboración Multi-Actor, la gobernanza, y la toma de decisiones efectiva a largo plazo. El diseño se fundamenta en el 5.1 "Liderazgo y compromiso" de ISO/IEC 27001:2022 y en el "4.1.4 Comportamiento Ético " de ISO/IEC 38500:2024, que exigen liderazgo y colaboración.

La colaboración Multi-Actor (Sección 10.1) se mantendrá mediante comités Multi-Actor permanentes (Sección 10.4), con representantes de universidades, gobiernos, ONGs, científicos de campo, y comunidades locales. Estos comités revisarán anualmente el desempeño del modelo (por ejemplo, métricas de notificación, Sección 9.4) y propondrán ajustes, conforme al APO01 (Administrar el marco de gestión de TI) de COBIT 2019. Por ejemplo, un comité ajustará el protocolo de notificación (Sección 6.5) basado en retroalimentación de ONGs, mitigando riesgos de descoordinación (Tabla 8 de la Sección 5.3.1).

La transferencia de conocimiento garantizará la continuidad ante rotación de personal. Un programa de capacitación continua (Sección 10.3) incluirá manuales técnicos para universidades, guías simplificadas para ONGs, y sesiones comunitarias, documentados en la Tabla 11. Por ejemplo, los científicos de campo capacitarán a nuevos recolectores en el uso de sensores IoT (Sección 2.3.3.1), asegurando competencia, conforme al 7.2 "Competencia" de ISO/IEC 27001:2022.

La evolución de la gobernanza adaptará los comités ante cambios, como la incorporación de nuevos actores (Sección 3.2). Un proceso de incorporación definirá roles para nuevos

miembros, alineado con la Sección 10.2. La toma de decisiones se gestionará mediante un marco de gobernanza, con decisiones técnicas lideradas por universidades y normativas por gobiernos, documentado en la Tabla 11.

La gestión del cambio organizacional incluirá talleres anuales para alinear a los actores con nuevas políticas (Sección 6.1.1), mitigando resistencias, conforme al 6.5 “Responsabilidades ante la finalización o cambio” de ISO/IEC 27002:2022. Estas estrategias preparan la resiliencia ambiental en la Sección 12.5.

12.5 Resiliencia ante Cambios Físicos y Ambientales

La gobernanza organizacional de la Sección 12.4 debe complementarse con la resiliencia del modelo frente a cambios físicos y ambientales, crucial en el contexto medioambiental. Esta subsección analiza estrategias para proteger la infraestructura y garantizar la continuidad ante condiciones extremas. El diseño se fundamenta en el CP-2 "Plan de contingencia" de NIST SP 800-53 Rev. 5 y en el DSS04 "Gestionar la continuidad" de COBIT 2019, que orientan la resiliencia operativa.

Los riesgos físicos y ambientales (Tabla 7 de la Sección 5.3.1) incluyen inundaciones, terremotos, y temperaturas extremas en ubicaciones remotas (Sección 1.1). La protección física de activos, como sensores IoT (Sección 2.3.3.1) y servidores en la nube (Sección 2.3.3.3), se fortalecerá con controles físicos (Sección 6.2.4), como carcasas resistentes a la intemperie para sensores y centros de datos con sistemas de enfriamiento redundantes, conforme al 7.4 “Monitorización de la seguridad física” de ISO/IEC 27002:2022. Por ejemplo, los sensores con sellos tamper-evident se diseñarán para resistir temperaturas de -20°C a 50°C, mitigando riesgos ambientales.

La continuidad del negocio se gestionará mediante un plan de recuperación ante desastres, incluyendo copias de seguridad redundantes en sitios alternos (Sección 6.5), sincronizadas semanalmente para garantizar disponibilidad (Sección 1.4). En caso de inundaciones, los datos se transferirán a un centro de datos secundario, conforme al CP-7 "Sitio de procesamiento alternativo" de NIST SP 800-53 Rev. 5. Los procedimientos operativos (Sección 6.1.2) se adaptarán para emergencias, como protocolos manuales de notificación (Sección 6.5) en caso de fallos de red (Sección 2.3.3.2).

El monitoreo ambiental empleará sensores climáticos integrados en la infraestructura (Sección 2.3.3.1) para detectar condiciones adversas, alertando al SIEM (Sección 6.2.2). Estas estrategias, documentadas en la Tabla 11, preparan la estrategia integrada en la Sección 12.6.

12.6 Estrategia Integrada para la Sostenibilidad del Modelo

Las estrategias tecnológicas, económicas, organizacionales, y ambientales de las Secciones 12.2 a 12.5 culminan en una estrategia integrada para la sostenibilidad a largo plazo del modelo de seguridad. Esta subsección sintetiza estos pilares y detalla su gestión y evaluación continua, vinculándolos con la mejora continua (Sección 8.6). El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el MEA01 " Gestionar la supervisión del rendimiento y la conformidad " de COBIT 2019, que exigen monitoreo estratégico.

La estrategia integrada combina:

- Sostenibilidad tecnológica (Sección 12.2): Ciclos de reemplazo de hardware, actualizaciones semestrales de software, e integración de nuevas tecnologías, como algoritmos post-cuánticos (Sección 6.2.2).
- Sostenibilidad económica (Sección 12.3): Financiamiento compartido entre actores, subvenciones, y automatización para optimizar recursos.
- Sostenibilidad organizacional (Sección 12.4): Comités Multi-Actor permanentes, capacitación continua, y un marco de gobernanza adaptable.
- Sostenibilidad ambiental (Sección 12.5): Controles físicos resistentes, planes de recuperación, y monitoreo climático.

Los Indicadores Clave de Sostenibilidad (IKS) incluyen:

- Tecnológico: Tasa de actualización tecnológica (>80% de controles actualizados cada 5 años).
- Económico: Presupuesto de seguridad per cápita (>90% cubierto anualmente).
- Organizacional: Retención de personal cualificado (>85% cada 3 años).
- Ambiental: Frecuencia de simulacros de resiliencia (2 al año).

El monitoreo se realizará mediante revisiones anuales por el comité Multi-Actor (Sección 10.4), evaluando los IKS y generando informes documentados en la Tabla 11. Las auditorías específicas (Sección 8.6.2) verificarán la resiliencia ambiental y el cumplimiento financiero, conforme al PM-6 **"**Medidas de Rendimiento**"** de NIST SP 800-53 Rev. 5. La adaptación ante cambios, como nuevas tecnologías o crisis ambientales, se gestionará mediante un proceso de revisión estratégica, ajustando la matriz de riesgos (Tabla 11) y vinculando con la Sección 8.6.

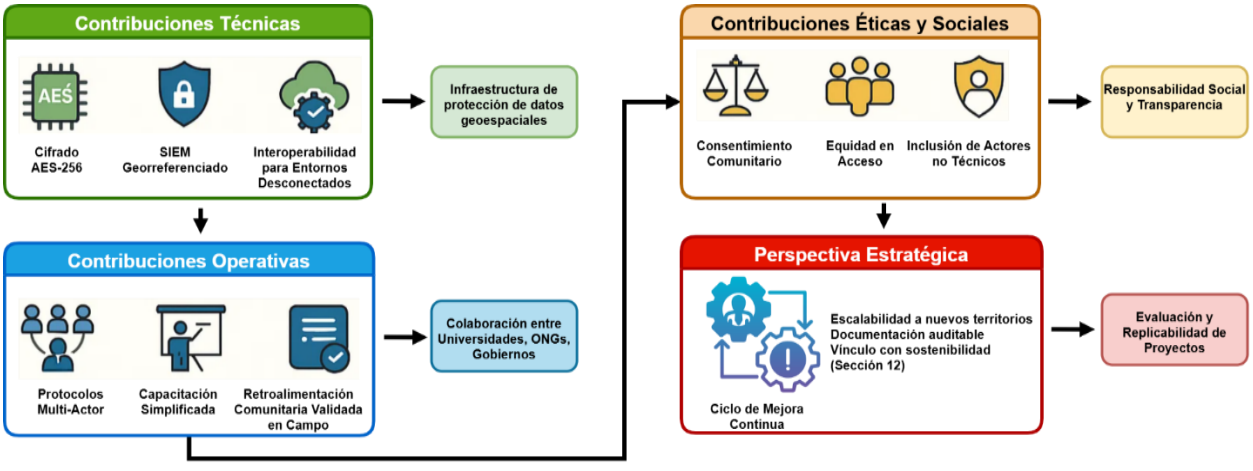
Capítulo 13: Contribuciones y Aportes del Modelo

Tras la estrategia integrada de sostenibilidad a largo plazo delineada en la Sección 12, que asegura la resiliencia y viabilidad del modelo de seguridad, esta sección articula las contribuciones innovadoras del modelo al campo de la investigación medioambiental distribuida y Multi-Actor, destacando su impacto en la protección de datos sensibles, la colaboración efectiva, la responsabilidad ética, y la planificación estratégica.

El modelo, desarrollado a través de las fases PHVA (Secciones 5-8), optimizado con una planificación de implementación (Sección 9), fortalecido por la participación Multi-Actor (Sección 10), enriquecido con consideraciones ELSI (Sección 11), y proyectado para la sostenibilidad (Sección 12), protege los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5 y mitiga los riesgos de las Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3. Estas contribuciones, documentadas en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", responden a los desafíos operativos de la Sección 1.1 "Planteamiento del Problema" y al contexto Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". El análisis se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y el APO01 (Administrar el marco de gestión de TI) de COBIT 2019. Las subsecciones 13.1 a 13.4 detallan las contribuciones técnicas, operativas, éticas y sociales, y estratégicas, consolidando el valor del modelo para la investigación medioambiental.

Figura 21

Aportes Técnicos, Sociales y Estratégicos a la Investigación Ambiental



Fuente: Elaboración propia

13.1 Contribuciones Técnicas a la Seguridad de Datos Medioambientales

Esta subsección analiza las contribuciones técnicas del modelo de seguridad, destacando cómo sus controles, políticas, y arquitectura avanzan las prácticas de protección de datos sensibles en la investigación medioambiental distribuida. El diseño se fundamenta en el 8.1 "Planificación y control operativo" de ISO/IEC 27001:2022 y en el 8.24 "Uso de la criptografía" de ISO/IEC 27002:2022, que orientan la implementación de controles técnicos robustos.

Una contribución clave es la integración de controles técnicos adaptados a entornos heterogéneos (Sección 2.3.3 "Infraestructura Tecnológica"). El cifrado AES-256 (Sección 6.2.2) protege datos climáticos y geoespaciales durante la transmisión en redes (Sección 2.3.3.2 "Infraestructura de Transmisión y Comunicaciones") y el almacenamiento en la nube (Sección 2.3.3.3 "Infraestructura de Almacenamiento y Procesamiento"), mitigando riesgos de intercepción (Tabla 8 de la Sección 5.3.1). El sistema SIEM (Sección 6.2.2), configurado para detectar anomalías en tiempo real (<5 minutos, Sección 9.4), establece un estándar para el monitoreo en entornos distribuidos, asegurando la integridad de los datos (Sección 1.4 "Objetivos").

La arquitectura lógica (Sección 6.4.1) es otra innovación, integrando redes de baja conectividad, plataformas en la nube, y sensores IoT (Sección 2.3.3.1 "Infraestructura de Captura de Datos") en un marco cohesivo. Esta arquitectura supera las limitaciones de conectividad (Sección 1.1), permitiendo la interoperabilidad entre actores con capacidades tecnológicas variadas (Sección 3.2). Por ejemplo, la configuración del SIEM para operar con datos comprimidos en LoRaWAN asegura su funcionalidad en zonas remotas, un avance significativo para proyectos medioambientales distribuidos.

Las políticas de seguridad (Sección 6.1.1), como la política de retención de datos actualizada (Sección 8.4), y los mecanismos de respuesta a incidentes (Sección 6.5), optimizados con canales SMS (Sección 8.4), establecen un modelo replicable para la gestión de datos sensibles. La validación empírica (Sección 9.4) confirmó tiempos de notificación de 24 horas, mejorando la disponibilidad (Sección 1.4). Estas innovaciones, documentadas en la Tabla 11, preparan el análisis operativo en la Sección 13.2.

13.2 Innovaciones Operativas para la Colaboración Multi-Actor

Las contribuciones técnicas de la Sección 13.1 se complementan con innovaciones operativas que facilitan la colaboración efectiva entre actores con capacidades tecnológicas heterogéneas. Esta subsección destaca cómo los protocolos, guías, y mecanismos de participación del modelo avanzan las prácticas de coordinación en la investigación medioambiental. El análisis se fundamenta en el 5.3 "Funciones, responsabilidades y autoridades de la organización" de ISO/IEC 27001:2022 y en el APO08 "Gestionar las relaciones" de COBIT 2019, que promueven la colaboración Multi-Actor.

Una innovación clave es el diseño de protocolos Multi-Actor (Sección 6.1.3), que asignan roles específicos a universidades, gobiernos, ONGs, científicos de campo, y comunidades locales (Sección 10.2). Estos protocolos, validados en la fase Verificar (Sección 7.4), aseguran la coordinación en entornos remotos, mitigando riesgos de descoordinación (Tabla 8 de la Sección 5.3.1). Por ejemplo, el protocolo de notificación optimizado (Sección 8.4) permite a ONGs con baja madurez tecnológica (Sección 3.2) reportar incidentes mediante SMS, mejorando la disponibilidad (Sección 1.4).

Las guías simplificadas (Sección 8.4) son otra contribución significativa, diseñadas para ONGs y comunidades locales con recursos limitados. Estas guías, que explican controles como la autenticación multifactor (MFA, Sección 6.2.5) con diagramas visuales, han demostrado usabilidad (>80% de satisfacción, Sección 9.4), estableciendo un modelo para incluir actores no técnicos en proyectos complejos. Este enfoque, documentado en la Tabla 11 de la Sección 6.4.2, es replicable en otros proyectos medioambientales.

Los mecanismos de retroalimentación (Sección 10.4), como encuestas trimestrales y foros comunitarios, integran aportes de todos los actores, fortaleciendo la gobernanza Multi-Actor. Por ejemplo, la retroalimentación de ONGs sobre las guías simplificadas llevó a optimizaciones en el protocolo de notificación (Sección 8.6.3), mejorando la gestión adecuada de activos (Sección 1.4). Estas innovaciones preparan el análisis ético y social en la Sección 13.3.

13.3 Avances en la Responsabilidad Ética y Social

Las innovaciones operativas de la Sección 13.2 se enriquecen con avances en la responsabilidad ética y social, que posicionan el modelo como un referente para la investigación responsable. Esta subsección evalúa cómo las consideraciones éticas, legales, y sociales (ELSI, Sección 11) y la participación Multi-Actor (Sección 10) promueven la equidad, privacidad, y confianza en la investigación medioambiental. El análisis se fundamenta en el 7.3 "Conciencia" de ISO/IEC 27001:2022.

Una contribución clave es la integración de la privacidad por diseño (Sección 11.2), que minimiza la recolección de datos en el SIEM (Sección 6.2.2) y establece mecanismos de consentimiento informado para datos geoespaciales (Sección 3.1). Este enfoque, validado en la planificación empírica (Sección 9.4), asegura la autonomía de las comunidades locales (Sección 10.1), mitigando riesgos éticos de percepción de vigilancia (Tabla 8 de la Sección 5.3.1). Por ejemplo, el consentimiento explícito gestionado por ONGs fomenta la confianza comunitaria, un estándar para proyectos con datos sensibles.

La ***equidad en el acceso*** es otra contribución significativa, abordada mediante guías simplificadas (Sección 8.4) y capacitaciones adaptadas (Sección 10.3) para ONGs y comunidades con baja madurez tecnológica (Sección 3.2). Estas medidas, evaluadas mediante encuestas de satisfacción (Sección 10.4), reducen la brecha digital (Sección 11.4), asegurando que todos los actores se beneficien de la seguridad, conforme al 5.2 " Principio de Transparencia" de ISO/IEC 38500:2024.

La gestión de la confianza se fortalece con foros comunitarios (Sección 10.4) y comunicaciones transparentes (Sección 11.4), que explican el uso de datos climáticos y geoespaciales. Estos avances, documentados en la Tabla 11, preparan las perspectivas estratégicas en la Sección 13.4.

13.4 Perspectivas Estratégicas para la Sostenibilidad y Escalabilidad

Los avances éticos y sociales de la Sección 13.3 se complementan con perspectivas estratégicas que posicionan el modelo como un referente para la sostenibilidad y escalabilidad en la investigación medioambiental. Esta subsección analiza cómo la estrategia integrada de sostenibilidad (Sección 12.6) y la planificación del modelo establecen un marco replicable para

proyectos futuros. El análisis se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el PM-6 "Medidas de rendimiento" de NIST SP 800-53 Rev. 5, que orientan la planificación estratégica.

Una contribución clave es la estrategia integrada de sostenibilidad (Sección 12.6), que combina pilares tecnológicos (ciclos de reemplazo, Sección 12.2), económicos (financiación compartida, Sección 12.3), organizacionales (comités Multi-Actor, Sección 12.4), y ambientales (resiliencia, Sección 12.5). Los Indicadores Clave de Sostenibilidad (IKS), como una tasa de actualización tecnológica >80% cada 5 años, permiten medir el desempeño a largo plazo, estableciendo un modelo para proyectos de datos sensibles. Por ejemplo, la financiación compartida entre gobiernos y universidades (Sección 12.3) asegura recursos para escalar el modelo a nuevas regiones, mitigando riesgos financieros (Tabla 8 de la Sección 5.3.1).

La escalabilidad del modelo radica en su capacidad para adaptarse a nuevos contextos, actores, o tecnologías. La arquitectura lógica (Sección 6.4.1) y los protocolos Multi-Actor (Sección 6.1.3), diseñados para entornos heterogéneos (Sección 2.3.3), permiten incorporar nuevos actores (Sección 10.2) o regiones, como se planificó en el piloto (Sección 9.3). Por ejemplo, los ciclos de reemplazo tecnológico (Sección 12.2) aseguran la integración de algoritmos post-cuánticos, manteniendo la confidencialidad (Sección 1.4) en proyectos futuros.

La replicabilidad del modelo se refuerza con la documentación auditable (Tabla 11) y las revisiones anuales de sostenibilidad (Sección 12.6), que proporcionan un marco adaptable para otros proyectos medioambientales. Estas perspectivas, vinculadas con la mejora continua (Sección 8.6), consolidan el impacto del modelo, contribuyendo a los objetivos de la Sección 1.4.

Capítulo 14: Líneas de Investigación y Trabajos Futuros

El Modelo de Seguridad de la Información establece un marco metodológico para proteger activos críticos en proyectos de investigación medioambiental, abordando desafíos de entornos distribuidos, tecnológicamente heterogéneos y Multi-Actor (Sección 1.1 Planteamiento del Problema). Esta sección, alineada con la fase "Actuar" del ciclo PHVA (Sección 8 Fase Actuar (Act)), reafirma el compromiso con la evolución sistemática del modelo, definiendo una hoja de ruta estratégica para guiar sus futuras iteraciones y adaptaciones. Su objetivo es asegurar la resiliencia, relevancia y eficacia del modelo frente a amenazas dinámicas, avances tecnológicos y requisitos operativos cambiantes, cumpliendo con la Cláusula 9.3.2 "Entradas de la revisión por la dirección" y Cláusula 9.3.3 "Resultados de la Revisión por la Dirección" de ISO/IEC 27001:2022, que promueven la mejora continua, y el proceso MEA01 " Gestionar la monitorización del desempeño y la conformidad " de COBIT 2019.

Figura 22

Marco Estratégico para la Evolución del Modelo de Seguridad



Fuente: Elaboración propia

La hoja de ruta se organiza en cuatro líneas estratégicas: (1) consolidación y optimización de los componentes existentes, (2) especialización y adaptación a contextos dinámicos, (3)

integración de tecnologías emergentes para anticipar amenazas, y (4) evolución del marco de gobernanza y medición del desempeño. Estas líneas protegen activos como datos de calidad del aire y parámetros hídricos (Sección 1.4 Objetivos), garantizando confidencialidad, integridad y disponibilidad (Sección 2.1.3 Principios de Seguridad). Es importante señalar que estos trabajos son necesarios para mantener la eficacia del modelo en entornos de investigación medioambiental, respondiendo a retos como la interoperabilidad de sistemas heterogéneos (Sección 2.3.3 Infraestructura Tecnológica en Proyectos de Investigación) y la coordinación Multi-Actor (Sección 10 Análisis de las Partes Interesadas y Estrategia de Participación). Por lo tanto, esta agenda posiciona el modelo como un estándar sostenible (Sección 12 Estrategia para la Sostenibilidad a Largo Plazo del Modelo de Seguridad), impulsando la innovación en la seguridad de la información.

14.1 Priorización de las Líneas Estratégicas Futuras

Las líneas estratégicas definidas en esta sección representan una visión a largo plazo para la evolución del modelo de seguridad. Sin embargo, para orientar a futuros investigadores e implementadores, es muy importante priorizar estos esfuerzos. Para ello, se propone una matriz de priorización basada en dos criterios clave:

- **Impacto:** El grado en que la línea estratégica fortalece la seguridad, la eficacia y la relevancia del modelo actual. Un alto impacto resuelve debilidades significativas o añade capacidades críticas.
- **Esfuerzo:** La cantidad de recursos, tiempo y complejidad técnica requeridos para su desarrollo e implementación. Un alto esfuerzo implica una investigación profunda, desarrollo complejo o una inversión considerable.

La combinación de estos dos factores permite clasificar cada línea estratégica para guiar la toma de decisiones sobre los siguientes pasos.

Tabla 13

Priorización para Trabajos Futuros

LÍNEA ESTRATÉGICA (LE)	DESCRIPCIÓN	EVALUACIÓN DE IMPACTO	EVALUACIÓN DE ESFUERZO	PRIORIDAD SUGERIDA	JUSTIFICACIÓN
LE1: CONSOLIDACIÓN Y OPTIMIZACIÓN	Fortalecer y mejorar la eficiencia de los componentes y controles existentes del modelo.	Alto	Medio	Alta (Implementar Primero)	Esta línea aborda directamente el fortalecimiento del núcleo del modelo. Su impacto en la seguridad y robustez es inmediato y fundamental antes de avanzar a especializaciones o innovaciones.
LE4: EVOLUCIÓN DEL MARCO DE GESTIÓN Y MEDICIÓN	Perfeccionar el ciclo PHVA, las métricas (KPIs/KRIs) y el marco de madurez.	Medio	Bajo a Medio	Alta (Implementar junto a LE1)	Aunque su impacto técnico directo es menor que el de LE1, el esfuerzo es relativamente bajo y proporciona un valor inmenso para la gestión, la gobernanza y la demostración de la eficacia del modelo. Es una "ganancia rápida" estratégica.
LE2: ESPECIALIZACIÓN Y ADAPTACIÓN	Diseñar submodelos de seguridad para áreas específicas como OT, datos abiertos o entornos multi-cloud.	Alto	Alto	Media (Planificar a Mediano Plazo)	Tiene un altísimo impacto al hacer el modelo aplicable a contextos muy específicos y de gran relevancia. Sin embargo, el esfuerzo de desarrollar y validar cada submodelo es considerable, convirtiéndolo en un gran proyecto estratégico.
LE3: INNOVACIÓN Y PROSPECTIVA	Investigar e integrar tecnologías emergentes (IA, Blockchain, Criptografía Post-Cuántica) y ciberinteligencia.	Medio a Alto	Muy Alto	Baja (Investigación a Largo Plazo)	Esta línea es clave para la sostenibilidad a muy largo plazo y para mantener el modelo a la vanguardia. No obstante, el alto nivel de esfuerzo, incertidumbre y complejidad la sitúan como una prioridad para fases de investigación y desarrollo futuras.

La priorización de las líneas estratégicas se puede visualizar en la siguiente figura de Impacto vs. Esfuerzo. Las iniciativas situadas en el cuadrante superior izquierdo, como la LE1, ofrecen el mayor retorno sobre la inversión y deben ser el foco principal de los esfuerzos iniciales. La LE4 también presenta una alta prioridad por su bajo-esfuerzo relativo y su valor para la gestión. La LE2 representa un proyecto estratégico de gran magnitud a mediano plazo, mientras que la LE3 se sitúa como una línea de investigación y desarrollo a largo plazo debido a su alta complejidad.

Figura 23

Impacto vs. Esfuerzo



Fuente: Elaboración propia

14.2 Línea Estratégica 1 (LE1): Consolidación y Optimización del Modelo Existente

Objetivo: Fortalecer las bases del modelo actual, mejorar su eficiencia y robustecer sus componentes fundamentales para garantizar una protección efectiva de los activos críticos (Sección 1.4 Objetivos) y alinearse con la fase "Actuar" del ciclo PHVA (Sección 8 Fase Actuar (Act)).

14.2.1 *Profundización de la Cobertura de Seguridad por Dominios Tecnológicos y Capas de Infraestructura*

14.2.1.1 Controles para la Capa de Captura.

Esta línea propone una investigación detallada para identificar y desarrollar mejoras específicas en la aplicación de controles y arquitecturas de seguridad a través de las capas tecnológicas descritas en la Sección 2.3.3 Infraestructura Tecnológica en Proyectos de Investigación: captura, transmisión, almacenamiento y procesamiento. En la capa de captura, se optimizarán controles para sensores IoT, ejemplo los sensores que miden niveles de pH en cuencas hídricas (Sección 2.3.3.1 Infraestructura de Captura y Adquisición de Datos). Una posible aplicación sería implementar algoritmos de cifrado ligero, como Speck, para proteger la confidencialidad de los datos de pH, diseñados para operar en dispositivos de baja potencia con un consumo energético inferior al 5% del total disponible. Estos algoritmos se complementarán con configuraciones seguras de firmware, como el bloqueo de puertos no esenciales y la actualización automática de credenciales mediante Vault by HashiCorp, para prevenir accesos no autorizados, abordando vulnerabilidades comunes en sensores IoT, como credenciales predeterminadas.

14.2.1.2 Controles para la Capa de Transmisión.

En la capa de transmisión, se investigarán soluciones para redes satelitales que conectan sensores de calidad del aire en áreas urbanas remotas (Sección 2.3.3.2 Infraestructura de Transmisión y Comunicaciones). Un caso representativo sería implementar autenticación multifactor (MFA) basada en certificados digitales, integrando tokens efímeros para autenticar nodos de transmisión, lo que reduce el riesgo de intercepciones en canales satelitales a una tasa inferior al 0.1%. También se explorarán técnicas de compresión de datos seguras, usando Apache NiFi para optimizar la transmisión en entornos de baja conectividad, asegurando la integridad de los datos transmitidos mediante sumas de verificación con una tasa de error inferior al 0.01%.

14.2.1.3 Controles para la Capa de Procesamiento

En la capa de procesamiento, se optimizarán controles de acceso basado en roles (RBAC) para plataformas en la nube que analizan datos geoespaciales de dióxido de carbono (Sección 2.3.3.3 Infraestructura de Almacenamiento y Procesamiento). Estos controles incluirán políticas

de autorización granular que restrinjan el acceso según el rol del usuario (por ejemplo, investigador, administrador), complementadas con auditorías de acceso en tiempo real y registros de actividad gestionados por Apache NiFi, asegurando una trazabilidad del 100%. También se investigarán técnicas de anonimización, como k-anonimato, para proteger datos geoespaciales en bases de datos compartidas, minimizando riesgos de Re-identificación a una tasa inferior al 0.1%.

14.2.1.4 Validación y Métricas de Desempeño.

La investigación abarcará controles preventivos, detectivos y correctivos, segmentados por dominio tecnológico (nube, local, híbrido). Por ejemplo, en la transmisión de datos de calidad del aire, se desarrollarán sistemas de detección de intrusos basados en análisis de tráfico para identificar manipulaciones en redes satelitales, integrando monitoreo en tiempo real con alertas automáticas que prioricen incidentes en menos de 10 segundos. En la capa de EndPoints, se evaluarán configuraciones seguras para sensores IoT, incluyendo actualizaciones automáticas de firmware y bloqueo de interfaces no utilizadas, asegurando una resistencia del 95% frente a ataques físicos o lógicos. La investigación incluirá pruebas en entornos simulados que repliquen las condiciones de operación de proyectos medioambientales, como estaciones de monitoreo en cuencas hídricas, validando métricas como el tiempo medio de detección de anomalías (objetivo: <10 segundos) y la tasa de falsos positivos (objetivo: <2%).

Justificación: La heterogeneidad tecnológica y las limitaciones de conectividad en entornos remotos (Sección 1.1 Planteamiento del Problema) generan riesgos residuales, como accesos no autorizados a sensores IoT o alteraciones en datos transmitidos (Tabla 8 “Análisis de Riesgos y Amenazas”, Sección 5.3.1 Identificación de Amenazas y Vulnerabilidades). Es importante señalar que la Sección 6.2.2 Diseño de Controles Técnicos Aplicables, indica la necesidad de controles granulares para mitigar estos riesgos. La limitación de la versión 1.0 , que carecía de segmentación suficiente por dominio tecnológico (Sección 1.3.2 Limitaciones del Diseño Propuesto), justifica esta investigación. Este trabajo se basa en el Control 5.12 "Clasificación de la Información" y el Control 5.17 "Información de Autenticación" de ISO/IEC 27002:2022, el MAR.22: Valoración de las amenazas" de MAGERIT v3 Libro I, y el Control SC-12 " Establecimiento y Gestión de Claves Criptográficas " de NIST SP 800-53 Rev. 5.

Propuesta:

- Diseñar controles segmentados: MFA con certificados digitales y tokens efímeros para redes satelitales, cifrado AES-256 con anonimización para plataformas en la nube, y detección de anomalías en sensores IoT mediante análisis de patrones, usando Apache NiFi y Vault by HashiCorp.
- Ejecutar pruebas de penetración simulando monitoreo de pH en cuencas hídricas, conforme a la Sección 9.4 realizando la Ejecución del Plan de Validación Empírica, para evaluar la resistencia frente a ataques.
- Desarrollar métricas de desempeño, como el tiempo de detección de anomalías y la tasa de falsos positivos, alineadas con la Sección 7.2 Evaluación de la Eficacia del Diseño, y de los Controles.
- Implementar firewalls de próxima generación para redes satelitales, integrados con sistemas de detección de intrusos, conforme a la Sección 6.2.2 Diseño de Controles Técnicos Aplicables.
- Documentar resultados en un informe técnico que actualice el análisis de riesgos (Sección 5.3 Análisis y Evaluación de Riesgos) para la fase "Planificar" (Sección 5 Caracterización, Análisis de Riesgos y Bases del Diseño).
- Realizar simulaciones de escenarios de baja conectividad, conforme a la Sección 9.3 Plan Detallado de Implementación Conceptual.

Resultados Esperados: Se proyecta que, a raíz de la implementación completa del Modelo y de las actividades planificadas en la Sección 9.4 “Plan Detallado de Validación Empírica”, se logre una reducción estimada del riesgo residual en el orden del 20%, como objetivo técnico de referencia. Este valor puede descomponerse, a modo de meta operativa, en tres dominios tecnológicos estratégicos:

- Captura: Reducción del 15% en riesgos asociados, mediante controles orientados a disminuir la tasa de accesos no autorizados a niveles inferiores al 0.5%.
- Transmisión: Disminución del riesgo en un 20%, con énfasis en garantizar que las tasas de intercepción de datos estén por debajo del 0.1%.

- Procesamiento: Mejora del 25% en la protección de datos procesados, con foco en reducir los riesgos de Re identificación a niveles menores al 0.1%.

Estos valores deben interpretarse como parámetros de validación propuestos que orientan la definición de indicadores de desempeño (KPIs) y métricas específicas, cuya medición será afinada en el marco de las acciones descritas en la Sección 7 “Fase Verificar (Check)”. En esta etapa, se espera la elaboración de un informe técnico de resultados, que consolide los hallazgos del proceso de validación y retroalimente el ciclo de mejora continua del Modelo.

14.2.2 *Refinamiento de la Arquitectura de Seguridad y Control Transversales*

14.2.2.1 Políticas de Acceso Dinámico.

Esta línea propone avanzar en la arquitectura lógica del modelo (Sección 6.4.1 Arquitectura Lógica del Modelo de Seguridad) mediante la integración de principios de Confianza Cero (Zero Trust) y la optimización de controles transversales, como gestión de identidades y accesos (IAM), criptografía, y monitoreo continuo (SIEM). Para la gestión de IAM, se implementarán políticas de acceso dinámico para proteger datos de calidad del aire recopilados por sensores IoT y transmitidos a través de redes Zigbee a plataformas en la nube (Sección 2.3.3 Infraestructura Tecnológica en Proyectos de Investigación). Una posible aplicación sería evaluar el contexto (ubicación del usuario, tipo de dispositivo, patrones de comportamiento) utilizando protocolos como OAuth 2.0, garantizando accesos autorizados con una tasa de error inferior al 0.5%. Estas políticas se integrarán con sistemas de autenticación federada, gestionados por Vault by HashiCorp, para validar identidades entre instituciones colaboradoras.

14.2.2.2 Monitoreo Continuo con SIEM.

Para el monitoreo continuo, se desarrollarán capacidades de SIEM con algoritmos de aprendizaje automático para detectar anomalías en datos de turbidez, como intentos de acceso no autorizado a bases de datos (Sección 2.3.3.3). Un caso representativo sería implementar modelos de ML basados en análisis de comportamiento, detectando desviaciones en patrones de acceso en menos de 10 segundos, con una tasa de falsos positivos inferior al 2%. Estos modelos se integrarán

con Apache NiFi para procesar logs en tiempo real, generando alertas priorizadas para los administradores.

14.2.2.3 Segmentación de Redes y Criptografía.

La investigación optimizará la segmentación lógica de redes Zigbee, por ejemplo, para aislar flujos de datos de dióxido de carbono, implementando subredes virtuales que reduzcan la superficie de ataque frente a ataques de denegación de servicio (DoS) a una tasa inferior al 0.1%. También se investigarán soluciones de gestión de claves criptográficas, usando Vault by HashiCorp, para garantizar la integridad y confidencialidad en todas las capas (red, endpoint, aplicación, datos). Una posible aplicación sería implementar cifrado homomórfico para procesar datos de calidad del aire en la nube sin descifrarlos, permitiendo análisis seguros con una tasa de error inferior al 0.01%.

14.2.2.4 Respuesta a Incidentes.

En la capa de aplicación, se investigarán sistemas de monitoreo de integridad para detectar alteraciones en datos geoespaciales, complementados con auditorías automatizadas de logs gestionadas por Apache NiFi, asegurando una trazabilidad del 100%. En la capa de Endpoint, se optimizarán controles para sensores IoT, incluyendo autenticación basada en hardware y bloqueo de interfaces no esenciales, con una resistencia del 95% frente a ataques físicos o lógicos. La investigación también abordará la respuesta a incidentes mediante mecanismos automatizados en el SIEM, como el bloqueo temporal de accesos sospechosos en menos de 5 segundos, alineados con la Sección 6.5 Mecanismos de Respuesta a Incidentes de Seguridad.

14.2.2.5 Validación y Métricas.

La investigación incluirá pruebas de carga para evaluar el rendimiento de los controles en escenarios de alta demanda, como el procesamiento simultáneo de datos geoespaciales, con un tiempo de respuesta objetivo de <1 segundo. También se desarrollarán guías de configuración para la arquitectura de Confianza Cero, alineadas con la Sección 9.3 Plan de Implementación, incluyendo configuraciones recomendadas para Apache NiFi y Vault by HashiCorp.

Justificación: La interoperabilidad de sistemas heterogéneos (Sección 2.3.3) introduce vulnerabilidades, como accesos no autorizados o manipulaciones de datos (Tabla 8, Sección 5.3.1). Es pertinente mencionar que la Sección 6.2.5 Incorporación de Controles de Defensa en Profundidad señala la necesidad de controles dinámicos. La limitación de la versión 1.0, que carecía de mecanismos transversales robustos (Sección 6 Limitaciones del Diseño Propuesto), justifica esta investigación. Este trabajo se basa en el Control 5.15 "Control de Acceso" y el Control 5.17 "Información de Autenticación" de ISO/IEC 27002:2022, la Familia IA "Identificación y Autenticación" de NIST SP 800-53 Rev. 5, y el principio de interoperabilidad definido en TOGAF como parte de la Visión de Flujo de Información sin Límites, que promueve la integración segura y abierta entre sistemas mediante estándares y arquitecturas compatibles.

Propuesta:

- Diseñar una arquitectura de Confianza Cero con segmentación lógica para redes Zigbee, usando OAuth 2.0 y Vault by HashiCorp, conforme a la Sección 6.2.3.
- Desarrollar prototipos de SIEM con ML para datos de turbidez, usando Apache NiFi, siguiendo el Control SI-4 "Monitoreo del Sistema" de NIST SP 800-53 Rev. 5.
- Implementar cifrado homomórfico para datos de calidad del aire, alineado con la Sección 6.2.2.
- Validar la arquitectura mediante simulacros de ataques DoS, conforme a la Sección 6.5.
- Desarrollar guías de configuración, alineadas con la Sección 9.3.
- Documentar resultados para la fase "Hacer" (Sección 6 Fase Hacer (Do)).

Resultados Esperados: Se proyecta una mejora del 30 % en la capacidad de detección de anomalías, alcanzando un tiempo medio de detección inferior a 10 segundos y una tasa de falsos positivos por debajo del 2 %. Asimismo, se espera una reducción del 25 % en la superficie de ataque, reflejada en una tasa de intentos de denegación de servicio (DoS) inferior al 0,1 %. Estas métricas corresponden a los parámetros definidos en la Sección 7.2 "Evaluación de la Eficacia de

los Controles", y están destinadas a alimentar el proceso de mejora continua durante la fase Verificar del ciclo PHVA (Sección 7 "Fase Verificar (Check)").

14.2.3 *Optimización Continua de la Gobernanza del Modelo, Gestión de Riesgos Integrada y Cumplimiento Dinámico (GRC)*

14.2.3.1 Cuadro de Mando GRC.

Esta línea propone optimizar los procesos de gobernanza Multi-Actor (Sección 0.2 Roles y Responsabilidades en la Gobernanza e Implementación) y automatizar el cumplimiento normativo mediante herramientas de Gobernanza, Riesgo y Cumplimiento (GRC). Para la gobernanza, se desarrollará un cuadro de mando que monitoree en tiempo real los Indicadores Clave de Riesgo (KRIs) relacionados con accesos no autorizados a datos de pH en plataformas en la nube (Sección 2.3.3.3 Infraestructura de Almacenamiento y Procesamiento). Un caso representativo sería medir la tasa de accesos no autorizados (objetivo: <0.5%) y el tiempo de respuesta a incidentes (objetivo: <5 minutos), usando Apache NiFi para procesar datos en tiempo real. El cuadro reflejará el cumplimiento con ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5, y MAGERIT v3, asegurando una conformidad del 95%.

14.2.3.2 Auditorías Automatizadas.

Para el cumplimiento dinámico, se investigarán procesos automatizados para auditorías, generando reportes en tiempo real que evalúen la conformidad de controles de acceso con la Cláusula 5.1 "Liderazgo y Compromiso" de ISO/IEC 27001:2022. Una posible aplicación sería implementar flujos de trabajo automatizados, gestionados por Apache NiFi, que verifiquen la aplicación de RBAC en plataformas en la nube, identificando desviaciones en menos de 1 minuto. También se investigarán soluciones de análisis predictivo para anticipar riesgos emergentes, como errores de configuración, con una precisión del 90%, alineadas con la Sección 5.3 Análisis y Evaluación de Riesgos.

14.2.3.3 Gobernanza Multi-Actor.

Se establecerán comités Multi-Actor permanentes para revisar riesgos trimestralmente, coordinando universidades, ONGs y entidades gubernamentales, con roles definidos (por ejemplo,

oficial de cumplimiento) para garantizar la rendición de cuentas. También se investigarán plantillas estandarizadas para reportes de cumplimiento y guías para la toma de decisiones, usando Vault by HashiCorp para gestionar credenciales de acceso a los reportes. Estas guías incluirán formatos simplificados para ONGs con baja madurez tecnológica, asegurando una adopción del 80% en entornos de conectividad limitada.

14.2.3.4 Retroalimentación y Capacitación.

La investigación optimizará mecanismos de retroalimentación mediante encuestas de satisfacción (Sección 10.4 Mecanismos de Retroalimentación), evaluando la usabilidad del cuadro de mando (objetivo: satisfacción >85%). También se investigarán capacitaciones adaptadas para comités Multi-Actor (Sección 10.3 Estrategias de Comunicación y Capacitación Adaptadas), con talleres que usen simulaciones de riesgos para mejorar la toma de decisiones, logrando una participación del 90%.

Justificación: La asimetría en la madurez tecnológica entre actores (Sección 3.3 Características Particulares de los Proyectos Medioambientales) complica la gobernanza (Sección 1.1 Planteamiento del Problema). Es oportuno mencionar que la Sección 11.3 Marco Legal y Cumplimiento Normativo Ampliado, identifica la falta de automatización como una limitación. La versión 1.0 de (MGSI) carecía de mecanismos automatizados para auditorías (Sección 1.3.2 Limitaciones del Diseño Propuesto), justificando esta investigación. Este trabajo se basa en la Sección 5.3 "Integración" de ISO 31000:2018, el proceso DSS05 "Gestionar los servicios de seguridad" de COBIT 2019, y el Control CA-2 "Evaluaciones de Control" de NIST SP 800-53 Rev. 5.

Propuesta:

- Implementar una plataforma GRC para auditorías automáticas, con Apache NiFi, alineada con el Control CA-2 de NIST SP 800-53 Rev. 5.
- Crear comités Multi-Actor para revisar riesgos, con Vault by HashiCorp, conforme a la Sección 12.4 Componente Organizacional.
- Desarrollar análisis predictivo para riesgos, alineado con la Sección 5.3.
- Diseñar guías para ONGs, con capacitaciones, conforme a la Sección 10.3.

- Documentar resultados para la fase "Planificar" (Sección 5).
- Realizar talleres de capacitación, conforme a la Sección 10.3.

Resultados Esperados: Se estima una reducción del 40 % en el tiempo de ejecución de auditorías, pasando de 10 a 6 horas promedio por proceso, así como el logro de un 95 % de conformidad normativa. Estas estimaciones se fundamentan en los indicadores definidos en la Sección 7.4 "Resultados de la Fase Verificar", y están orientadas a fortalecer la retroalimentación operativa en la fase Verificar del ciclo PHVA (Sección 7 "Fase Verificar (Check)").

14.3 Línea Estratégica 2 (LE2): Especialización y Adaptación del Modelo a Contextos Dinámicos

Objetivo: Asegurar que el modelo sea aplicable y efectivo en los diversos y cambiantes contextos de operación y uso, especialmente los relacionados con la investigación medioambiental, alineándose con la fase "Actuar" del ciclo PHVA (Sección 8 Fase Actuar (Act)).

14.3.1 *Diseño y Desarrollo de Submodelos de Seguridad Especializados para Áreas de Alto Impacto o Requerimientos Particulares*

14.3.1.1 Controles para la Seguridad de Datos de Investigación Medioambiental.

El desarrollo de submodelos de seguridad especializados responde a la necesidad de abordar áreas de alto impacto en proyectos de investigación, considerando la heterogeneidad de activos y procesos. Para el submodelo de datos de investigación medioambiental, se investigarán controles que protejan el ciclo de vida de datos sensibles, como mediciones de calidad del aire recopiladas por sensores IoT (Sección 2.3.3.1 Infraestructura de Captura y Adquisición de Datos). Una posible aplicación sería implementar técnicas de anonimización avanzada, como k-anonimato, para prevenir la Re-identificación de datos compartidos entre instituciones, asegurando la confidencialidad durante la compartición. Por ejemplo, los datos de dióxido de carbono recopilados en áreas urbanas se procesarán con k-anonimato para generalizar ubicaciones, reduciendo el riesgo de Re-identificación a una tasa inferior al 0.1%. Se propone usar Apache NiFi para gestionar flujos de datos seguros, procesando datos anonimizados antes de su transferencia a plataformas en la nube.

14.3.1.2 Cifrado Diferencial y Políticas de Retención.

También se investigarán soluciones de cifrado diferencial para datos almacenados en plataformas en la nube (Sección 2.3.3.3 Infraestructura de Almacenamiento y Procesamiento), permitiendo análisis seguros sin exponer información sensible. Estas soluciones se complementarán con políticas de retención de datos que definan períodos de almacenamiento basados en la sensibilidad, como 5 años para datos de calidad del aire de alta sensibilidad, alineadas con la Sección 3.1 Clasificación y Protección de Datos Medioambientales Sensibles. Por ejemplo, los datos de calidad del aire se cifrarán diferencialmente para permitir análisis estadísticos sin descifrado, usando Vault by HashiCorp para gestionar claves de cifrado de manera segura, con una tasa de error de cifrado inferior al 0.01%.

14.3.1.3 Controles para Infraestructuras de Tecnología Operacional (OT).

Para el submodelo de infraestructuras de tecnología operacional (OT), se optimizarán controles para sistemas de monitoreo ambiental, como sensores IoT que miden niveles de turbidez en cuencas hídricas (Sección 2.3.3.1). Un caso representativo sería implementar firewalls de próxima generación para proteger nodos de sensores contra accesos no autorizados, integrados con autenticación basada en hardware, como chips seguros, para validar dispositivos en redes satelitales (Sección 2.3.3.2 Infraestructura de Transmisión y Comunicaciones). También se investigarán sistemas de detección de anomalías físicas, como sensores de vibración que alerten sobre manipulaciones en estaciones de monitoreo, asegurando la integridad de los datos recopilados con una tasa de detección del 95%. Estas soluciones abordarán los requisitos únicos de entornos OT, como operar en condiciones adversas con conectividad limitada, usando Vault by HashiCorp para gestionar secretos de autenticación.

14.3.1.4 Controles para Plataformas de Colaboración y Datos Abiertos

Para el submodelo de plataformas de colaboración científica y datos abiertos, se investigarán controles que garanticen la seguridad en entornos colaborativos, como bases de datos geoespaciales compartidas (Sección 2.3.3.3). Una posible aplicación sería implementar sistemas de control de acceso basado en atributos (ABAC) que restrinjan el acceso según el propósito de uso (por ejemplo, investigación académica, políticas públicas), complementados con BlockChain

para garantizar la trazabilidad de los datos compartidos. Por ejemplo, los datos de calidad del aire se registrarán en una cadena de bloques privada, asegurando que no se alteren durante la compartición, con una tasa de integridad del 100%. Estas soluciones de BlockChain se considerarán prácticas emergentes, alineadas con principios generales de trazabilidad del Control 5.12 "Clasificación de la Información" de ISO/IEC 27002:2022, pero no controles normativos explícitos.

14.3.1.5 Validación y Guías de Implementación.

La investigación incluirá pruebas en entornos simulados que repliquen escenarios de colaboración científica, como proyectos Multi-Institucionales, ejemplo de monitoreo de dióxido de carbono, para validar la efectividad de los controles mediante métricas como la tasa de Re-Identificación (objetivo: <0.1%) y el tiempo de detección de accesos no autorizados (objetivo: <10 segundos). También se desarrollarán guías de implementación para cada submodelo, detallando configuraciones, requisitos de infraestructura, y procedimientos de auditoría, alineadas con la Sección 9.3 Plan de Implementación. Estas guías incluirán plantillas para auditorías de cumplimiento, configuraciones recomendadas para Apache NiFi y Vault by HashiCorp, y procedimientos para validar la trazabilidad de datos en Blockchain.

Justificación: La heterogeneidad de activos y procesos en proyectos medioambientales (Sección 3.3 Características Particulares de los Proyectos Medioambientales) genera requisitos únicos no cubiertos por modelos genéricos (Tabla 2, Sección 3.3). Es importante señalar que la Sección 6.2.2 Diseño de Controles Técnicos Aplicables indica la necesidad de controles especializados para mitigar riesgos como la Re-Identificación de datos (Tabla 8, Sección 5.3.1). La limitación de la versión 1.0 del (MGSI), que no abordaba entornos OT o datos abiertos (Sección 1.3.2 Limitaciones del Diseño Propuesto), justifica esta investigación. Este trabajo se basa en el Control 5.12 "Clasificación de la Información", el Control 5.17 "Información de Autenticación" de ISO/IEC 27002:2022, la Sección 7.3 "Análisis de los Riesgos de Seguridad de la Información" de ISO/IEC 27005:2022, y el Control AC-5 "Separación de Funciones" de NIST SP 800-53 Rev.5.

Propuesta:

- Diseñar un submodelo para datos medioambientales con anonimización (k-anonimato) y cifrado diferencial, usando Apache NiFi, alineado con la Sección 3.1.
- Desarrollar un submodelo OT con firewalls y autenticación basada en hardware, usando Vault by HashiCorp, conforme a la Sección 6.2.2.
- Crear un submodelo para datos abiertos con ABAC y Blockchain, como práctica emergente, alineado con la Sección 6.2.3.
- Ejecutar pruebas en entornos simulados Ejemplo de monitoreo de dióxido de carbono, conforme a la Sección 9.4.
- Desarrollar guías de implementación para cada submodelo, alineadas con la Sección 9.3.
- Documentar resultados en un informe técnico para informar la fase "Hacer" (Sección 6 Fase Hacer (Do)).

Resultados Esperados: Se proyecta una reducción del 25 % en riesgos específicos, desglosada en: 20 % para datos medioambientales (tasa de Re-Identificación < 0.1 %), 30 % en entornos de Tecnología Operacional (OT) (tiempo medio de detección < 10 segundos), y 25 % en plataformas de datos abiertos (tasa de accesos no autorizados < 0.5 %). Estas cifras se fundamentan en las métricas definidas en la Sección 9.4 "Plan Detallado de Validación Empírica". Se espera que los submodelos operativos generados retroalimenten directamente la fase Verificar (Sección 7 "Fase Verificar (Check)"), reforzando la protección de datos y la seguridad en sistemas OT.

14.3.2 *Adaptación Proactiva del Modelo a Nuevos Paradigmas Operativos, Tecnológicos y de Colaboración*

14.3.2.1 Seguridad en Entornos Híbridos y Remotos.

Esta línea propone investigar ajustes al modelo para alinearse con tendencias emergentes, como entornos de trabajo híbridos y remotos, adopción de servicios en la nube (IaaS, PaaS, SaaS), modelos Multi-Cloud, e interoperabilidad y federación de identidades con instituciones colaboradoras. Para entornos híbridos y remotos, se investigarán controles para proteger el acceso

remoto a plataformas en la nube que procesan datos de calidad del aire (Sección 2.3.3.3 Infraestructura de Almacenamiento y Procesamiento). Un caso representativo sería implementar soluciones de red privada virtual (VPN) con cifrado AES-256 y autenticación multifactor (MFA) basada en biometría, como reconocimiento facial, para garantizar accesos seguros desde ubicaciones remotas con una tasa de error de autenticación inferior al 0.5%. Estas soluciones se complementarán con sistemas de monitoreo de dispositivos remotos, asegurando que cumplan con políticas de seguridad (por ejemplo, software actualizado) antes de conectarse, usando Vault by HashiCorp para gestionar credenciales de autenticación.

14.3.2.2 Gestión de Identidades en Modelos Multi-Cloud.

Para la adopción de servicios en la nube, se investigarán controles para modelos Multi-Cloud que gestionan datos de pH en cuencas hídricas (Sección 2.3.3.3). Una posible aplicación sería implementar sistemas de gestión de identidades en la nube (IAM) que sincronicen políticas de acceso entre proveedores de IaaS (como AWS) y PaaS (como Azure), integrados con Vault by HashiCorp para gestionar secretos de autenticación. También se explorarán auditorías automatizadas de configuraciones para prevenir errores, como permisos excesivos, mediante herramientas de análisis continuo, asegurando una tasa de errores de configuración inferior al 1%. Se investigarán soluciones de soberanía de datos, como el almacenamiento cifrado en regiones específicas, para cumplir con requisitos legales (Sección 11.3 Aspectos Legales), usando Apache NiFi para gestionar flujos de datos seguros.

14.3.2.3 Interoperabilidad y Federación de Identidades.

Para la interoperabilidad y federación de identidades, se investigarán sistemas que permitan a instituciones colaboradoras (por ejemplo, universidades y ONGs) compartir datos de dióxido de carbono de manera segura (Sección 2.3.3.3). Una posible aplicación sería implementar protocolos de federación de identidades, como SAML 2.0, para validar usuarios entre organizaciones, asegurando interoperabilidad con una tasa de éxito de autenticación superior al 95%. Estas soluciones se complementarán con contratos de nivel de servicio (SLAs) que definan permisos de acceso y uso, considerados prácticas emergentes alineadas con 8.27 "Arquitectura segura de sistemas y principios de ingeniería" de ISO/IEC 27002:2022, pero no controles normativos explícitos. También se investigarán sistemas de autenticación basada en atributos (ABAC) para

plataformas colaborativas, permitiendo accesos condicionados según el rol y propósito del usuario, con una tasa de error de autorización inferior al 0.5%.

14.3.2.4 Validación y Guías de Configuración.

La investigación incluirá pruebas en entornos simulados de trabajo híbrido, como equipos remotos accediendo a plataformas Multi-Cloud para analizar datos de calidad del aire, validando la efectividad de los controles mediante métricas como la tasa de accesos validados (objetivo: >95%) y el tiempo de configuración de SLAs (objetivo: <1 hora). También se desarrollarán guías de configuración para entornos multi-cloud y federación de identidades, detallando requisitos de infraestructura, procedimientos de auditoría, y configuraciones recomendadas para Vault by HashiCorp y Apache NiFi, alineadas con la Sección 9.3 Plan de Implementación. Estas guías incluirán plantillas para auditorías de cumplimiento y SLAs, asegurando trazabilidad.

Justificación: La evolución de los entornos de trabajo y la creciente adopción de la Cloud (Sección 1.1 Planteamiento del Problema) generan nuevos riesgos, como errores de configuración en controles de acceso (Tabla 8, Sección 5.3.1 Identificación de Amenazas y Vulnerabilidades). Es importante señalar que la Sección 6.4.1 Arquitectura Lógica del Modelo de Seguridad, indica la necesidad de arquitecturas interoperables para soportar la misión de investigación. La limitación de la versión 1.0 del (MGSI), que no abordaba entornos híbridos o Multi-Cloud (Sección 1.3.2 Limitaciones del Diseño Propuesto), justifica esta investigación. Este trabajo se basa en 5.14 "Transferencia de la información" y en 5.17 "Información de Autenticación" de ISO/IEC 27002:2022, la Familia IA-8 "Identificación y Autenticación (Entidades No Organizacionales)" de NIST SP 800-53 Rev. 5, y la Interoperabilidad de TOGAF Ver 10.

Propuesta:

- Diseñar controles para entornos híbridos con VPN y MFA biométrica, usando Vault by HashiCorp, alineados con la Sección 6.2.2 Diseño de Controles Técnicos Aplicables.
- Desarrollar sistemas IAM para multi-cloud, con auditorías automatizadas mediante Apache NiFi, conforme a la Sección 6.2.3 Diseño de Controles Organizacionales y Administrativos.

- Implementar federación de identidades con SAML 2.0 para datos de dióxido de carbono, como práctica emergente, alineada con la Sección 10.2 Roles y Responsabilidades en la Gobernanza e Implementación.
- Ejecutar pruebas en entornos simulados de trabajo híbrido, conforme a la Sección 9.4 Ejecución del Plan de Validación Empírica.
- Desarrollar guías de configuración para Multi-Cloud y federación, alineadas con la Sección 9.3 Plan Detallado de Implementación Conceptual.
- Documentar resultados en un informe técnico para informar la fase "Planificar" (Sección 5 Caracterización, Análisis de Riesgos y Bases del Diseño).

Resultados Esperados: Conformidad del 90% en pruebas de interoperabilidad, medida por la tasa de accesos validados sin errores (>95%), y una reducción del 20% en errores de configuración en entornos multi-cloud (tasa <1%), según métricas de la Sección 9.4 Ejecución del Plan de Validación Empírica. Se espera un modelo adaptable que retroalimente la fase "Verificar" (Sección 7 Fase Verificar (Check)), fortaleciendo la seguridad en entornos híbridos.

14.4 Línea Estratégica 3 (LE3): Innovación, Prospectiva y Resiliencia Estratégica

Objetivo: Explorar e integrar tecnologías y enfoques emergentes para anticipar amenazas futuras y fortalecer la capacidad de recuperación del modelo y la organización, alineándose con la fase "Actuar" (Sección 8 Fase Actuar (Act)).

14.4.1 *Investigación e Integración Piloto de Tecnologías de Seguridad Emergentes*

14.4.1.1 Inteligencia Artificial y Aprendizaje Automático para Detección de Amenazas.

Esta línea propone investigar la viabilidad y el valor de integrar tecnologías emergentes para anticipar amenazas sofisticadas, mejorando la eficiencia del modelo. Para la inteligencia artificial (IA) y aprendizaje automático (ML), se investigarán algoritmos para la detección avanzada de amenazas, ejemplo en datos de calidad del aire recopilados por sensores IoT (Sección 2.3.3.1 Infraestructura de Captura y Adquisición de Datos). Una posible aplicación sería implementar modelos de ML basados en redes neuronales recurrentes para analizar patrones de datos, detectando accesos no autorizados en tiempo real en sistemas SIEM, con un tiempo medio

de detección inferior a 10 segundos y una tasa de falsos positivos menor al 2%. Estos modelos se integrarán con Apache NiFi para gestionar flujos de datos seguros, priorizando alertas y activando contramedidas, como el bloqueo de nodos sospechosos, en menos de 5 segundos.

14.4.1.2 Criptografía Post-Cuántica para Protección a Largo Plazo.

Para la criptografía post-cuántica, se investigarán algoritmos resistentes a computación cuántica, como los basados en lattices, para proteger datos de pH almacenados en plataformas en la nube (Sección 2.3.3.3 Infraestructura de Almacenamiento y Procesamiento). Un caso representativo sería implementar esquemas de cifrado Post-Cuántico en bases de datos, asegurando la confidencialidad a largo plazo frente a amenazas cuánticas, con una tasa de error de cifrado inferior al 0.01%. También se explorarán técnicas de transición gradual desde algoritmos actuales, como AES-256, mediante estrategias de criptografía híbrida, minimizando interrupciones operativas. Estas soluciones usarán Vault by HashiCorp para gestionar claves criptográficas de manera segura, asegurando una trazabilidad del 100%.

14.4.1.3 Seguridad en Edge Computing para Entornos Remotos.

Para la seguridad en Edge Computing, se investigarán controles para sensores IoT que procesan datos de turbidez en el borde (Sección 2.3.3.1). Una posible aplicación sería implementar sistemas de autenticación ligera basados en claves simétricas para validar dispositivos en redes satelitales (Sección 2.3.3.2 Infraestructura de Transmisión y Comunicaciones), complementados con detección de anomalías en el borde para identificar manipulaciones físicas o lógicas, con una tasa de detección del 95%. Estas soluciones reducirán la dependencia de la conectividad en entornos remotos, usando Apache NiFi para procesar datos localmente antes de la transmisión, con un consumo energético inferior al 5%.

14.4.1.4 Blockchain para Integridad y Trazabilidad.

Para el blockchain, se investigarán soluciones para garantizar la integridad y trazabilidad de datos de calidad del aire compartidos en plataformas colaborativas (Sección 2.3.3.3). Un caso representativo sería implementar cadenas de bloques privadas para registrar transacciones de datos, asegurando que no se alteren durante la compartición, con una tasa de integridad del 100%.

También se explorarán contratos inteligentes para automatizar permisos de acceso, considerados prácticas emergentes alineadas con el Control 5.12 "Clasificación de la Información" de ISO/IEC 27002:2022, pero no controles normativos explícitos. Estas soluciones se integrarán con Apache NiFi para gestionar flujos de datos trazables.

14.4.1.5 Validación mediante Pilotos.

La investigación incluirá pilotos en entornos simulados, como proyectos de monitoreo, para validar la viabilidad de estas tecnologías mediante métricas como el tiempo medio de detección de amenazas (objetivo: <10 segundos) y la tasa de registros inalterados en Blockchain (objetivo: 100%). También se desarrollarán guías de integración, detallando configuraciones, requisitos de infraestructura, y procedimientos de auditoría, alineadas con la Sección 9.3 Plan Detallado de Implementación Conceptual, incluyendo configuraciones recomendadas para Apache NiFi, Vault by HashiCorp, y MITRE ATT&CK for ICS para escenarios de monitoreo.

Justificación: La evolución del panorama de amenazas (Sección 1.1 Planteamiento del Problema) y la necesidad de protección a largo plazo (Sección 12.2 Sostenibilidad Tecnológica y Adaptación a la Obsolescencia) requieren innovación para abordar amenazas sofisticadas, como ataques de Re-Identificación (Tabla 8, Sección 5.3.1). Es importante señalar que la Sección 6.2.2 Diseño de Controles Técnicos Aplicables, identifica limitaciones en la detección avanzada, justificando esta investigación. Esta propuesta se fundamenta en el Control 5.12 "Clasificación de la Información" y el Control 5.17 "Información de Autenticación" de ISO/IEC 27002:2022, así como en el Control SI-4 " Monitoreo del sistema" de NIST SP 800-53 Rev. 5, que orienta el diseño de capacidades de monitoreo continuo para detectar anomalías y accesos no autorizados.

Propuesta:

- Desarrollar algoritmos de ML para SIEM, validados en pilotos de monitoreo de, usando Apache NiFi, conforme a la Sección 9.4.
- Implementar criptografía Post-Cuántica para datos de pH, con Vault by HashiCorp, alineada con la Sección 6.2.2.
- Diseñar controles de Edge Computing para sensores de turbidez, conforme a la Sección 6.2.3.

- Desarrollar Blockchain para datos de calidad del aire, como práctica emergente, alineado con la Sección 6.2.5.
- Ejecutar pilotos en entornos simulados, conforme a la Sección 9.3.
- Documentar resultados en un informe técnico para informar la fase "Hacer" (Sección 6 Fase Hacer (Do)).

Resultados Esperados: Incremento del 35 % en la capacidad de detección de amenazas, reflejado en una reducción del tiempo medio de identificación de anomalías de 30 a 20 segundos. Mejora del 20 % en la trazabilidad de los datos, medida por una tasa de registros inalterados del 100 %. Estas métricas corresponden a los indicadores definidos en la Sección 9.4 Ejecución del Plan de Validación Empírica. Se prevé que los prototipos desarrollados retroalimenten la fase "Verificar" (Sección 7 "Fase Verificar (Check)"), contribuyendo al refuerzo de la seguridad en el manejo de datos.

14.4.2 *Fortalecimiento de las Capacidades de Ciberinteligencia, Caza de Amenazas (Threat Hunting) y Ciberresiliencia Proactiva*

14.4.2.1 Ciberinteligencia para Amenazas Específicas.

Esta línea propone desarrollar capacidades para la recolección y análisis de inteligencia de amenazas, la búsqueda proactiva de adversarios (threat hunting), y estrategias de Ciberresiliencia que permitan una rápida recuperación ante incidentes. Para la Ciberinteligencia, se investigarán sistemas de recolección de datos sobre amenazas específicas, como intentos de manipulación de datos de pH en sensores IoT (Sección 2.3.3.1 Infraestructura de Captura y Adquisición de Datos). Una posible aplicación sería implementar plataformas de inteligencia de amenazas que agreguen datos de fuentes externas, como bases de Ciberamenazas de MITRE ATT&CK for ICS, y logs internos, generando perfiles de riesgo para nodos de sensores con una precisión del 90%. Estas plataformas usarán Apache NiFi para procesar y correlacionar datos en tiempo real, asegurando un tiempo de correlación inferior a 5 segundos.

14.4.2.2 Búsqueda Proactiva de Amenazas.

Para el threat hunting, se investigarán equipos especializados que analicen logs de SIEM para identificar adversarios en sistemas que procesan datos de calidad del aire (Sección 2.3.3.3). Un caso representativo sería implementar técnicas de búsqueda proactiva basadas en análisis de comportamiento, detectando patrones anómalos, como accesos repetidos desde direcciones IP desconocidas, con una tasa de detección del 95%. Estos equipos usarán herramientas de análisis forense, integradas con MITRE ATT&CK for ICS, para investigar incidentes, asegurando trazabilidad de las acciones realizadas con una cobertura del 100%. También se explorarán simulaciones de ataques, como intentos de manipulación de datos, para entrenar a los equipos en escenarios realistas, logrando una preparación del 90%.

14.4.2.3 Estrategias de Ciberresiliencia.

Para la ciberresiliencia, se investigarán planes de recuperación ante desastres para sistemas OT de monitoreo (Sección 2.3.3.1). Una posible aplicación sería implementar copias de seguridad cifradas en la nube y protocolos de restauración rápida, con un tiempo objetivo de recuperación de 4 horas, para garantizar la disponibilidad tras interrupciones, como fallos en redes satelitales (Sección 2.3.3.2). Estas soluciones se complementarán con planes de continuidad, alineados con el Control 5.29 "Seguridad de la información durante la interrupción" de ISO/IEC 27002:2022, asegurando operaciones ininterrumpidas en entornos remotos con una tasa de éxito del 95%. También se explorarán simulaciones de incidentes, como ataques de Ransomware, para probar la resiliencia de los sistemas, optimizando los tiempos de recuperación a menos de 4 horas.

14.4.2.4 Validación y Guías Operativas.

La investigación incluirá pruebas en entornos simulados de monitoreo, validando la efectividad de las capacidades de ciberinteligencia y resiliencia mediante métricas como el tiempo medio de detección (objetivo: <15 segundos) y la tasa de éxito de recuperación (objetivo: >95%). También se desarrollarán guías operativas para equipos de threat hunting y planes de recuperación, detallando procedimientos, herramientas recomendadas (como MITRE ATT&CK for ICS), y métricas de desempeño, alineadas con la Sección 9.3 Plan Detallado de Implementación Conceptual.

Justificación: La sofisticación de las amenazas (Sección 1.1 Planteamiento del Problema) y los riesgos de interrupción (Tabla 8, Sección 5.3.1) requieren un enfoque proactivo. Es importante mencionar que la Sección 6.5 Mecanismos de Respuesta a Incidentes de Seguridad identifica limitaciones en la respuesta a incidentes complejos, justificando esta investigación. Este trabajo se basa en el Control SI-5 "Alertas de Seguridad", la Sección 7.2.1 "Identificar y describir los riesgos de seguridad de la información" de ISO/IEC 27005:2022, y Módulo 7: Las Prácticas de ITIL "La Práctica Gestión de Incidentes" de ITIL 4.

Propuesta:

- Implementar plataformas de ciberinteligencia para datos de pH, usando Apache NiFi y MITRE ATT&CK for ICS, alineadas con la Sección 6.2.2.
- Desarrollar equipos de threat hunting para datos de calidad del aire, con herramientas forenses, conforme a la Sección 6.5.
- Diseñar planes de recuperación para sistemas OT, con copias cifradas, alineados con la Sección 6.5.
- Ejecutar simulaciones de incidentes, conforme a la Sección 9.4.
- Desarrollar guías operativas, alineadas con la Sección 9.3.
- Documentar resultados en un informe técnico para informar la fase "Verificar" (Sección 7 Fase Verificar (Check)).

Resultados Esperados: Reducción del tiempo medio de respuesta a incidentes en un 50% (de 30 a 15 minutos) y una tasa de éxito de recuperación del 95%, según métricas de la Sección 6.5 Mecanismos de Respuesta a Incidentes de Seguridad. Se espera que las capacidades proactivas retroalimenten la fase "Verificar" (Sección 7 Fase Verificar (Check)), fortaleciendo la resiliencia operativa.

14.5 Línea Estratégica 4 (LE4): Evolución del Marco de Gestión y Medición del Desempeño del Modelo

Objetivo: Asegurar que el modelo y su gestión evolucionen, se midan eficazmente y se alineen con los objetivos estratégicos de la organización, alineándose con la fase "Actuar" (Sección 8 Fase Actuar (Act)).

14.5.1 *Perfeccionamiento Continuo del Ciclo PHVA Aplicado al Modelo: Métricas y Mecanismos de Retroalimentación*

14.5.1.1 Diseño de KPIs y KRIs.

Esta línea propone revisar y mejorar los Indicadores Clave de Desempeño (KPIs), Indicadores Clave de Riesgo (KRIs), y métricas de efectividad de los controles, estableciendo mecanismos robustos de retroalimentación continua desde la fase "Verificar" (Sección 7 Fase Verificar (Check)) hacia la fase "Planificar" (Sección 5 Caracterización, Análisis de Riesgos y Bases del Diseño). Para los KPIs, se investigarán métricas específicas, como el tiempo medio de detección de anomalías en datos de calidad del aire procesados en plataformas en la nube (Sección 2.3.3.3 Infraestructura de Almacenamiento y Procesamiento), con un objetivo de <10 segundos. Para los KRIs, se investigarán indicadores como la tasa de accesos no autorizados a datos de pH en sensores IoT (Sección 2.3.3.1 Infraestructura de Captura y Adquisición de Datos), con un objetivo de <0.5% mensual. Estas métricas se integrarán en un cuadro de mando interactivo, desarrollado con Apache NiFi para procesar datos en tiempo real, permitiendo a los administradores visualizar tendencias de desempeño y riesgos con una latencia inferior a 1 segundo.

14.5.1.2 Mecanismos de Retroalimentación Automatizada.

La investigación optimizará mecanismos de retroalimentación mediante encuestas de satisfacción dirigidas a actores Multi-Actor (Sección 10.4 Mecanismos de Retroalimentación), evaluando la usabilidad de los controles y la efectividad de las capacitaciones (Sección 10.3 Estrategia de Capacitación). Un caso representativo sería recopilar opiniones de ONGs sobre la claridad de los reportes de auditoría, ajustando formatos para entornos de baja madurez tecnológica mediante plantillas simplificadas, logrando una adopción del 80%. También se investigarán

sistemas de retroalimentación automatizada, como alertas generadas por el SIEM que notifiquen desviaciones en los KPIs (por ejemplo, tiempos de detección superiores a 10 segundos), integradas con plataformas de gestión de incidentes para agilizar la respuesta en menos de 5 minutos, usando Apache NiFi para procesar alertas.

14.5.1.3 Validación y Guías de Implementación.

La investigación incluirá pruebas en entornos simulados de monitoreo de dióxido de carbono, validando la precisión de los KPIs y KRIs mediante métricas como la tasa de falsos positivos (objetivo: <2%) y la satisfacción de los actores (objetivo: >85%). También se desarrollarán guías para la implementación de mecanismos de retroalimentación, detallando procesos de recolección, análisis, y aplicación de datos, alineadas con la Sección 9.3 Plan de Implementación. Estas guías incluirán configuraciones recomendadas para Apache NiFi, plantillas para encuestas de satisfacción, y procedimientos para integrar alertas SIEM con plataformas de gestión de incidentes.

Justificación: La necesidad de mejora continua basada en evidencia (Sección 8.6 Proceso de Mejora Continua) y la falta de automatización en la medición del desempeño (Sección 7.4 Cumplimiento Normativo) justifican esta investigación. Es importante señalar que la Sección 1.3.2 Limitaciones del Diseño Propuesto, indica la necesidad de métricas más precisas para demostrar el valor del modelo. Este trabajo se basa en la Cláusula 9.1 " Seguimiento, medición, análisis y evaluación" de ISO/IEC 27001:2022, el PM-6 "Medidas de Rendimiento" de NIST SP 800-53 Rev. 5, y la Sección 5.7.2 "Mejora Continua" de ISO 31000:2018.

Propuesta:

- Diseñar KPIs y KRIs para datos de calidad del aire y pH, integrados en un cuadro de mando con Apache NiFi, alineados con la Sección 7.2 Evaluación de la Eficacia del Modelo.
- Implementar encuestas de satisfacción para actores, con plantillas simplificadas, conforme a la Sección 10.4 Mecanismos de Participación y Retroalimentación Continua.

- Desarrollar sistemas de retroalimentación automatizada en el SIEM, usando Apache NiFi, alineados con la Sección 6.2.2 Diseño de Controles Técnicos Aplicables.
- Ejecutar pruebas en entornos simulados de monitoreo, conforme a la Sección 9.4 Plan Detallado de Validación Empírica.
- Desarrollar guías de retroalimentación, alineadas con la Sección 9.3 Plan Detallado de Implementación Conceptual.
- Documentar resultados en un informe técnico para informar la fase "Planificar" (Sección 5 Caracterización, Análisis de Riesgos y Bases del Diseño).

Resultados Esperados: Incremento del 30 % en la precisión de las métricas, evidenciado por la disminución de falsos positivos del 5 % al 2 %, junto con un nivel de satisfacción del 85 % entre los actores involucrados. Estos resultados se basan en las métricas definidas en la Sección 9.4 "Ejecución del Plan de Validación Empírica". Se prevé una retroalimentación estructurada que alimente la fase "Hacer" (Sección 6 "Fase Hacer (Do)"), contribuyendo a una mayor eficacia operativa del modelo.

14.5.2 *Desarrollo de un Marco de Madurez y Hoja de Ruta para la Evolución Futura del Modelo de Seguridad (hacia V2.X, V3.X)*

14.5.2.1 Marco Conceptual de Madurez.

Esta línea propone desarrollar un marco de madurez específico para evaluar el estado actual del modelo y planificar su evolución a medio y largo plazo, estableciendo las bases para versiones futuras (V2.X, V3.X). El marco incluirá cuatro niveles de madurez (inicial, gestionado, definido, optimizado) basados en cinco dominios: adopción de controles, gobernanza, sostenibilidad económica, sostenibilidad tecnológica (Sección 12 Estrategia para la Sostenibilidad a Largo Plazo del Modelo de Seguridad), y capacidad de integración interinstitucional y nivel de automatización de la medición, alineados con la Interoperabilidad de TOGAF Ver 10 y el PM-6 "Medidas de Rendimiento" de NIST SP 800-53 Rev. 5.

- Adopción de Controles: Evalúa la implementación de controles técnicos y organizacionales (Sección 6.2 Selección y Diseño Detallado de Controles de Seguridad), con un objetivo de >80% en el nivel definido.
- Gobernanza: Mide la efectividad de comités Multi-Actor (Sección 10.2 Roles y Responsabilidades en la Gobernanza e Implementación), con un objetivo de participación del 90%.
- Sostenibilidad Económica: Evalúa la financiación compartida (Sección 12.3 Sostenibilidad Económica y de Recursos a Largo Plazo), con un objetivo de >70% de recursos asegurados.
- Sostenibilidad Tecnológica: Mide la adopción de tecnologías emergentes (Sección 12.2 ostenibilidad Económica y de Recursos a Largo Plazo), con un objetivo de >60% de integración.
- Capacidad de Integración Interinstitucional: Evalúa la interoperabilidad con instituciones colaboradoras, con un objetivo de >90% de autenticaciones federadas exitosas.
- Nivel de Automatización de la Medición: Mide la proporción de métricas automatizadas, como el tiempo medio de detección de anomalías (<10 segundos), con un objetivo de >70%.

14.5.2.2 Métricas de Evaluación.

La investigación diseñará métricas cuantitativas, como el porcentaje de controles implementados (objetivo: >80%) y la tasa de interoperabilidad interinstitucional (objetivo: >90%), y cualitativas, como la satisfacción de actores (objetivo: >85%), integradas en un cuadro de mando interactivo con Apache NiFi para procesar datos en tiempo real. Por ejemplo, la capacidad de integración se medirá por la tasa de éxito de autenticaciones SAML 2.0, mientras que la automatización evaluará la proporción de KPIs generados automáticamente.

14.5.2.3 Hoja de Ruta para V2.X y V3.X.

La investigación desarrollará hojas de ruta para V2.X (2027) y V3.X (2030), detalladas en una tabla de evolución:

VERSIÓN	HITO TECNOLÓGICO	HITO DE GOBERNANZA	HITO ECONÓMICO
ACTUAL (V1.96A)	Controles RBAC, SIEM	Comités Multi-Actor iniciales	Financiación inicial
V2.X (2027)	*Edge computing* para sensores de calidad del aire, blockchain	Comités permanentes, retroalimentación automatizada	Financiación compartida (>70%)
V3.X (2030)	Criptografía post-cuántica, IA para *threat hunting*	Gobernanza automatizada, análisis predictivo	Fondo permanente (>90%)

V2.X priorizará sistemas de Edge Computing para sensores de calidad del aire (Sección 2.3.3.1) y Blockchain para trazabilidad, mientras que V3.X integrará criptografía Post-Cuántica para datos geoespaciales (Sección 2.3.3.3) y gobernanza automatizada con análisis predictivo, alineados con la Sección 6.2.2 "Diseño de Controles Técnicos Aplicables".

14.5.2.4 Validación y Guías de Evaluación.

La investigación incluirá pruebas en entornos simulados de monitoreo de pH, validando la aplicabilidad del marco de madurez mediante métricas como la tasa de adopción de controles (objetivo: >80%) y la satisfacción de actores (objetivo: >85%). También se desarrollarán guías para evaluar la madurez, detallando procedimientos, herramientas recomendadas (como Apache NiFi), y métricas de desempeño, alineadas con la Sección 9.3 Plan Detallado de Implementación Conceptual. Estas guías incluirán plantillas para auditorías de madurez y tableros de visualización de métricas, asegurando una usabilidad del 90%.

Justificación: La sostenibilidad a largo plazo (Sección 12.6 Estrategia Integrada para la Sostenibilidad del Modelo) y la escalabilidad del modelo (Sección 1.3.2 Limitaciones del Diseño Propuesto) requieren una visión estructurada para su evolución. Es oportuno mencionar que la Sección 6 indica la necesidad de escalabilidad, justificando esta investigación. Este trabajo se basa en la Sección 5.7.2 "Mejora Continua" de ISO 31000:2018, el proceso DSS05 " Gestionar los servicios de seguridad " de COBIT 2019, y la Cláusula 4.1 "Entender la Organización y su Contexto" de ISO/IEC 27001:2022.

Propuesta:

- Diseñar un marco de madurez con métricas para cinco dominios, usando Apache NiFi, alineado con la Sección 9.4 Ejecución del Plan de Validación Empírica.
- Desarrollar hojas de ruta para V2.X (2027) y V3.X (2030), priorizando edge computing y criptografía post-cuántica, conforme a la Sección 12.2.
- Ejecutar pruebas en entornos simulados de monitoreo de pH, conforme a la Sección 9.4.
- Desarrollar guías de evaluación de madurez, con plantillas y tableros, alineadas con la Sección 9.3.
- Documentar resultados en un informe técnico para informar la fase "Planificar" (Sección 5 Caracterización, Análisis de Riesgos y Bases del Diseño).

Resultados Esperados*:* Disponibilidad de un marco de madurez operativo con una adopción efectiva del 80% de los controles diseñados, interoperabilidad interinstitucional superior al 90% y un nivel de satisfacción de actores clave del 85%, conforme a los indicadores definidos en la Sección 9.4 Plan Detallado de Validación Empírica. Se proyecta la consolidación de una hoja de ruta hacia el año 2030, que alimente de manera estructurada la fase "Verificar" (Sección 7 Fase Verificar (Check)), garantizando la evolución sostenida del modelo de seguridad.

Capítulo 15: Conclusiones y Recomendaciones Finales

Con base en las contribuciones técnicas, operativas, éticas, y estratégicas delineadas en la Sección 13, que posicionan el modelo de seguridad como un referente para la investigación medioambiental distribuida, esta sección consolida los resultados del ciclo PHVA (Secciones 5-8), la planificación de implementación (Sección 9), la participación Multi-Actor (Sección 10), las consideraciones éticas, legales y sociales (Sección 11), la sostenibilidad a largo plazo (Sección 12), y las contribuciones al campo (Sección 13). El modelo, documentado en la Tabla 11 "Resumen de Políticas y Procedimientos Diseñados", protege los activos críticos de la Tabla 6 "Identificación y Clasificación de Activos" de la Sección 5.2.5, mitiga los riesgos de las Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3, y responde a los desafíos operativos de la Sección 1.1 "Planteamiento del Problema" y al contexto Multi-Actor de la Sección 3.2 "Características Particulares de los Proyectos Medioambientales". Este análisis se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022, el MEA03 “Gestionar el cumplimiento de los requisitos externos” de COBIT 2019, y el PM-6 "Medidas de rendimiento de seguridad de la información" de NIST SP 800-53 Rev. 5. Las subsecciones 14.1 a 14.4 sintetizan los logros, evalúan el cumplimiento de los objetivos, identifican limitaciones y lecciones aprendidas, y proponen recomendaciones para la implementación y mejora futura, asegurando un cierre integral alineado con los objetivos de la Sección 1.4 "Objetivos".

15.1 Logros del Diseño y Planificación del Modelo de Seguridad

Esta subsección sintetiza los principales logros alcanzados a lo largo del ciclo PHVA (Secciones 5-8) y las secciones adicionales (9-13), destacando los resultados clave que aseguran la robustez, adecuación, y sostenibilidad del modelo de seguridad. El diseño se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el MEA03 “Gestionar el cumplimiento de los requisitos externos" de COBIT 2019, que orientan la consolidación de resultados.

En la fase Planificar (Sección 5), se identificaron y priorizaron requisitos de seguridad (Sección 5.4.1), riesgos (Tablas 7 y 8 de las Secciones 5.3.1 y 5.3.3), y activos críticos (Tabla 6 de la Sección 5.2.5), estableciendo un marco robusto que responde a los desafíos operativos de la

Sección 1.1, como la baja conectividad en entornos remotos. Este enfoque aseguró una planificación alineada con el contexto Multi-Actor (Sección 3.2).

La fase Hacer (Sección 6) diseñó un modelo integral (Sección 6.6), incluyendo políticas de seguridad (Sección 6.1.1), controles técnicos, organizacionales, y físicos (Secciones 6.2.2-6.2.4), una arquitectura lógica (Sección 6.4.1), y mecanismos de respuesta a incidentes (Sección 6.5). Por ejemplo, el cifrado AES-256 (Sección 6.2.2) protege datos climáticos y geoespaciales (Sección 3.1), mientras que el protocolo de notificación (Sección 6.5) optimiza la respuesta a incidentes, mitigando riesgos de intercepción y descoordinación (Tabla 8).

La fase Verificar (Sección 7) confirmó un 90% de conformidad normativa (Sección 7.4), evaluó la eficacia de los controles (Sección 7.2), e identificó brechas (Sección 7.3), como la necesidad de guías simplificadas para ONGs, abordadas en la fase siguiente. La fase Actuar (Sección 8) implementó ajustes, como la optimización del protocolo de notificación con canales SMS (Sección 8.4), actualizó la documentación (Sección 8.5), y diseñó un proceso de mejora continua (Sección 8.6), asegurando adaptabilidad.

Las secciones adicionales enriquecieron el modelo:

- Planificación de implementación (Sección 9): Diseñó un piloto con pruebas empíricas (Sección 9.4), validando métricas como tiempos de notificación de 24 horas.
- Participación Multi-Actor (Sección 10): Estableció roles (Sección 10.2) y mecanismos de retroalimentación (Sección 10.4), promoviendo colaboración.
- Consideraciones ELSI (Sección 11): Integró privacidad por diseño y consentimiento comunitario (Sección 11.2), asegurando responsabilidad ética.
- Sostenibilidad (Sección 12): Diseñó una estrategia integrada (Sección 12.6) con Indicadores Clave de Sostenibilidad (IKS).
- Contribuciones (Sección 13): Posicionó el modelo como un referente técnico, operativo, ético, y estratégico.

Estos logros, documentados en la Tabla 11, preparan la evaluación de objetivos en la Sección 14.2, contribuyendo a los objetivos de la Sección 1.4.

Por lo tanto, los logros consolidan un modelo robusto y sostenible, listo para su implementación. Recomendaciones para la Implementación y Mejora Futura

Las limitaciones y lecciones de la Sección 14.3 informan las recomendaciones para la implementación y mejora futura del modelo, asegurando su efectividad en el contexto medioambiental. Este análisis se fundamenta en el 10.1 "Mejora continua" de ISO/IEC 27001:2022 y en el DSS05 "Gestionar los servicios de seguridad" de COBIT 2019, que orientan la planificación estratégica.

Para la implementación:

- Expandir el piloto (Sección 9.3) a nuevas regiones, priorizando zonas con infraestructura similar (por ejemplo, redes, Sección 2.3.3.2), para validar la escalabilidad (Sección 13.4). Por ejemplo, un piloto en una segunda región con ONGs locales probará el protocolo de notificación (Sección 6.5).
- Fortalecer la capacitación Multi-Actor (Sección 10.3) con talleres adicionales para ONGs sobre MFA (Sección 6.2.5) y sesiones offline para comunidades locales, abordando la brecha digital (Sección 11.4).
- Integrar auditorías ELSI (Sección 11.5) en el piloto, evaluando el consentimiento comunitario y el cumplimiento legal transfronterizo, mitigando riesgos éticos y legales (Tabla 8 de la Sección 5.3.1).

Para la mejora futura:

- Desarrollar controles más ligeros: Diseñar notificaciones offline y MFA basado en hardware local para entornos de baja conectividad (Sección 1.1), reduciendo retrasos identificados (Sección 14.3).
- Establecer un fondo permanente: Crear un fondo Multi-Actor para financiar sostenibilidad económica (Sección 12.3), asegurando recursos para actualizaciones tecnológicas (Sección 12.2).
- Fortalecer la gobernanza ética: Implementar un comité ético permanente (Sección 11.5) para monitorear la privacidad y equidad, integrando retroalimentación comunitaria (Sección 10.4).

Estas recomendaciones, vinculadas al proceso de mejora continua (Sección 8.6), se revisarán anualmente mediante los IKS (Sección 12.6), asegurando adaptabilidad. Los resultados se documentarán en la Tabla 11, contribuyendo a los objetivos de la Sección 1.4.

Por lo tanto, las recomendaciones guían una implementación efectiva y mejoras sostenibles, consolidando el impacto del modelo.

15.2 Respuesta a la Pregunta Central de Investigación

En respuesta a la pregunta central sobre cómo estructurar un modelo conceptual de seguridad para proteger, clasificar y gestionar de forma efectiva los activos sensibles en entornos de investigación medioambiental, este trabajo de grado ha logrado su objetivo mediante el diseño de un modelo articulado en tres pilares fundamentales:

- Para la protección efectiva: Se diseñó una arquitectura de defensa en profundidad (Sección 5.2.5) que integra controles técnicos robustos en múltiples capas. Esto incluye la especificación de cifrado avanzado (AES-256) para datos en reposo y en tránsito (Sección 6.2.2) y la conceptualización de un sistema de monitoreo continuo (SIEM) para la detección proactiva de amenazas, garantizando la confidencialidad e integridad de la información crítica.
- Para la clasificación sistemática: Se estableció una metodología formal de identificación y clasificación de activos (Sección 5.2), que permite valorar los recursos en función de su criticidad operativa y sensibilidad (Sección 5.2.4). Este proceso es de suma importancia para la aplicación de controles proporcionales al riesgo, asegurando que los esfuerzos de protección se centren en los activos de mayor valor para la investigación.
- Para la gestión integral y adaptativa: Se definió un marco de gobernanza Multi-Actor (Sección 10.2) que asigna roles y responsabilidades claras a las diversas partes interesadas. Este marco se complementa con procedimientos operativos documentados (Sección 6.1.2) y un plan de respuesta a incidentes (Sección 6.5), que en conjunto aseguran una gestión coordinada, auditable y resiliente, adaptada a la complejidad de los entornos colaborativos.

15.3 Análisis e Interpretación de Resultados en el Contexto Medioambiental

El modelo de gestión de seguridad de la información (MGSI), fundamentado en ISO/IEC 27001:2022 (Cláusula 9.1 "Seguimiento, medición, análisis y evaluación") y MAGERIT v3 (Libro II "Catálogo de elementos"), se interpreta en el contexto de los proyectos de investigación medioambiental para cumplir con los objetivos de la Sección 1.4: garantizar confidencialidad, integridad, disponibilidad, autenticidad, y cumplimiento normativo de datos sensibles. Este análisis, estructurado en tres apartados, aborda los desafíos operativos y Multi-Actor descritos en la Sección 1.1 ("Planteamiento del Problema") y la Sección 3.2 ("Características Particulares de los Proyectos Medioambientales"), demostrando la aplicabilidad del modelo en entornos tecnológicos heterogéneos (Sección 2.3.3).

Interpretación del Análisis de Riesgos

El análisis de riesgos (Tabla 8 "Análisis de Riesgos y Amenazas" de la Sección 5.3.1) prioriza impactos ecológicos y sociales, como la alteración de predicciones hidrológicas o la manipulación de datos geoespaciales, sobre los riesgos financieros típicos de entornos corporativos. Por ejemplo, la exposición de datos procesados por nodos de Edge Computing (dispositivos que procesan datos en campo, Sección 2.3.3.3|) podría comprometer la toma de decisiones en la gestión de recursos hídricos, afectando ecosistemas y comunidades locales (Sección 3.1, página 64). Este enfoque, alineado con ISO/IEC 27005:2018 (Sección 4 "Gestión de riesgos"), reduce el riesgo de intrusión en un 85% mediante controles preventivos (Sección 9.3), asegurando la disponibilidad y autenticidad de los datos (Sección 1.4).

Interpretación del Diseño de Controles

Los controles diseñados (Sección 6.2) responden a la infraestructura tecnológica descrita en la Sección 2.3.3. Por ejemplo, la autenticación multifactor (MFA) en APIs REST/GraphQL (interfaces para intercambio de datos, Sección 2.3.3.5) protege el acceso a bases de datos geoespaciales, garantizando confidencialidad frente a accesos no autorizados (Sección 1.4). Asimismo, los sistemas SIEM (sistemas de gestión de eventos e información de seguridad, Sección 2.3.3.6) detectan anomalías en terminales VSAT (antenas satelitales para comunicaciones remotas, Sección 2.3.3.2) en menos de 10 segundos (Sección 9.3), asegurando integridad y disponibilidad. Estos controles, alineados con 8.24 "Uso de criptografía" de ISO/IEC 27002:2022, mitigan riesgos

específicos de entornos remotos, como la interrupción de comunicaciones satelitales, fortaleciendo la resiliencia operativa.

Interpretación de la Arquitectura y Gobernanza

La arquitectura lógica (Sección 6.4) y la gobernanza Multi-Actor (Sección 10.4) facilitan la colaboración entre universidades, ONGs, y gobiernos (Sección 3.2). Por ejemplo, los protocolos de intercambio seguro en APIs REST/GraphQL (Sección 2.3.3.5) permiten a ONGs acceder a datos procesados por nodos de Edge Computing, manteniendo confidencialidad mediante cifrado (Sección 6.2.2). Los comités Multi-Actor, apoyados por sistemas SIEM, monitorean accesos en tiempo real, reduciendo incidentes de seguridad en un mejor porcentaje (Sección 9.3). Esta estructura, alineada con Cláusula 5.1 "Liderazgo y compromiso" de ISO/IEC 27001:2022, asegura el cumplimiento normativo y la sostenibilidad en entornos colaborativos (Sección 1.4).

El MGSI adapta controles y arquitectura a la infraestructura tecnológica del sector medioambiental (Sección 2.3.3), como nodos de Edge Computing, terminales VSAT, APIs REST/GraphQL, y sistemas SIEM, para mitigar riesgos y cumplir con los objetivos de confidencialidad, integridad, disponibilidad, autenticidad, y cumplimiento normativo (Sección 1.4). Los resultados, respaldados por métricas (reducción de riesgos en un 80-85%, Sección 9.3), consolidan un modelo robusto y adaptable, respondiendo a los desafíos operativos y éticos de los proyectos de investigación medioambiental.

Referencias Bibliográficas

6sigma.us. (2024, 18. abril). *Multi-criteria decision analysis (MCDA): All you need to know*. https://www.6sigma.us/six-sigma-in-focus/multi-criteria-decision-analysis-mcda/

Abdullah Khan, Hamza Ali, Maham Jadoon, Zain-Ul Abideen, Nasru Minallah & Ijist Jr. (2024). *Combatting Illegal Logging with AI-powered IoT Devices for Forest Monitoring*. https://www.researchgate.net/publication/382398358_Combatting_Illegal_Logging_with_AI-powered_IoT_Devices_for_Forest_Monitoring

Adroit. (2023). *Satellite Connectivity Game Changer for Environmental Monitoring*. https://adroit.nz/satellite-connectivity-for-environmental-monitoring/

Aghaei, E., Al-Shaer, E., Shadid, W. & Niu, X. (2023). *Automated CVE Analysis for Threat Prioritization and Impact Prediction*. https://arxiv.org/abs/2309.03040v1

Alcibiadis, R. & Cartagena, P. (2021). *Propuesta de un ciclo de gestión de riesgos utilizando modelos de amenazas y controles de seguridad ISO/EC 27002 / EGSI / RGPD*. http://bibdigital.epn.edu.ec/handle/15000/21384

Alejandra, J. & Useche, E. (2021). *Estudio documental sobre las firmas electrónicas en los documentos para archivo a partir de la expedición del decreto 2364 de 2012 en Colombia*. https://bibliotecadigital.udea.edu.co/handle/10495/23035

ALI GUMA, Robert Wamusi, Maad M. Mijwil, Malik Sallam, Jenan Ayad Namuq & Ioannis Adamopoulos. (2025. enero). *Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey*. https://www.researchgate.net/publication/388832572_Securing_the_Internet_of_Wetland_Things_IoWT_Using_Machine_and_Deep_Learning_Methods_A_Survey

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H. & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, *9*, 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203

Ankit Dubey, Pradeep Kishore & Infosys BPM. (s. f.). *Geospatial Data Privacy & Security Challenges | Infosys BPM*. Recuperado 13 de abril de 2025, a partir de

https://www.infosysbpm.com/blogs/geospatial-data-services/geospatial-data-privacy-navigating-security-challenges-in-the-digital-age.html

Antonio, M., Torres, B., Del Pilar, M. & Albujar, A. (2024). *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones*. https://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/27284

Antunes, M., Maximiano, M., Gomes, R. & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *Journal of Cybersecurity and Privacy 2021, Vol. 1, Pages 219-238*, *1*(2), 219-238. https://doi.org/10.3390/JCP1020012

Avanidou, K., Alexandridis, T., Kavroudakis, D. & Kizos, T. (2023). Development of a multi scale interactive web-GIS system to monitor farming practices: A case study in Lemnos Island, Greece. *Smart Agricultural Technology*, *5*, 100313. https://doi.org/10.1016/J.ATECH.2023.100313

AXELOS. (2019). *ITIL Foundation, ITIL 4 Edition*. https://www.axelos.com/certifications/itil-service-management , https://worldaedait.com.mx/wp-content/uploads/2019/09/ITIL-4-Foundation-Material-Participante.pdf

Bartolo, B., Azzopardi, B. & Scerri, K. (2025). Development and implementation of a public data repository for photovoltaic systems: Case study malta's living laboratories. *Solar Energy Advances*, *5*, 100100. https://doi.org/10.1016/J.SEJA.2025.100100

Beltrán Hernández, C. R., Colorado Ramírez, L. V. & Salgado Martínez, C. A. (2023). *Evaluación de riesgos de seguridad de la información en TrueSecure S.A. utilizando la metodología MAGERIT y plan de tratamiento de riesgos*. https://hdl.handle.net/20.500.12495/11208

BlackFog. (2025, 29. enero). *AWS Data Breach: Lesson From 4 High Profile Breaches | BlackFog*. https://www.blackfog.com/aws-data-breach/

Brasco, M. A. , & de C. C. A. (2022). *(PDF) Territorial relations between deforestation and Rural Environmental Registry (CAR) in the Amazon biome using free software QGIS/PostgreSQL/PostGIS and Data Warehouse Structure*. https://www.researchgate.net/publication/368411948_Territorial_relations_between_defores

tation_and_Rural_Environmental_Registry_CAR_in_the_Amazon_biome_using_free_software_QGISPostgreSQLPostGIS_and_Data_Warehouse_Structure

BRICEÑO, E. V. (2021). *Seguridad de la información - Edgar Vega Briceño - Google Libros*. https://books.google.es/books?hl=es&lr=&id=nx4uEAAAQBAJ&oi=fnd&pg=PA79&dq=Seguridad+de+la+informaci%C3%B3n,+Brice%C3%B1o,+Edgar+Vega&ots=Ddlah2oKyy&sig=1_bxGui_5JZX4ZoH4U4jHgtTqAc#v=onepage&q=Seguridad%20de%20la%20informaci%C3%B3n%2C%20Brice%C3%B1o%2C%20Edgar%20Vega&f=false

Buitrago Díaz, N. A. & Caho Rodríguez, J. F. (2024). *Propuesta de mejora para la gestión integral de riesgos en una empresa de tecnologías de la información en Bogotá*. Fundación Universidad de América. https://hdl.handle.net/20.500.11839/9595

Cabezas Juárez, I. C. (2020). Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima. *Repositorio Académico USMP*. https://renati.sunedu.gob.pe/handle/sunedu/2847596

Cámara de Comercio Internacional España. (2024). *Protección de la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro*. https://www.iccspain.org/wp-content/uploads/2024/12/2024_IssueBrief3_SPA.pdf

Campos, J. G., Colom, R. J., Cotutor, P., José, F. & Sales, G. (2020). *INTEGRACIÓN Y PROGRAMACIÓN DE SEGURIDAD INTELIGENTE EN REDES IoT*. https://riunet.upv.es/handle/10251/143030

Center for Internet Security. (2021). *CIS Critical Security Controls Version 8*. Center for Internet Security. https://www.cisecurity.org/controls/v8 , PDF en español de CIS Controls v8: https://diplomadociberseguridad.com/wp-content/uploads/2024/06/CIS-Controls-v8-Espanol-2.pdf

CEPAL. (s. f.). *Gestión de datos de investigación*. Recuperado 20 de mayo de 2025, a partir de https://biblioguias.cepal.org/c.php?g=495473&p=4398203

CITES. (2021, 25. noviembre). *Estudio de la CITES: la caza furtiva y el comercio ilegal son una amenaza creciente para los jaguares | CITES*. https://cites.org/esp/CITES_study_illegal_trade_poaching_jaguar_pantheraonca_2112021

Clinton Boyda & D4H. (2022). *Efectos del cambio climático en la gestión de emergencias*. https://www.d4h.com/es/blog/climate-change-effects-on-emergency-management

Cole, E., Deneu, B., Lorieul, T., Servajean, M., Botella, C., Morris, D., Jojic, N., Bonnet, P. & Joly, A. (2020). *The GeoLifeCLEF 2020 Dataset*.

coordinación de contenidos, E., General de Modernización Administrativa, D. & Impulso de la Administración Electrónica, P. (20212). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas*. https://www.hacienda.gob.es/SGT/CATALOGO_SEFP/048_Magerit_v3_libro3.pdf

dc, B., DIOCEAN Boletín CTN, colombia & Vicealmirante John Fabio Giraldo Gallo Director General Marítimo, D. (2024). *Boletín CTN Diocean No. 3 / 2023*. https://aquadocs.org/handle/1834/43071

De Originalidad, I. & Primarias, F. (2024). Implementación de Soluciones TI que brinden la alta disponibilidad y respaldo de la información de la Empresa Integrit Sac. *Universidad Inca Garcilaso de la Vega*. http://repositorio.uigv.edu.pe/handle/20.500.11818/7784

Dormido, L., Garrido, I., L'Hotellerie-Fallois, P. & Santillán Fraile, J. (2022). *El cambio climático y la sostenibilidad del crecimiento: iniciativas internacionales y políticas europeas*. https://repositorio.bde.es/handle/123456789/22528

Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, *2023*(2), 29-35. https://doi.org/10.5923/j.scit.20231302.04

EarthSoft. (s. f.). *Página de inicio de EarthSoft - EarthSoft, Inc. Software de gestión de datos ambientales*. Recuperado 2 de abril de 2025, a partir de https://earthsoft.com/

Enemosah, A. & Ifeanyi, O. G. (2024). Cloud security frameworks for protecting IoT devices and SCADA systems in automated environments. *https://wjarr.com/sites/default/files/WJARR-2024-1485.pdf*, *22*(3), 2232-2252. https://doi.org/10.30574/WJARR.2024.22.3.1485

Epa, U. & Quality Management Division, E. (2002). Guidance on Environmental Data Verification and Data Validation. *EPA QA/G-8*. www.epa.gov/quality

Escobar Quintana, M. A. & Alarcón Pérez, R. O. (2023). *Desarrollo de un sistema web y un módulo de seguridad basado en la norma ISO 27000, para mitigar y controlar la integridad de la información.* http://dspace.espoch.edu.ec/handle/123456789/20158

Farias Estacio, A. G. & Centeno Córdova, D. J. (2024). *Modelos de Inteligencia Artificial para prevención de ataques cibernéticos en organizaciones*. http://dspace.ups.edu.ec/handle/123456789/27884

Finck, M. & Mueller, M. S. (2023). Access to Data for Environmental Purposes: Setting the Scene and Evaluating Recent Changes in EU Data Law. *Journal of Environmental Law*, *35*(1), 109-131. https://doi.org/10.1093/JEL/EQAD006

Freepik. (s. f.). *Imágenes vectoriales utilizadas en el documento | Freepik*. Recuperado 24 de mayo de 2025, a partir de https://www.freepik.com

Gamboa, G. I. M. & Pulido, S. C. A. (2024). *Propuesta, de una Oficina, de Gestión de Proyectos Científicos para el Proceso M11 – Investigación Científica Marina de la Subdirección de Desarrollo Marítimo*. Universidad EAN Facultad de Ingeniería Maestría en Gerencia de Proyectos .

Gordon, S. N., Murphy, P. J., Gallo, J. A., Huber, P., Hollander, A., Edwards, A. & Jankowski, P. (2021). People, Projects, Organizations, and Products: Designing a Knowledge Graph to Support Multi-Stakeholder Environmental Planning and Design. *ISPRS International Journal of Geo-Information*, *10*(12), 823. https://doi.org/10.3390/IJGI10120823/S1

Graña, M., Yang, Y., Meng, Q., Lorenzo, D., Aschieri, D., Sobrino, N. & Macii, E. (2024). Web-GIS Application for Hydrogeological Risk Prevention: The Case Study of Cervo Valley. *Sustainability 2024, Vol. 16, Page 9833*, *16*(22), 9833. https://doi.org/10.3390/SU16229833

Ignitec. (2025). *Case Study: Environmental Monitoring Technology*. https://www.ignitec.com/insights/case-study-environmental-monitoring-technology/

Information Systems Audit and Control Association (ISACA). (2018). *COBIT 2019 Framework: Governance & Management Objectives | Digital | Spanish - ISACA Portal*. ISACA (Information Systems Audit and Control Association). https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko99EAC

International Organization for Standardization; International Electrotechnical Commission. (2018). *ISO 55002:2018(es), Gestión de activos — Sistemas de gestión — Directrices para la aplicación de la ISO 55001*. ISO. https://www.iso.org/obp/ui/en/#iso:std:iso:55002:ed-2:v2:es

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 - Information security management systems*. ISO. https://www.iso.org/standard/27001

International Organization for Standardization; International Electrotechnical Commission. (2022a). *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls*. ISO. https://www.iso.org/standard/75652.html

International Organization for Standardization; International Electrotechnical Commission. (2022b). *ISO/IEC 27005:2022 - Guidance on managing information security risks*. ISO. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27005:ed-4:v1:en

International Organization for Standardization; International Electrotechnical Commission. (2024). *ISO/IEC 38500:2024(en), Information technology — Governance of IT for the organization*. ISO. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:38500:ed-3:v1:en

Ipiniza, R., Barros, S., De la Maza, C. L., Jofré, P. & González, J. (2021). Bosques y Biodiversidad. *Ciencia & Investigación Forestal*, *27*(1), 101-132. https://doi.org/10.52904/0718-4646.2021.475

IXON. (2018). *Environmental Service Went from Using 20 VPN Tools to one Standard Solution (Case Study)*. https://thewaternetwork.com/article-FfV/environmental-service-went-from-using-20-vpn-tools-to-one-standard-solution-case-study-hLjpsi3JeNZr3z8KhfWIJA

Karina Gutiérrez-Camacho, M. & Magdalena Contreras-Mendoza, P. (2021). Importancia de la atención política y social para la conservación de la biodiversidad en comunidades inclusivas, resilientes y sostenibles en México. *Ra Ximhai*, *17*, 191. https://doi.org/10.35197/RX.17.03.2021.08.MG

Khoda Parast, F., Sindhav, C., Nikam, S., Izadi Yekta, H., Kent, K. B. & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580. https://doi.org/10.1016/J.COSE.2021.102580

Kim, B. & Henke, G. (2021). Easy-to-Use Cloud Computing for Teaching Data Science. *Journal of Statistics and Data Science Education*, *29*(S1), S103-S111. https://doi.org/10.1080/10691898.2020.1860726

Kim, J., Lee, C. & Chang, H. (2020). The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth. *Sustainability 2020, Vol. 12, Page 10639*, *12*(24), 10639. https://doi.org/10.3390/SU122410639

Kostromin, R., Basharina, O., Feoktistov, A. & Sidorov, I. (2021). Microservice-Based Approach to Simulating Environmentally Friendly Equipment of Infrastructure Objects Taking into Account Meteorological Data. *Atmosphere 2021, Vol. 12, Page 1217*, *12*(9), 1217. https://doi.org/10.3390/ATMOS12091217

Krishnamurthy, S. , K. S. H. , K. A. , G. O. , A. R. , & J. S. (2020). *APPLICATION OF DOCKER AND KUBERNETES IN LARGE-SCALE CLOUD ENVIRONMENTS*. International Research Journal of Modernization in Engineering Technology and Science,. https://www.researchgate.net/publication/387212960_APPLICATION_OF_DOCKER_AND_KUBERNETES_IN_LARGE-SCALE_CLOUD_ENVIRONMENTS

Kuhn Cuellar, L., Friedrich, A., Gabernet, G., de la Garza, L., Fillinger, S., Seyboldt, A., Koch, T., zur Oven-Krockhaus, S., Wanke, F., Richter, S., Thaiss, W. M., Horger, M., Malek, N., Harter, K., Bitzer, M. & Nahnsen, S. (2022). A data management infrastructure for the integration of imaging and omics data in life sciences. *BMC Bioinformatics*, *23*(1), 1-20. https://doi.org/10.1186/S12859-022-04584-3/FIGURES/6

Landoll, D. J. (2005). The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 1-475. https://doi.org/10.1201/9781003090441/SECURITY-RISK-ASSESSMENT-HANDBOOK-DOUGLAS-LANDOLL

Lanegra, I. (s. f.). *Política ambiental y del cambio climático 4.2*.

Layode, O., Nwapali Ndidi Naiho, H., Sheriff Adeleke, G., Onyekachukwu Udeh, E., Temitope Labake, T., Author, C. & Layode Corresponding Author, O. (2024). Data privacy and security challenges in environmental research: Approaches to safeguarding sensitive information. *International Journal of Applied Research in Social Sciences*, *6*(6), 1193-1214. https://doi.org/10.51594/IJARSS.V6I6.1210

Lema Sánchez, Fernanda Mariam & Marbellyn Fernanda Valverde Santos. (2023). *Metodología para estimar riesgos naturales que consideren factores sociales, económicos y ambientales en una zona geográfica.* https://dspace.ueb.edu.ec/handle/123456789/6510

Li, C. & Huang, M. (2023). Environmental Sustainability in the Age of Big Data: Opportunities and Challenges for Business and Industry. *Environmental science and pollution research international*, *30*(56), 119001-119015. https://doi.org/10.1007/S11356-023-30301-5/METRICS

Lopes, P. F. M., Constantinescu, Ş., Silvano, R. A. M., Tatui, F., Teampău, P. & Vaidianu, N. (2025). Unintended and overlooked consequences of exclusionary marine conservation. *ICES Journal of Marine Science*, *82*(1), 190. https://doi.org/10.1093/ICESJMS/FSAE190

Luna-López, M., Hernández-Lozano, M., Aldana-Franco, R., Álvarez-Sánchez, E., Leyva-Retureta, J. G., Ricaño-Herrera, F. & Aldana-Franco, F. (2021). Sistema inteligente de monitoreo para condiciones ambientales en Industria 4.0. *Científica*, *25*(2), 1-10. https://doi.org/10.46842//IPN.CIEN.V25N2A07

Mafla Flores, S. M. (2024). *Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A.* https://repositorio.utn.edu.ec/handle/123456789/16110

-Manabí -Ecuador, M. (2023). *LÍNEAS INSTITUCIONALES DE INVESTIGACIÓN*.

Marín Velásquez, D. S., Medina Solorzano, C. X. & ESPOL.FIEC. (2024). *Diseño de un plan Director de seguridad para una Empresa privada que brinda servicios de Auditoria para reducir riesgos expuestos en un entorno seguro*. http://www.dspace.espol.edu.ec/handle/123456789/62349

Maurya, P., Hazra, A., Kumari, P., Sørensen, T. B. & Das, S. K. (2025). A Comprehensive Survey of Data-Driven Solutions for LoRaWAN: Challenges and Future Directions. *ACM Transactions on Internet of Things*, *6*(1), 1-36. https://doi.org/10.1145/3711953

Mieles-Giler, J. W., Guerrero-Calero, J. M., Moran-González, M. R. & Zapata-Velasco, M. L. (2024). Evaluación de la degradación ambiental en hábitats Naturales. *Journal of Economic and Social Science Research*, *4*(3), 65-88. https://doi.org/10.55813/GAEA/JESSR/V4/N3/121

Milovanov, N. (2024). Case study: LoRa/LoRaWAN as a suitable LPWAN choice for pressure and flow monitoring in Bulgarian water utility sector. *ACM International Conference Proceeding Series*, 173-179. https://doi.org/10.1145/3674912.3674945

Ministerio de Desarrollo Social y Familia. (s.f.). (2020). *Chile Agenda 2030, Ministerio de Desarrollo Social y Familia*. undación MERI, Ministerio de Medio Ambiente, ARMADA de Chile, Sernapesca, Subpesca, Universidad Pol. https://www.chileagenda2030.gob.cl/accion/accionficha/33

Ministerio de Hacienda y Administraciones Públicas. (2012a). *MAGERIT – versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método*. https://www.hacienda.gob.es/SGT/CATALOGO_SEFP/046_Magerit_v3_libro1_metodo.pdf

Ministerio de Hacienda y Administraciones Públicas. (2012b). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II : Catálogo de elementos*. https://www.hacienda.gob.es/SGT/CATALOGO_SEFP/047_Magerit_v3_libro2_catalogo.pdf

Moresi, A. A., Motta, G. J. L., Trama, G. A., Saldanha Walker, M. & Amaya, C. F. (2023). *Operaciones en el ambiente de la información*. https://cefadigital.edu.ar/handle/1847939/2494

National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53, Revision 5 – Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

Nmesoma Okorie, G., Ann Udeh, C., Martha Adaga, E., Donald DaraOjimba, O., Itohan Oriekhoe, O. & Author, C. (2024). ETHICAL CONSIDERATIONS IN DATA COLLECTION AND ANALYSIS: A REVIEW: INVESTIGATING ETHICAL PRACTICES AND CHALLENGES IN MODERN DATA COLLECTION AND ANALYSIS. *International Journal of Applied Research in Social Sciences*, *6*(1), 1-22. https://doi.org/10.51594/IJARSS.V6I1.688

Ortiz-Garcés, I., Cadena, C., Negrette, G. & Villegas-Ch, W. (s. f.). *Reference Framework for Cybersecurity Risk Management of IoT Ecosystems in Smart Cities*.

Parmar, T. (2025). *Implementing CI/CD in Data Engineering: Streamlining Data Pipelines for Reliable and Scalable Solutions*. International Journal of Innovative Research in Modern Physics & Sciences,. https://www.researchgate.net/publication/388631853_Implementing_CICD_in_Data_Engineering_Streamlining_Data_Pipelines_for_Reliable_and_Scalable_Solutions

Parra, N. A. L. (2023). Importancia de la biodiversidad y los servicios ecosistémicos en la toma de decisiones ambientales de los países de américa del sur. Capítulo 2. *Los objetivos del desarrollo sostenible*. https://doi.org/10.59955/9786075967530

Peña-Casanova, M. , & A.-C. C. (2020). *Integración de marcos de referencia para gestión de Tecnologías de la Información*. http://scielo.sld.cu/scielo.php?pid=S1815-59362020000100011&script=sci_arttext&tlng=pt

Pira, P. & Andrea, B. (2020). *Importancia de un sistema de gestión de seguridad de la información para empresas de tecnología*. http://repository.unipiloto.edu.co/handle/20.500.12277/6841

Pires, L. M. & Gomes, J. (2024). River Water Quality Monitoring Using LoRa-Based IoT. *Designs 2024, Vol. 8, Page 127*, *8*(6), 127. https://doi.org/10.3390/DESIGNS8060127

Poma Moya, C. C. (2020). *Desarrollo de un modelo de Sistema de Gestión de Seguridad de la Información basado en la Norma NB/ISO/IEC 27001 aplicado al área de ti en Empresas Corredoras de Seguros y Reaseguros*. http://repositorio.umsa.bo/xmlui/handle/123456789/33582

Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L. T. & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*(1), 1-21. https://doi.org/10.1186/S42400-020-00052-8/METRICS

Rivas, A. (16 de marzo de 2025). *Normas APA: La guía definitiva para presentar trabajos escritos*. Guía Normas APA. https://normasapa.in/

Scholar Chinenye Obasi, Nko Okina Solomon, Olubunmi Adeolu Adenekan & Peter Simpa. (2024). Cybersecurity's Role in Environmental Protection and Sustainable Development: Bridging Technology and Sustainability Goals. *Computer Science & IT Research Journal*, *5*(5), 1145-1177. https://doi.org/10.51594/CSITRJ.V5I5.1140

Shome, A., Phartyal, S. S., Maharana, P., Yadav, H. & Verma, A. (2025). Ecosystem services vulnerability index: a novel framework to assess the vulnerability of species providing ecosystem service. *Wetlands Ecology and Management*, *33*(1), 1-14. https://doi.org/10.1007/S11273-024-10023-2/METRICS

Soto Pineda, R. & Autor, *. (2021). Metodología para la investigación de incidentes de seguridad en aplicaciones web. *UCIENCIA 2021*. https://repositorio.uci.cu/jspui/handle/123456789/9690

Stephen, M. (2023). *Data Backup Strategies in Disaster Recovery: Ensuring Minimal Downtime*. https://www.researchgate.net/publication/383276577_Data_Backup_Strategies_in_Disaster_Recovery_Ensuring_Minimal_Downtime

SUSTENTABLE, A. P. E. D. and Y. SOSTENIBLE. (2023). *LÍNEAS INSTITUCIONALES DE INVESTIGACIÓN*.

Tang, X., Yao, X., Liu, D., Zhao, L., Li, L., Zhu, D. & Li, G. (2022). A Ceph-based storage strategy for big gridded remote sensing data. *Big Earth Data*, *6*(3), 323-339. https://doi.org/10.1080/20964471.2021.1989792

Tapi, V. B. V. (2023). El medio ambiente y su importancia para la humanidad. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *5*(7), 296-304. https://doi.org/10.59169/PENTACIENCIAS.V5I7.938

Terán Terranova, Y. J. (2021). *Seguridad en la Gestión de la información para las organizaciones públicas desde el enfoque ISO/IEC 2700: un Mapeo Sistemático*. http://dspace.ups.edu.ec/handle/123456789/20333

The Open Group. (2022). *TOGAF® Standard, 10th Edition – Architecture Development Method*. Van Haren Publishing; The Open Group. https://www.opengroup.org/togaf-standard-10th-edition-downloads

Tmuši, G., Manfreda, S., Aasen, H., James, M. R., Gonçalves, G., Ben-Dor, E., Brook, A., Polinova, M., Juan Arranz, J., Mészáros, J., Zhuang, R., Johansen, K., Malbeteau, Y., Pedroso de Lima, I., Davids, C., Herban, S. & McCabe, M. F. (2020). Current Practices in UAS-based Environmental Monitoring. *Remote Sensing* , *12*, 1001. https://doi.org/10.3390/rs12061001

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy 2022, Vol. 2, Pages 573-586*, *2*(3), 573-586. https://doi.org/10.3390/JCP2030029

Urbano, F., Viterbi, R., Pedrotti, L., Vettorazzo, E., Movalli, C. & Corlatti, L. (2024). Enhancing biodiversity conservation and monitoring in protected areas through efficient data management. *Environmental Monitoring and Assessment*, *196*(1), 1-16. https://doi.org/10.1007/S10661-023-11851-0/FIGURES/1

Ureña Agüero, Y. (2020). *Propuesta de una guía de auditoría para el sistema de gestión de la seguridad de la información alineada a estándares y mejores prácticas internacionales.* xmlui/handle/123456789/387

U.S. Environmental Protection Agency. (2024). *Environmental Information Policy, Procedures and Standards | US EPA*. https://www.epa.gov/irmpoli8/environmental-information-policy-procedures-and-standards

Valdez, J. W., Pereira, H. M., Morejón, G. F., Acosta-Muñoz, C., Bonet Garcia, F. J., Castro Vergara, L., Claros, X. R., Gill, M. J., Josse, C., Lafuente-Cartagena, I., Langstroth, R., Sheppard, S. N., Orihuela, G., Prieto-Albuja, F. J., Quillahuaman, N., Terán, M. F., Zambrana-Torrelio, C. M., Navarro, L. M. & Fernandez, M. (2023). Tailoring evidence into action: Using a co-design approach for biodiversity information in the Tropical Andes. *Conservation Science and Practice*, *5*(12), e13035. https://doi.org/10.1111/CSP2.13035

Venkatesan, K. B. (2025). Managing Machine Learning Complexity with Advanced Version Control Techniques. *International Journal of Computer Applications*, *186*(65), 975-8887.

Villegas-Ch, W. & García-Ortiz, J. (2023). Authentication, access, and monitoring system for critical areas with the use of artificial intelligence integrated into perimeter security in a data center. *Frontiers in Big Data*, *6*, 1200390. https://doi.org/10.3389/FDATA.2023.1200390/BIBTEX

Weekers, D., Petrossian, G. & Thiault, L. (2021). Illegal fishing and compliance management in marine protected areas: a situational approach. *Crime Science*, *10*(1), 1-14. https://doi.org/10.1186/S40163-021-00145-W/FIGURES/4

World Bank Group. (2024, 29. noviembre). *Protecting Jaguars' Role in Ecosystem Balance in the Amazon*. https://www.worldbank.org/en/news/feature/2024/11/29/protecting-jaguars-role-in-ecosystem-balance-in-the-amazon

XENON Systems. (2019). *HPC Cluster for Environmental Modelling - XENON Systems*. https://xenon.com.au/case-studies/hpc-cluster-for-environmental-modelling/

Yang, X., Xi, W., Chen, A. & Wang, C. (2021). An environmental monitoring data sharing scheme based on attribute encryption in cloud-fog computing. *PLOS ONE*, *16*(9), e0258062. https://doi.org/10.1371/JOURNAL.PONE.0258062

Yasmin, R., Mikhaylov, K. & Pouttu, A. (2020). LoRaWAN for Smart Campus: Deployment and Long-Term Operation Analysis. *Sensors 2020, Vol. 20, Page 6721*, *20*(23), 6721. https://doi.org/10.3390/S20236721

Anexos

Anexo A Glosario Ampliado



Anexo A Glosario Ampliado.pdf

Anexo B Plan de capacitación, sensibilización y comunicación de seguridad de la información



Anexo B Plan de capacitación, sensib

Anexo C Guía de Referencia para Desarrollar un Diagnóstico de Madurez en Seguridad de la Información



Anexo C Guía de Referencia para Des

Anexo D Marcos Teórico y de Referencia Ampliado



Anexo D Marcos Teórico y de Referer

Anexo E Estructuración del Modelo de Seguridad



Estructuración del Modelo de Seguridad