

DISEÑO DE MODELO DE CIBERSEGURIDAD PARA INSTITUCIONES FINANCIERAS: IDENTIFICACIÓN, CLASIFICACIÓN Y PROTECCIÓN DE ACTIVOS CRÍTICOS IFA (INTERNET FACING APPLICATIONS)

LUZ ADRIANA LOAIZA MORENO

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
MAESTRÍA EN GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ, COLOMBIA
Abril de 2025

DISEÑO DE MODELO DE CIBERSEGURIDAD PARA INSTITUCIONES FINANCIERAS: IDENTIFICACIÓN, CLASIFICACIÓN Y PROTECCIÓN DE ACTIVOS CRÍTICOS IFA (Internet Facing Applications)

Luz Adriana Loaiza Moreno

Monografía para optar por el titulo magister en gestión y seguridad de la información

Director del Proyecto de grado
Miguel Ángel Leguizamón Páez
Magister En Ciencias De La Información Y Las Comunicaciones

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
MAESTRÍA EN GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ, COLOMBIA
Abril de 2025

CONTENIDO

1 Planeación 13
1.1 Resumen 13
1.2 Abstract 13
1.3 Introducción 15
1.4 Contextualización del tema 15
1.5 Formulación del problema 16
1.6 Objetivo General 17
1.6.1 Objetivos Específicos 17
1.7 Metodología 18
1.7.1 Metodología integrada para la identificación y protección de activos críticos IFAS en entidades financieras. 18
1.7.2 Fase 1: Análisis de marcos de trabajo e identificación de activos críticos. 18
1.7.3 Fase 2: Evaluación de vulnerabilidades y brechas de seguridad. 18
1.7.4 Fase 3: Diseño de un Modelo de Buenas Prácticas de Ciberseguridad 19
1.7.5 Fase 4: Documentación y Fortalecimiento de la Madurez Cibernética 19
1.8 Justificación 19
1.9 Marco Teórico 21
1.9.1 Ciberseguridad en la banca 21
1.9.2 Los ciberataques más comunes a las entidades financieras 21
1.9.3 Guía para la gestión y clasificación de activos de información 22
1.9.4 Seguridad de la información 23

1.9.5 Marco de ciberseguridad del NIST (NIST CSF) 23
1.9.6 Fundación de software de aplicaciones abiertas 24
1.9.7 Framework COBIT 26
1.9.8 Internet facing applications (IFA) 26
1.9.9 Herramientas de ciberseguridad en instituciones financieras 27
1.9.10 Marco institucional 28
1.9.11 Regulación y normativas de ciberseguridad 28
1.9.12 Rol de las instituciones reguladoras y supervisión 31
2 Desarrollo Metodológico 35
2.1 Fase 1: Análisis de los modelos, estándares y marcos de trabajo para la identificación de Activos críticos 35
2.1.1 Revisión documental 36
2.1.2 Análisis de Estándares 36
2.1.3 Análisis de Normativas Locales para Instituciones Financieras 41
2.1.4 Metodología de Mapeo de Procesos Críticos 47
2.1.5 Método de Análisis 48
2.1.6 Análisis de riesgos de los procesos 57
2.1.7 Evaluación de controles existentes en la organización 60
2.1.8 Análisis de impacto en el negocio (BIA) 67
2.1.9 Definición de planes de contingencia 76
2.1.10 Mantenimiento y Mejora Continua de los Planes 89
2.1.11 Documentación Asociada 90
2.1.12 Integración con el Marco de Gestión de Continuidad 91
2.1.13 Conclusiones y recomendaciones implementación plan de contingencia 91
2.1.14 Identificación de activos IFAS 93

2.2 Fase 2: Metodología de identificación y clasificación de vulnerabilidades y brechas de seguridad en entidades financieras 101

2.2.1 Análisis de riesgos 101

2.2.2 Metodología NIST SP 800-30 para Evaluación de Riesgos 101

2.2.3 Ejemplos: escenarios de Ataque MITRE ATT&CK para Activos IFAS 108

2.2.4 Controles de Mitigación Recomendados según NIST SP 800-53 112

2.2.5 Plan de Remediación y Gestión Continua de Riesgos 113

2.2.6 Metodología de Gap Analysis para activos IFAS 114

2.2.7 Simulación de ataques 120

2.2.8 Análisis final fase 2 128

2.3 Fase 3: diseño de un modelo control de buenas prácticas de ciberseguridad implementando controles y procedimientos de contención y mitigación. 128

2.3.1 Definición de controles 129

2.3.2 Definición de Controles 129

2.3.3 Controles Administrativos 132

2.3.4 Gestión de incidentes de seguridad 134

2.3.5 Cumplimiento y gobernanza 135

2.3.6 Resiliencia operativa 136

2.3.7 Procedimientos de respuesta a incidentes para activos IFAS 136

2.3.8 Integración de estándares: alineación del modelo con ISO 27001 y NIST CSF 142

2.3.9 Análisis fase 3 153

2.4 Fase 4: Elaboración de documentación de las buenas prácticas que permitan fortalecer el nivel de madurez cibernética en entidades financieras 154

2.4.1 Elaboración de manuales 154

2.4.2 Consideraciones especiales para internet facing applications 160

2.4.3 Guía para la gestión de vulnerabilidades y respuesta a incidentes 161
2.4.4 Gestión de vulnerabilidades 161
2.4.5 Respuesta a incidentes 165
2.4.6 Capacitación y difusión; taller para equipos técnicos: implementación del modelo de ciberseguridad 170
2.4.7 Evaluación de Madurez Cibernética para Instituciones Financieras 170
2.4.8 Metodología de Evaluación 174
2.4.9 Marco de Gobernanza 180
2.4.10 Ciclo de Mejora Continua (PDCA) 181
2.4.11 Metodología para Evaluación Pre/Post Implementación 181
2.4.12 Ejercicio: informe de madurez cibernética pre/post implementación 183
3 Análisis de resultados 194
3.1 Análisis de los Resultados por Fase 194
3.1.1 Resultados Fase 1: análisis marcos de trabajo e identificación de activos críticos 194
3.1.2 Resultados Fase 2: evaluación de vulnerabilidades y brechas de seguridad .. 195
3.1.3 Resultados de la Fase 3: diseño de un modelo de buenas prácticas de ciberseguridad 196
3.1.4 Resultados Fase 4: documentación y fortalecimiento de la madurez cibernética 196
3.1.5 Conclusiones del Análisis 198
4 CONCLUSIONES 200
5 REFERENCIAS BIBLIOGRÁFICAS 202
Anexo 1 Estructura de la Encuesta 206
Anexo 3 Ciclo de Mejora Continua (PDCA) 225

Lista de tablas

Tabla N°. 1 37
Tabla N°. 2 38
Tabla N°. 3 40
Tabla N°. 4 42
Tabla N°. 5 43
Tabla N°. 6 45
Tabla N°. 7 48
Tabla N°. 8 49
Tabla N°. 9 51
Tabla N°. 10 52
Tabla N°. 11 54
Tabla N°. 12 56
Tabla N°. 13 59
Tabla N°. *14* 61
Tabla N°. *15* 62
Tabla N°. 16 62
Tabla N°. *17* 63
Tabla N°. *18* 64
Tabla N°. 19 64
Tabla N°. 20 65
Tabla N°. 21 66
Tabla N°. 22 69
Tabla N°. *23* 70
Tabla N°. *24* 71
Tabla N°. 25 71
Tabla N°. 26 72
Tabla N°. 27 73
Tabla N°. 28 73
Tabla N°. 29 74
Tabla N°. 30 75

Tabla N°. 31 77
Tabla N°. 32 78
Tabla N°. 33 79
Tabla N°. 34 80
Tabla N°. 35 80
Tabla N°. 36 81
Tabla N°. 37 82
Tabla N°. 39 84
Tabla N°. 40 84
Tabla N°. 41 85
Tabla N°. 42 86
Tabla N°. 43 86
Tabla N°. 44 87
Tabla N°. 45 88
Tabla N°. 46 88
Tabla N°. 47 89
Tabla N°. 48 89
Tabla N°. 49 90
Tabla N°. 50 91
Tabla N°. 51 95
Tabla N°. 52 98
Tabla N°. 53 99
Tabla N°. 54 100
Tabla N°. 55 101
Tabla N°. 56 102
Tabla N°. 57 103
Tabla N°. 58 104
Tabla N°. 59 105
Tabla N°. 60 106
Tabla N°. 61 106
Tabla N°. 62 107

Tabla N°. 63 108
Tabla N°. 64 109
Tabla N°. 65 110
Tabla N°. 66 111
Tabla N°. 67 112
Tabla N°. 68 113
Tabla N°. 69 114
Tabla N°. 70 114
Tabla N°. 71 115
Tabla N°. 72 116
Tabla N°. 73 119
Tabla N°. 74 121
Tabla N°. 75 122
Tabla N°. 76 123
Tabla N°. 77 124
Tabla N°. 78 125
Tabla N°. 79 126
Tabla N°. 80 127
Tabla N°. 81 130
Tabla N°. 82 130
Tabla N°. 83 131
Tabla N°. 84 131
Tabla N°. 85 132
Tabla N°. 86 133
Tabla N°. 87 133
Tabla N°. 88 134
Tabla N°. 89 134
Tabla N°. 90 135
Tabla N°. 91 136
Tabla N°. 92 137
Tabla N°. 93 137

Tabla N°. 94 138
Tabla N°. 95 138
Tabla N°. 96 138
Tabla N°. 97 139
Tabla N°. 98 139
Tabla N°. 99 140
Tabla N°. 100 140
Tabla N°. 101 140
Tabla N°. 102 141
Tabla N°. 103 141
Tabla N°. 104 142
Tabla N°. 105 143
Tabla N°. 106 144
Tabla N°. 107 145
Tabla N°. 108 146
Tabla N°. 109 147
Tabla N°. 110 148
Tabla N°. 111 149
Tabla N°. 112 150
Tabla N°. 113 151
Tabla N°. 114 152
Tabla N°. 115 154
Tabla N°. 116 155
Tabla N°. 117 155
Tabla N°. 118 156
Tabla N°. 119 156
Tabla N°. 120 157
Tabla N°. 121 157
Tabla N°. 122 158
Tabla N°. 123 158
Tabla N°. 124 159

Tabla N°. 125 160
Tabla N°. 126 160
Tabla N°. 127 161
Tabla N°. 128 162
Tabla N°. 129 163
Tabla N°. 130 163
Tabla N°. 131 164
Tabla N°. 132 165
Tabla N°. 133 165
Tabla N°. 134 166
Tabla N°. 135 166
Tabla N°. 136 167
Tabla N°. 137 169
Tabla N°. 138 169
Tabla N°. 139 171
Tabla N°. 140 172
Tabla N°. 141 173
Tabla N°. 142 174
Tabla N°. 143 175
Tabla N°. 144 175
Tabla N°. 145 176
Tabla N°. 146 176
Tabla N°. 147 177
Tabla N°. 148 178
Tabla N°. 149 180
Tabla N°. 150 180
Tabla N°. 151 181
Tabla N°. 153 186
Tabla N°. 154 187
Tabla N°. 155 187
Tabla N°. 156 188

Lista de ilustraciones

Ilustración N° 1 Pregunta 1..... 213
Ilustración N° 2 Pregunta 2..... 213
Ilustración N° 3 Pregunta 3..... 214
Ilustración N° 4 Pregunta 4..... 214
Ilustración N° 5 Pregunta 5..... 215
Ilustración N° 6 Pregunta 6..... 215
Ilustración N° 7 Pregunta 7..... 216
Ilustración N° 8 Pregunta 8..... 216
Ilustración N° 9 Pregunta 9..... 217
Ilustración N° 10 Pregunta 10..... 217
Ilustración N° 11Pregunta 11..... 218
Ilustración N° 12 Pregunta 12..... 218
Ilustración N° 13 Pregunta 13..... 219
Ilustración N° 14 Pregunta 14..... 219
Ilustración N° 15 Pregunta 15..... 220
Ilustración N° 16 Pregunta 16..... 220
Ilustración N° 17 Pregunta 17..... 220
Ilustración N° 18 Pregunta 18..... 221
Ilustración N° 19 Pregunta 19..... 221
Ilustración N° 20 Pregunta 20..... **¡Error! Marcador no definido.**

1 Planeación

1.1 Resumen

Esta investigación se desarrolla a partir del diseño de un modelo de buenas prácticas de ciberseguridad enfocado principalmente en la protección de los activos críticos de Información (IFAS) para instituciones financieras. A través de la definición de 4 fases, las cuales en su desarrollo buscan brindar herramientas que permitan fortalecer la postura de ciberseguridad de las entidades financieras frente a las amenazas que se encuentran en evolución constante.

La investigación inicia con un análisis de marcos y estándares como ISO 27001, NIST SP 800-53 y COBIT 2019 que permiten obtener herramientas para identificar y clasificar los activos críticos de IFAS según la tríada CIA (Confidencialidad, Integridad, Disponibilidad). Posteriormente, evalúa las vulnerabilidades y las brechas de seguridad utilizando las metodologías de evaluación de riesgos NIST SP 800-30, complementadas con ejercicios de Red Team para evaluar la resiliencia de los activos críticos.

La contribución principal se enfoca en diseñar un modelo de protección apoyado en la definición de controles técnicos y administrativos los cuales están alineados con estándares internacionales como ISO 27001 y las funciones CSF de NIST (Identificar, Proteger, Detectar, Responder, Recuperar). Mediante la propuesta de guías de respuesta a incidentes basadas en NIST IR 8353 para escenarios como ataques de ransomware y violaciones de datos.

La última fase está enfocada en la documentación de los lineamientos que en los ejercicios propuestas apoyan el mejoramiento continuo de la madurez de la ciberseguridad en las entidades financieras, lo anterior incluye parámetros de clasificación de activos, protocolos de gestión de vulnerabilidades y procedimientos generales de respuesta a incidentes. El modelo permite realizar una medición utilizando mediante el uso del modelo de madurez de ciberseguridad CMMI y los niveles definidos por NIST CSF, lo cual proporciona a las entidades los pasos a seguir en el objetivo del mejoramiento continuo de sus capacidades de ciberseguridad y su resiliencia general ante amenazas.

1.2 Abstract

This research revolves around developing a design for a cybersecurity best practices model primarily focused on protecting critical Information assets (IFAS) in financial institutions. Through methodological exploration, 4 phases are defined, which in their development seek to

provide tools that strengthen the cybersecurity posture of financial entities against continuously evolving threats.

The research begins with an analysis of frameworks and standards such as ISO 27001, NIST SP 800-53, and COBIT 2019 that provide tools to identify and classify IFAS critical assets according to the CIA triad (Confidentiality, Integrity, Availability). Subsequently, it evaluates vulnerabilities and security gaps using NIST SP 800-30 risk assessment methodologies, complemented by red team exercises to assess the resilience of critical assets.

The main contribution focuses on designing a protection model supported by the definition of technical and administrative controls which are aligned with international standards such as ISO 27001 Annex A and NIST CSF functions (Identify, Protect, Detect, Respond, Recover). This is done through proposed incident response guidelines based on NIST IR 8353 for scenarios such as ransomware attacks and data breaches.

The final phase focuses on documenting the guidelines that, in the proposed exercises, support the continuous improvement of cybersecurity maturity in financial entities. This includes asset classification parameters, vulnerability management protocols, and general incident response procedures. The model allows measurement using the CMMI cybersecurity maturity model and the levels defined by NIST CSF, which provides entities with steps to follow in the objective of continuous improvement of their cybersecurity capabilities and their general resilience against threats.

1.3 Introducción

La ciberseguridad se ha convertido en un componente crítico para las instituciones del sector financiero, cuyas operaciones dependen en gran medida de sus soluciones tecnológicas y la conexión digital que permite mejorar la experiencia de sus usuarios. La protección de activos IFAS (Internet Facing Aplications) garantizan la continuidad operativa y así como confianza de los usuarios teniendo en cuenta que las amenazas cibernéticas se encuentran en constante evolución.

El análisis de marcos de trabajo reconocidos como ISO 27001, NIST SP 800-53 y COBIT 2019, permitió en una segunda instancia realizar una propuesta de evaluación de riesgos y vulnerabilidades basada en los parámetros definidos en la NIST SP 800-30. El diseño del modelo sugerido se encuentra alineado con estándares como el NIST Cybersecurity Framework y finaliza con la documentación del modelo y las medidas consideradas pertinentes en pro de fortalecer la postura de ciberseguridad en las entidades.

El resultado esperado de esta investigación es un modelo práctico y adaptable que permita a las instituciones financieras mejorar significativamente la protección de sus activos críticos, incrementar su capacidad de respuesta ante incidentes y elevar su nivel de madurez en ciberseguridad, contribuyendo así a la resiliencia del sector financiero.

1.4 Contextualización del tema

En la era digital, los activos de información se han convertido en uno de los recursos más valiosos para las organizaciones. Sin embargo, la falta de identificación y gestión adecuada de estos activos de información puede generar graves consecuencias, como la exposición de vulnerabilidades críticas que pueden ser explotadas por atacantes cibernéticos. Según (ASOBANCARIA. (2024), 2024), el malware bancario representa el 77% de los incidentes, seguido por el ciber fraude con un 16% y la suplantación de aplicaciones con un 7%. Los datos recopilados permiten identificar con precisión las vulnerabilidades y desafíos actuales que afectan al sector financiero. De acuerdo con un informe de IBM (IBM Security, 2023) el 60% de las empresas no tienen un inventario completo de sus activos de información, lo que dificulta la protección de sus sistemas y datos.

Esta problemática se agrava cuando los procesos misionales de la organización no están claramente definidos, lo que aumenta el riesgo de interrupciones operativas, pérdidas financieras y reputacionales.

La identificación de activos de información es el primer paso para implementar una técnica de seguridad de la información. Un estudio reciente de (Gartner, 2023) reveló que el 45% de las brechas de seguridad ocurren debido a la falta de visibilidad sobre los activos críticos, lo que permite a los atacantes explotar vulnerabilidades desconocidas. Además, el informe (IBM Security, 2023) de IBM (IBM Security, 2023) destacó que el costo promedio de una violación de datos alcanzó los 4.45 millones de dólares, un aumento del 15% respecto al año anterior, siendo la falta de gestión de activos uno de los factores contribuyentes.

1.5 Formulación del problema

La creciente sofisticación del cibercrimen en Colombia representa un desafío crítico para el sector financiero. Según el (Centro Cibernético Policial Informe anual de delitos informáticos en Colombia 2023., (2023)), en los últimos años ha registrado un incremento del 42% en delitos informáticos, destacándose el fraude electrónico y la suplantación bancaria como los principales vectores de ataque. Este escenario se agrava al analizar el Índice Nacional de Seguridad Cibernética (NCSI, 2023), que posiciona a Colombia en el puesto 69/160 países, evidenciando rezagos en la adopción de marcos normativos y capacidades técnicas para mitigar riesgos digitales. Aunque la Superintendencia Financiera de Colombia (2023) reporta avances en el nivel de madurez en ciberseguridad —con un crecimiento del 15% en la implementación de controles básicos—, persisten brechas de seguridad, como la falta de claridad en la identificación de activos críticos y la escasez de personal especializado en gestión de riesgos asociados a los mismos.

Estas deficiencias generan procesos de evaluación de riesgos diferenciados y una priorización inadecuada de activos, lo que incrementa la exposición a amenazas como ransomware, phishing avanzado y APTs (Advanced Persistent Threats). De acuerdo con Forrester Research (2023), el 68% de las instituciones financieras en Latinoamérica carecen de un inventario actualizado de sus activos críticos, lo que dificulta la implementación de controles proactivos. Esta situación no solo facilita la materialización de incidentes, sino que también deriva en pérdidas financieras (estimadas en USD 2.5 millones por incidente, según IBM X-Force, 2023) y daños reputacionales irreparables lo que puede generar la perdida de la confianza en dichas entidades financieras.

El foco de la problemática se centra en la falta de un modelo para la identificación y clasificación de activos críticos IFAS (Información Financiera Altamente Sensible). Por lo que se hace necesario realizar una clasificación muy clara y precisa, basada en estándares como ISO/IEC

27001 o el NIST Cybersecurity Framework, lo que garantizara a largo plazo que las entidades financieras estén y alineadas en sus habilidades de protección con la criticidad de sus recursos (activos de información). Es importante indicar que la rápida evolución de técnicas como el credential stuffing o la explotación de vulnerabilidades en APIs bancarias —reportadas por OWASP (2023)— exige no solo herramientas tecnológicas, sino también capacitación continua y gobiernos de datos robustos al interno de las organizaciones.

En este contexto, surge la siguiente pregunta de investigación:

¿Cómo diseñar un modelo de buenas prácticas de ciberseguridad mediante la identificación y clasificación de activos críticos IFAS aplicado a instituciones financieras, que garantice la integridad, confidencialidad y disponibilidad de la información, alineado con estándares internacionales de seguridad de la información?

1.6 Objetivo General

Diseñar un modelo de buenas prácticas de ciberseguridad para instituciones financieras en la identificación, clasificación y protección de activos críticos de información IFAS, buscando mejorar sus niveles de madurez cibernética.

1.6.1 *Objetivos Específicos*

- Realizar un análisis de modelos, estándares y marcos de trabajo, para la identificación de activos críticos IFAS para comprender la importancia de estos en las entidades financieras.
- Identificar vulnerabilidades que puedan comprometer la integridad y confidencialidad de los activos críticos IFAS en las entidades financieras, considerando las brechas de seguridad que los afecten.
- Diseñar un modelo de buenas prácticas de ciberseguridad centrado en la protección de activos críticos IFAS, mediante la consideración de medidas preventivas y procedimientos de respuesta a incidentes para garantizar la seguridad de dichos activos.
- Documentar buenas prácticas que fortalezcan los niveles de madurez cibernética en entidades financieras mediante el reconocimiento de las vulnerabilidades identificadas.

1.7 Metodología

1.7.1 *Metodología integrada para la identificación y protección de activos críticos IFAS en entidades financieras.*

Esta metodología combina los objetivos planteados con un planteamiento estructurado en **4 fases**, integrando estándares internacionales (*ISO/IEC 27001*, *NIST Cybersecurity Framework*) y herramientas técnicas para garantizar la protección de activos críticos y el fortalecimiento de la madurez cibernética.

1.7.2 *Fase 1: Análisis de marcos de trabajo e identificación de activos críticos.*

El objetivo de esta fase consiste en realizar un análisis a los modelos, estándares y marcos de trabajo para identificar activos críticos IFAS y su importancia en el sector financiero.

- **Revisión documental**:
    - Estudio de estándares (*ISO 27001*, *NIST SP 800-53*, *COBIT 2019*) y normativas locales.
    - Identificación de procesos críticos.

- **Identificación de activos IFAS**:
    - Encuesta colaborativa con áreas de TI, riesgos y negocio para identificar la problemática del levantamiento de activos.
- **Clasificación de activos**:
    - Taxonomía basada en confidencialidad, integridad y disponibilidad (Triada CIA).

1.7.3 *Fase 2: Evaluación de vulnerabilidades y brechas de seguridad.*

El objetivo de esta fase consiste en Identificar vulnerabilidades que comprometan la integridad y confidencialidad de los activos IFAS.

- **Análisis de riesgos**:
    - Evaluación de amenazas mediante **NIST SP 800-30** y escenarios de ataque.
- **Detección de brechas**:
    - Gap Analysis comparando controles actuales vs. estándares internacionales.
- **Simulación de ataques**:

- Realizar ejercicios de Red Team o pruebas de seguridad para probar la resiliencia de los activos críticos.

1.7.4 *Fase 3: Diseño de un Modelo de Buenas Prácticas de Ciberseguridad*

El objetivo de esta fase consiste en construir un modelo centrado en la protección proactiva y respuesta a incidentes para activos IFAS.

- **Definición de controles**:
  - Controles técnicos (encriptación, segmentación de redes) y administrativos (políticas de acceso mínimo).
- **Procedimientos de respuesta a incidentes**:
  - Diseño de playbooks basados en **NIST IR 8353** para escenarios como ransomware o filtración de datos.

- **Incorporación de estándares**:
  - Alineación del modelo con **ISO 27001** (Anexo A) y **NIST CSF** (Funciones: identificar, proteger, detectar, responder, recuperar).

1.7.5 *Fase 4: Documentación y Fortalecimiento de la Madurez Cibernética*

Basado en el desarrollo de las fases anteriores se realizará una documentación práctica que apoye el mejoramiento en la postura de madurez cibernética en entidades financieras.

- **Elaboración de manuales**:
  - Guías para la clasificación de activos, gestión de vulnerabilidades y respuesta a incidentes.
- **Capacitación y difusión**:
  - Propuesta de talleres para equipos técnicos y directivos sobre el modelo propuesto.
- **Evaluación de madurez**:
  - Medición usando el CMMI Cybersecurity Maturity Model o NIST CSF Tiers.

1.8 Justificación

Es necesaria la construcción de un metodología para la identificación, clasificación y protección de activos críticos de información (IFAS) en instituciones financieras colombianas sustentado en las siguientes premisas: el impacto económico de los ciberataques para las entidades financieras, las brechas técnicas identificadas en el sector y la necesidad de alineación con estándares de

seguridad internacionales y normativa nacional. A continuación, se presentan las vulneraciones presentadas a los activos expuestos a internet y las consecuencias que implicaron que acarrearon las instituciones financieras por dichas brechas de seguridad.

- **Impacto Económico y Operativo:** durante el 2023, Colombia registró un aumento del 42% en delitos informáticos, siendo el sector financiero el más afectado por fraudes y suplantaciones bancarias (Centro Cibernético Policial, 2023). Según el Cost of a Data Breach Report 2024 de IBM, el costo promedio de una brecha de datos en el sector financiero latinoamericano alcanzó los USD 5.3 millones, con un tiempo promedio de contención de 287 días. Estos datos subrayan la necesidad de tecnicas preventivas más que reactivas, como la gestión adecuada de activos críticos, para reducir costos, tiempos de respuesta y aumentar la resiliencia de estas entidades.
- **Brechas en la Gestión de Activos Críticos:** Un estudio de la Superintendencia Financiera de Colombia (2023) reveló que el 65% de las entidades financieras carecen de un inventario actualizado de sus activos de información, lo que genera una problemática al interno de las entidades al tratar de implementar controles de seguridad. Esta falta de definición lleva a realizar evaluaciones de riesgo parciales y exposición a amenazas como ransomware y APTs (Advanced Persistent Threats). A pesar que el National Cyber Security Index (2023) ubica a Colombia en el puesto 69 de 160 países, indicando el avance en la adopción de marcos normativos y capacidades técnicas, es notable que este indicador debe ser superado adoptando buenas prácticas de seguridad al interno de cada entidad.
- **Alineación con Estándares Globales:** La aplicación de modelos basados en ISO/IEC 27001 y NIST Cybersecurity Framework ha demostrado disminuir cerca de un 40% la probabilidad de incidentes de consideración en las entidades que se preocupan por gestionar sus activos críticos asociados a sus procesos misionales (Gartner, 2023). Sin embargo, en Colombia, solo el 30% de las entidades financieras han adoptado estos estándares de manera precisa (ASOBANCARIA, 2024).

La ausencia de un modelo claro y asociado a la gestión de IFAS no solo incrementa el riesgo de pérdida de información sensible, sino que también compromete la confianza en el sistema financiero. Por ello, esta propuesta metodológica busca generar un esquema que permitan trabajar sobre las brechas operativas, tecnológicas y humanas, garantizando que la identificación y

clasificación de activos críticos se realice sin comprometer su integridad, confidencialidad e integridad asociada a cada proceso critico al interno de una entidad financiera.

1.9 Marco Teórico

La conceptualización de la ciberseguridad representa un campo dinámico y multidimensional que va más allá de la simple protección tecnológica. Se trata de un ecosistema complejo que integra:

- **Aspectos Tecnológicos:** Herramientas, infraestructuras y soluciones técnicas
- **Dimensión Estratégica:** Planificación y gestión de riesgos
- **Componente Humano:** Cultura, concienciación y comportamiento
- **Perspectiva Regulatoria:** Cumplimiento normativo y estándares internacionales.

1.9.1 *Ciberseguridad en la banca*

En el entorno en general la ciberseguridad es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización (IBM, ¿Qué es la ciberseguridad? (s/f)., 2023) .

Ahora bien, en la Banca no tiene una interpretación muy distante del concepto general de ciberseguridad entendiendo que en la banca se conceptúa como un conjunto de tecnologías y métodos diseñados para garantizar la seguridad de los datos y activos de los clientes y mantener la reputación del banco (Rudra, 2023).

Durante los últimos años, check point research estuvo informando de un aumento interanual del 48% en los ciberataques basados en la cloud para 2022, como consecuencia del creciente traslado de las operaciones de las organizaciones a la cloud debido a la escalada de los procesos de transformación digital (ITware, 2023), lo que con lleva a enfocarse principalmente en aplicaciones que estén expuesta a la nube mediante la identificación y pertinente clasificación para garantizar la protección adecuada a las mismas .

1.9.2 *Los ciberataques más comunes a las entidades financieras*

El sector financiero se encuentra en constante peligro de fuentes externas, destacando la habilidad y perseverancia de los criminales para aprovechar cualquier falla en las entidades o descuido de los usuarios. El phishing es una táctica común que consiste en simular fuentes

confiables, como bancos, para obtener información confidencial a través de correos electrónicos fraudulentos.

El sistema financiero en general, es atacado diariamente por amenazas externas. Aunque la mayoría de los intentos no logran su cometido, también es cierto que los delincuentes son persistentes y cada vez más ingeniosos para aprovechar cualquier falencia de las entidades o descuido de los usuarios.

- **Phishing:** Se trata del envío de correos electrónicos con la apariencia de proceder de fuentes de confianza, como bancos, o entidades de seguro, pero en realidad es una suplantación. El objetivo de los delincuentes es obtener información confidencial de los usuarios, como las contraseñas, pin de tarjetas de crédito, por medio de links, archivos adjuntos, o formularios.
- **Malware financieros:** Los malware financieros son el problema más común asociado con las transacciones fraudulentas en la banca digital en la actualidad. Comúnmente identificado como troyano bancario, los malware financieros buscan acceder a las cuentas para robar dinero y datos financieros, así como proporcionar a los cibercriminales acceso a los activos y equipos de los usuarios y de las organizaciones financieras.
- **Ransomware:** Es un ciberdelito tipo secuestro. El ciberdelincuente toma control del equipo o sistema infectado y lo "secuestra" cifrando la información, y bloqueando la pantalla. Después, el usuario es víctima de extorsión, en donde comúnmente se le exige un pago económico a cambio de recuperar el normal funcionamiento (Seguridad., 2023).

1.9.3 *Guía para la gestión y clasificación de activos de información*

La realización de un inventario y clasificación de activos es una parte importante de la debida diligencia estratégica establecida en el Modelo de Seguridad y Privacidad de la Información, que se enfoca en garantizar la seguridad de los activos de información dentro de los procesos organizativos. La realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una

entidad, y cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos en el Ítem 8 de la Tabla 2 – de la guía Controles del estándar ISO/IEC 27001:2013:

- **Inventario de activos:** todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de los mismos.
- **Propiedad de los activos:** los activos de información del inventario deben tener un propietario.
- **Clasificación de la información:** La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- **Etiquetado y manipulado de la información:** Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización (MinTic, 2016).

1.9.4 *Seguridad de la información*

La seguridad de la información desempeña un papel crucial en la protección de los activos de una organización. Este concepto abarca un conjunto de prácticas y medidas diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la información. En términos de confidencialidad, se busca preservar la privacidad y el acceso autorizado a los datos sensibles, evitando cualquier divulgación no autorizada. La integridad, por otro lado, se refiere a la precisión y la fiabilidad de la información, asegurando que no sea alterada de manera no autorizada. Además, la disponibilidad se centra en garantizar que la información esté accesible cuando sea necesario, evitando interrupciones no planificadas.

La base teórica sólida al explicar estos principios clave de la seguridad de la información. Describe cómo estas funciones trabajan en conjunto para establecer un entorno digital seguro, vital para cualquier entidad que maneje datos sensibles. A través de esta comprensión teórica, los lectores obtienen las herramientas necesarias para evaluar y mejorar la postura de seguridad de su organización, fortaleciendo así la gestión de la información y protegiendo los activos valiosos contra amenazas cibernéticas (Bander, 2018).

1.9.5 *Marco de ciberseguridad del NIST (NIST CSF)*

Para mejorar la seguridad cibernética de las empresas, el marco de ciberseguridad del NIST (NIST CSF) ofrece una estructura completa. Al concentrarse en los activos críticos, se resaltan varias cuestiones importantes:

- **Identificación de Activos Críticos:** NIST CSF enfatiza la importancia de identificar y administrar activos de información críticos. Este método ayuda a las empresas a comprender mejor la naturaleza y el valor de sus activos, lo que da como resultado métodos de seguridad más efectivos.
- **Proteger Activos Críticos:** La protección es un principio del CSF. Se concentra en tomar medidas de seguridad específicas para proteger los activos críticos de las amenazas cibernéticas. Los controles de acceso, el cifrado y otras técnicas para reducir la vulnerabilidad pueden ser parte de esto.
- **Detección de Eventos:** Es crucial tener la capacidad de identificar eventos relacionados con activos importantes. El CSF aborda la necesidad de implementar sistemas de detección que puedan identificar rápidamente amenazas o violaciones de seguridad que puedan afectar estos activos (NIST, Cybersecurity Framework | NIST, 2013).

1.9.6 *Fundación de software de aplicaciones abiertas*

La Fundación OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web', en español) es una organización sin ánimo de lucro que se centra en mejorar la seguridad del software. Su misión es proporcionar recursos y herramientas que ayuden a las organizaciones a desarrollar, adquirir y mantener aplicaciones seguras. OWASP ha desarrollado una amplia gama de proyectos, guías y herramientas que abordan los principales desafíos de seguridad en el desarrollo de software.

Entre los recursos más destacados de OWASP se encuentra el "Top 10 de OWASP", que identifica las principales vulnerabilidades de seguridad en aplicaciones web. Este documento se actualiza periódicamente para reflejar las amenazas más recientes. Además, OWASP ofrece una amplia variedad de proyectos centrados en la seguridad, desde pruebas de seguridad hasta herramientas educativas.

El énfasis de OWASP en la transparencia, la colaboración y la accesibilidad ha convertido a la organización en un referente clave en la industria de la seguridad informática. Las prácticas y recomendaciones de OWASP son ampliamente adoptadas en el desarrollo de software seguro en todo el mundo.

La Fundación de Software de Aplicaciones Abiertas (OWASP) promueve buenas prácticas para mejorar la seguridad del software. Algunas de las recomendaciones clave incluyen:

- **Aplicar Principios de Seguridad desde el Inicio:** Integrar la seguridad en todas las etapas del ciclo de vida del desarrollo de software, desde el diseño hasta la implementación y el mantenimiento.
- **Concientización y Capacitación:** Fomentar la conciencia y la formación en seguridad entre los desarrolladores y profesionales de TI para que estén al tanto de las amenazas y las mejores prácticas.
- **Validación y Escape de Datos**: Implementar mecanismos de validación y escape de datos para prevenir la inyección de código y asegurar una manipulación segura de la información.
- **Gestión de Sesiones y Autenticación Segura:** Utilizar prácticas sólidas de gestión de sesiones y autenticación para garantizar la protección de las credenciales y prevenir el acceso no autorizado.
- **Control de Acceso:** Implementar controles de acceso adecuados para garantizar que los usuarios solo tengan acceso a los recursos que les corresponden y minimizar los riesgos de escalada de privilegios.
- **Seguridad en la Capa de Transporte:** Utilizar protocolos de cifrados seguros (como HTTPS) para proteger la información durante la transmisión y prevenir ataques de interceptación.
- **Monitoreo y Registro Seguro:** Establecer prácticas de monitoreo y registro de eventos para detectar posibles incidentes de seguridad y facilitar la respuesta rápida a amenazas.
- **Manejo Seguro de Errores:** Implementar un manejo seguro de errores para evitar la revelación de información sensible y ayudar a los desarrolladores a entender y abordar los problemas de manera eficiente.
- **Actualizaciones y Parches Regulares:** Mantener el software actualizado con las últimas correcciones de seguridad y parches para abordar vulnerabilidades conocidas.
- **Pruebas de Seguridad Continuas:** Realizar pruebas de seguridad de manera continua, incluyendo análisis estáticos y dinámicos, así como pruebas de penetración, para identificar y abordar posibles debilidades.

Estas prácticas son esenciales para construir aplicaciones seguras y resistir a las amenazas cibernéticas en un entorno digital en constante evolución.

1.9.7 *Framework COBIT*

Para que las técnicas de seguridad de la información sean eficaces, es necesario un planteamiento que incluya tanto el gobierno de la tecnología de la información como la gestión de servicios. En este contexto, se analiza el marco teórico COBIT (Objetivos de control de información y tecnologías relacionadas) creado por ISACA, enfocado en alinear los objetivos de TI con los del negocio y proporcionando controles y procesos específicos para garantizar la efectividad y seguridad en la implementación de tecnologías de la información lo que fortalece la capacidad de las organizaciones para gestionar y proteger sus activos críticos de manera eficiente.

- **COBIT (Control Objectives for Information and Related Technologies):** es un marco de gobierno y gestión de tecnologías de la información que proporciona a las organizaciones un conjunto de controles, procesos y mejores prácticas para garantizar la efectividad, eficiencia y seguridad en la implementación y uso de las tecnologías de la información. Desarrollado por ISACA (Information Systems Audit and Control Association), COBIT se centra en la alineación de las metas de TI con los objetivos del negocio, brindando una estructura que permite a las organizaciones supervisar y gestionar sus activos de información de manera más eficaz. Este marco aborda áreas clave como la entrega de servicios, la gestión de riesgos, el aseguramiento y la supervisión, proporcionando una guía para mejorar la seguridad de la información (COBIT, 2019).

1.9.8 *Internet facing applications (IFA)*

"Internet Facing Applications" (Aplicaciones Orientadas a Internet) se refiere a aquellas aplicaciones, servicios o sistemas que están diseñados y configurados para ser accesibles y utilizados a través de Internet. Estas aplicaciones están destinadas a interactuar directamente con usuarios, clientes u otras aplicaciones externas a través de la red mundial.

Estas aplicaciones deben considerar cuidadosamente su seguridad porque están disponibles desde Internet para evitar posibles amenazas cibernéticas. Esto requiere el uso de firewalls, cifrado de datos, autenticación sólida, monitoreo constante y prácticas de desarrollo seguras. La protección de la integridad, la confidencialidad y la disponibilidad de los datos y servicios que ofrecen es esencial para la seguridad de las aplicaciones en Internet.

Las aplicaciones web ofrecen una serie de beneficios significativos que han llevado a su amplia adopción en empresas de todos los tamaños. Su accesibilidad desde diversos navegadores y dispositivos, el desarrollo eficiente que permite ciclos cortos, la simplicidad para el usuario al no

requerir descargas, y la escalabilidad que facilita la adición de usuarios sin infraestructura lo que termina siendo una ventaja importante. Entre las aplicaciones web más comunes se encuentran aquellas destinadas al trabajo colaborativo, comercio electrónico, correo electrónico, banca en línea y documentación técnica.

La arquitectura cliente-servidor es necesaria para el funcionamiento de las aplicaciones web, dividiendo el código en scripts del lado del cliente y del servidor. El primero maneja la interfaz de usuario, mientras que el segundo se encarga del procesamiento de datos. A diferencia de los sitios web estáticos, las aplicaciones web brindan funcionalidades interactivas similares al software tradicional. Además, se destaca la diferencia entre aplicaciones web y nativas, siendo las últimas diseñadas específicamente para un entorno de usuario y descargadas en dispositivos, mientras que las aplicaciones web se entregan a través de navegadores web. AWS, con su servicio Amplify, proporciona una solución para el desarrollo, implementación y alojamiento de aplicaciones web, facilitando tanto el trabajo con el backend como la gestión del frontend y el alojamiento en la nube (Amazon.com, 2023).

1.9.9 *Herramientas de ciberseguridad en instituciones financieras*

El marco tecnológico para las herramientas de ciberseguridad en instituciones financieras se caracteriza por la adopción de soluciones avanzadas que aborden las amenazas cibernéticas de manera más precisa. Entre las herramientas clave se encuentran (Cisa.gov, Cisa.gov, 2023):

- **Firewalls Avanzados:** Implementación de firewalls de próxima generación que van más allá de la simple filtración de paquetes, incorporando inspección profunda de paquetes y capacidades de detección de intrusiones para proteger la red contra amenazas sofisticadas.
- **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS):** Utilización de soluciones IDS/IPS para monitorear y analizar el tráfico de red en tiempo real, identificando patrones de comportamiento anómalos y respondiendo de manera proactiva a posibles amenazas.
- **Antivirus y Antimalware Avanzado:** Implementación de soluciones de seguridad endpoint que van más allá de la detección básica de virus, utilizando tecnologías avanzadas como el análisis heurístico y el aprendizaje automático para identificar y mitigar amenazas.
- **Gestión de Identidad y Acceso (IAM):** Adopción de soluciones IAM para garantizar la autenticación segura de usuarios y el control preciso de los niveles de acceso, reduciendo así el riesgo de brechas de seguridad.

- **Análisis de Comportamiento del Usuario (UBA):** Implementación de herramientas UBA que monitorean el comportamiento de los usuarios en la red para detectar actividades inusuales o maliciosas, mejorando la capacidad de respuesta ante amenazas internas.
- **Sistemas de Gestión de Eventos e Información de Seguridad (SIEM):** Utilización de plataformas SIEM para recopilar, analizar y correlacionar eventos de seguridad en tiempo real, facilitando la identificación rápida de posibles incidentes.
- **Cifrado de Datos:** Aplicación de soluciones de cifrado para proteger datos sensibles, tanto en reposo como en tránsito, garantizando la confidencialidad de la información financiera.
- **Herramientas de Evaluación de Vulnerabilidades:** Empleo de herramientas que realizan escaneos regulares de la infraestructura en busca de vulnerabilidades, permitiendo corregirlas antes de que sean explotadas por posibles atacantes.
- **Blockchain y Tecnologías de Registro Distribuido (DLT):** Exploración de tecnologías como blockchain para mejorar la integridad y la transparencia en las transacciones financieras, reduciendo riesgos asociados a fraudes y manipulaciones.
- La combinación de estas herramientas en un marco tecnológico que permita fortalecer la postura de ciberseguridad de las instituciones financieras, proporcionando una defensa multifacética contra las amenazas emergentes en el panorama digital (Cisa.gov, Cybersecurity best practices, 2023).

1.9.10 *Marco institucional*

Dentro de este marco, la ciberseguridad se reconoce como un componente crucial para el desarrollo sostenible, la protección de la información y la preservación de la integridad de las instituciones financieras. Además, se enfatiza la importancia de adaptar las medidas y técnicas gubernamentales a los avances tecnológicos para garantizar una sociedad digital resistente y segura. Por lo tanto, este proyecto se enmarca en la visión constitucional de mejorar la seguridad y protección de los activos financieros cruciales en Colombia, contribuyendo a la realización de los principios constitucionales de bienestar general, seguridad y desarrollo.

1.9.11 *Regulación y normativas de ciberseguridad*

1.9.11.1 Circular Externa 042 de 2017 de la Superintendencia Financiera de Colombia (SFC).

La Superintendencia Financiera de Colombia (SFC) ha emitido la Circular Externa 042 de 2017 que juega un papel importante en la regulación y supervisión de las entidades financieras del país.

Esta circular proporciona pautas específicas sobre cómo gestionar los riesgos cibernéticos y la seguridad de la información en el sector financiero. La SFC detalla las medidas y controles que las entidades financieras deben implementar para reducir los riesgos relacionados con las amenazas cibernéticas en el documento.

La identificación y clasificación de activos de información crítica, la implementación de controles de acceso, la gestión de incidentes de seguridad y la realización de auditorías y evaluaciones de riesgos regulares son algunos de los temas que se abordan. La carta enfatiza la relevancia de tener un sistema de seguridad cibernética sólido y la importancia de establecer mecanismos efectivos para abordar emergencias. En síntesis, la Circular Externa 042 de 2017 de la SFC es una herramienta normativa esencial que guía a las entidades financieras en la implementación de prácticas de ciberseguridad y fomenta la resiliencia del sector ante las amenazas digitales cambiantes (Superintendencia Financiera de Colombia, superfinanciera.gov.co, 2023).

1.9.11.2 Ley Estatutaria 1581 de 2012 y Decreto Reglamentario 1377 de 2013

La Ley Estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013, también conocida como Ley de Protección de Datos Personales. La recolección, almacenamiento, uso, circulación y supresión de la información personal de los ciudadanos está regulada por estas normas. El derecho principal a la privacidad es protegido por la ley, que permite a las personas tener control sobre sus datos personales y promueve que las entidades responsables los traten correctamente. El Decreto Reglamentario 1377 de 2013 complementa la ley al definir temas específicos sobre el Registro Nacional de Bases de Datos y cómo las empresas deben gestionar y notificar a la Superintendencia de Industria y Comercio (SIC) las violaciones de seguridad de datos.

Las entidades financieras están obligadas por estas regulaciones a tomar medidas rigurosas para proteger la información personal de sus clientes y usuarios. Esto incluye la implementación de protocolos de seguridad, la designación de responsables de protección de datos, la realización de evaluaciones de riesgos y la notificación oportuna de eventos de seguridad. La normativa colombiana sobre protección de datos destaca la necesidad de proteger la privacidad de las personas en un entorno digital cada vez más complejo y conectado (Departamento Administrativo de la FunciónPública, 2023).

1.9.11.3 Ley 1121 de 2007 - Estatuto Orgánico del Sistema Financiero (EOSF)

La Ley 1121 de 2007, también conocida como el Estatuto Orgánico del Sistema Financiero (EOSF), es una legislación que regula el sistema financiero de Colombia. Esta ley establece los principios, reglas y procedimientos que rigen la organización y funcionamiento de las entidades financieras del país. El objetivo principal es aumentar la estabilidad, solidez y transparencia del sistema financiero para aumentar la confianza de los ciudadanos en las instituciones financieras.

El EOSF supervisa, controla y sanciona las entidades financieras, protege a los usuarios y previene el lavado de activos. Además, supervisa asuntos como la gestión de riesgos, las inversiones, la información financiera y las prácticas contables de las entidades que están bajo su jurisdicción. La ley tiene como objetivo mantener un equilibrio entre promover la eficiencia y la competitividad del sistema financiero y proteger los intereses de los clientes y la estabilidad económica del país (Senado de la Republica de Colombia, 2023).

1.9.11.4 Decreto 2257 de 2017

En Colombia, el Decreto 2257 de 2017 se presenta como una herramienta legal adecuada para abordar la ciberseguridad, particularmente en lo que respecta a las entidades financieras. Este decreto regula la gestión de riesgos cibernéticos y la seguridad de la información en el sector financiero. Abarca temas como la detección, evaluación y manejo de riesgos cibernéticos, y fomenta prácticas que mejoren la capacidad de las organizaciones para enfrentar amenazas digitales.

El Decreto 2257 proporciona instrucciones detalladas sobre cómo las entidades financieras deben implementar medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información. Establece las normas para la notificación de incidentes de seguridad con el fin de garantizar una respuesta rápida y coordinada a posibles ciberataques. Además, promueve la adopción de estándares internacionales en ciberseguridad y obliga a las entidades a tener un responsable de seguridad de la información. El decreto es un elemento esencial para reforzar la posición de las entidades financieras ante las amenazas cibernéticas que están aumentando y para asegurar la protección de la información confidencial de sus clientes (funcionpublica, 2023).

1.9.11.5 Resolución 2516 de 2018 de la SFC

La Resolución 2516 de 2018 de la Superintendencia Financiera de Colombia (SFC) es un marco regulatorio para el sector financiero del país. La ciberseguridad y la gestión de riesgos relacionados con la seguridad de la información en las entidades supervisadas por la SFC son sus principales preocupaciones. La resolución establece estándares específicos para mejorar las medidas de protección cibernética, con especial énfasis en la identificación, evaluación y tratamiento de los peligros que puedan comprometer la integridad y confidencialidad de la información manejada por estas entidades.

En detalle, la Resolución 2516 aborda la necesidad de implementar lineamientos y controles que mitiguen los riesgos cibernéticos, promoviendo así la resiliencia del sector financiero frente a amenazas digitales en constante evolución. Se establecen lineamientos claros para la notificación de incidentes de seguridad, asegurando una respuesta ante posibles ataques informáticos. Asimismo, la resolución exige la designación de responsables de seguridad de la información y fomenta la adopción de mejores prácticas y estándares internacionales en el ámbito de la ciberseguridad. En conjunto, la Resolución 2516 juega un papel importante en la consolidación de un entorno financiero más seguro y resistente a las amenazas digitales en Colombia (Superintendencia Financiera de Colombia, Fundacionmicrofinanzasbbva.org, 2023).

1.9.12 *Rol de las instituciones reguladoras y supervisión*

En Colombia, las instituciones reguladoras y de supervisión desempeñan roles clave en el ámbito de la ciberseguridad, especialmente en el sector financiero. Aquí se describen algunos de los roles de algunas de estas instituciones (MINTIC, Portal inicio, 2023):

- **Superintendencia Financiera de Colombia (SFC)**

La Superintendencia Financiera de Colombia (SFC) es responsable de la regulación y supervisión del sistema financiero de Colombia. La estabilidad, solidez y transparencia del sistema financiero del país son sus principales objetivos como entidad gubernamental autónoma. La SFC inspecciona, vigila y controla bancos, aseguradoras, sociedades fiduciarias y otras instituciones financieras. Dado el creciente papel de la tecnología en el sector financiero, su marco regulatorio abarca varios aspectos, incluida la ciberseguridad.

La SFC juega un papel importante en el ámbito de la ciberseguridad al establecer normas y directrices para proteger la integridad y confidencialidad de la información financiera. La organización establece normas específicas que requieren que las entidades financieras tomen medidas para prevenir, detectar y gestionar amenazas cibernéticas. Además, realiza auditorías y evaluaciones regulares para verificar el cumplimiento de estas normas y evaluar la capacidad de las entidades para responder ante incidentes de seguridad.

Además de sus responsabilidades regulatorias, la SFC es un organismo supervisor que supervisa de cerca las operaciones y prácticas de las entidades financieras para garantizar el cumplimiento de las regulaciones establecidas. La SFC tiene la autoridad de tomar medidas correctivas y aplicar sanciones en caso de incumplimientos o riesgos significativos. El sistema financiero colombiano se vuelve más resistente a las amenazas digitales gracias a su orientación proactivo en la ciberseguridad (Super intendencia Financiera de Colombia, 2023).

- **Banco de la República**

El papel del Banco de la República de Colombia primordial conforme a los lineamientos de la regulación y supervisión del sistema financiero del país. El Banco de la República juega un papel importante en la estabilidad económica como entidad emisora de la moneda y responsable de la política monetaria. El trabajo regulatorio incluye una variedad de temas, como la supervisión de las entidades financieras para asegurarse de que sean sólidas y contribuyan a la integridad del sistema financiero en general.

El Banco de la República establece normas y directrices en términos de ciberseguridad para garantizar la protección de la información financiera y la confianza en el sistema. En un entorno financiero cada vez más digitalizado, esta orientación es esencial. La entidad vigila activamente las prácticas de seguridad cibernética de las instituciones financieras bajo su jurisdicción y hace recomendaciones sobre cómo mejorar sus defensas contra ataques cibernéticos.

El Banco de la República también colabora en la coordinación de iniciativas con otras entidades regulatorias y supervisoras, trabajando juntos para enfrentar los desafíos que surgen en el sector financiero. La capacidad de las instituciones financieras para establecer políticas y sugerencias tiene un impacto en su dirección estratégica en cuanto a la seguridad cibernética, ya que fomenta la adopción de buenas prácticas que contribuyan a la resiliencia del sector financiero en un entorno digital en constante cambio (Banrep, 2021).

- **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**

La regulación y supervisión de la tecnología de la información y las comunicaciones en Colombia recae en el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Su responsabilidad principal es promover políticas públicas que promuevan un acceso justo a la tecnología de la información y protejan los derechos digitales de las personas. En este contexto, MinTIC juega un papel estratégico en la creación de estándares y reglamentos para garantizar la seguridad y privacidad de la información digital.

En lo que respecta a la ciberseguridad, MinTIC ha establecido pautas y estándares específicos para mejorar la protección de la información y los sistemas en un entorno cada vez más digital. Colabora estrechamente con otras entidades gubernamentales y actores del sector privado para coordinar esfuerzos y desarrollar técnicas que permitan combatir las amenazas cibernéticas. El Ministerio también desempeña un papel importante en fomentar buenas prácticas y aumentar la conciencia sobre ciberseguridad entre la población, las empresas e instituciones del país.

. Aparte de su misión de regulación, MinTIC se enfoca en fomentar la infraestructura tecnológica, la conectividad y la transformación digital en Colombia. Garantizar un entorno digital seguro y confiable que fomente el desarrollo sostenible del país y la participación activa de la sociedad en la era digital es su principal objetivo (MINTIC, Manual de Funciones del MinTIC - Manual de Funciones del MinTIC, 2023).

- **Comisión de Regulación de Comunicaciones (CRC)**

En Colombia, la Comisión de Regulación de Comunicaciones (CRC) es responsable de regular y supervisar el sector de las comunicaciones. Garantizar que todos los ciudadanos tengan acceso equitativo a los servicios de comunicación es su principal objetivo al promover un mercado de telecomunicaciones competitivo y eficiente. La CRC crea políticas y reglamentos para fomentar la competencia, proteger los derechos de los usuarios y garantizar que los servicios de comunicación sean de alta calidad y accesibles en todo el país.

La CRC juega un papel importante en el ámbito de la ciberseguridad al establecer normas y regulaciones para proteger la integridad de las redes y servicios de comunicación. Colabora estrechamente con otras entidades del gobierno y actores del sector para desarrollar lineamientos que aborden las amenazas cibernéticas y fortalezcan la resiliencia de las infraestructuras de comunicación críticas. Además, CRC ayuda a los proveedores de servicios y los usuarios finales a adoptar prácticas de ciberseguridad.

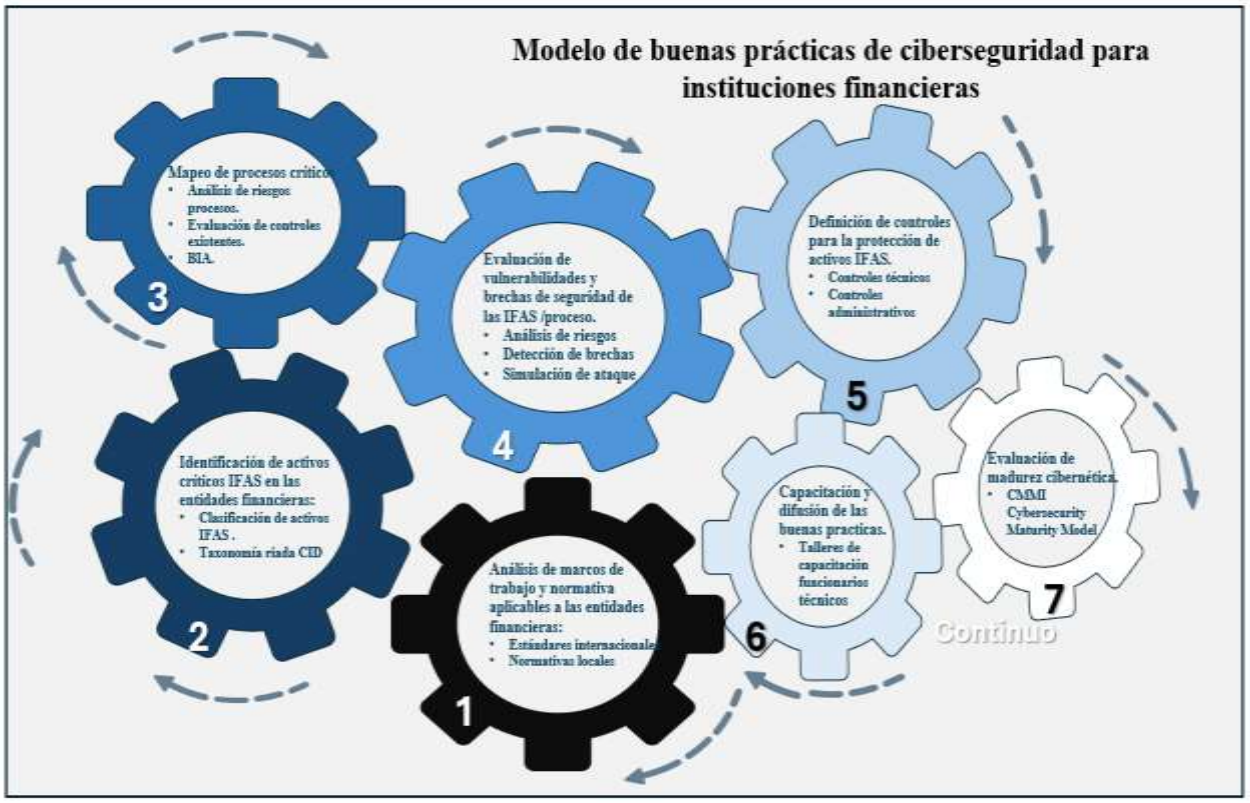
Además, la CRC garantiza que los operadores de telecomunicaciones cumplan con las políticas y regulaciones establecidas. Esto implica supervisar la calidad de los servicios, evaluar el desempeño de los operadores en términos de ciberseguridad y tomar medidas correctivas cuando sea necesario. En resumen, la Comisión de Regulación de Comunicaciones juega un papel importante en la creación de un entorno de comunicaciones seguro, eficiente y accesible para todos los ciudadanos de Colombia (CRC, 2022).

2 Desarrollo Metodológico

A continuación, se definen las fases correspondientes a cada uno de los componentes que hacen parte del marco modelo de buenas prácticas de ciberseguridad. En el siguiente esquema se encuentra general de cada uno de los componentes que se despliegan en cada fase en busca del desarrollo de los objetivos específicos propios de esta investigación.

Ilustración 1

Gráfico del modelo buenas prácticas de ciberseguridad en instituciones financieras.



Nota: esquema general de las buenas prácticas de ciberseguridad incluidas en cada fase metodológica.

2.1 Fase 1: Análisis de los modelos, estándares y marcos de trabajo para la identificación de Activos críticos

En el contexto de la seguridad de la información para instituciones financieras, la identificación y protección de los activos críticos de información (IFAS) es un ítem importante para garantizar la continuidad operativa y la resiliencia frente a las amenazas que se puedan presentar. Para ello,

es necesario analizar marcos de trabajo y estándares internacionales que permitan establecer una orientación estructurada y alineada con las mejores prácticas del sector financiero.

Esta fase se enfoca en realizar un análisis descriptivo de normativas y modelos de referencia, tales como ISO 27001, NIST SP 800-53 y COBIT 2019, así como en la revisión de regulaciones nacionales. A partir de este análisis, se realizará un mapeo de los procesos considerados más críticos, con el objetivo de identificar los activos esenciales para la operación y seguridad de las entidades financieras.

2.1.1 *Revisión documental*

El presente está enfocado la realización de un análisis de marcos de trabajo, estándares y normativas que están asociados la gestión de activos críticos en entidades financieras específicamente IFAS. La identificación y protección de activos críticos se hace necesaria para garantizar la continuidad operativa y la confianza en el sistema financiero. Los estándares internacionales (ISO 27001, NIST SP 800-53, COBIT 2019), que proporcionan mejores prácticas globalmente reconocidas; las normativas locales colombianas, que establecen el marco regulatorio específico del sector; y los procesos críticos, que permiten visualizar la interrelación entre los diferentes componentes de este gran sistema. La convergencia de estos elementos busca establecer un marco para la identificación, clasificación y protección de activos críticos en el entorno financiero actual, considerando tanto las exigencias regulatorias como las necesidades operativas de estas entidades.

2.1.2 *Análisis de Estándares*

En el ecosistema actual de amenazas cibernéticas en constante evolución, las instituciones financieras enfrentan desafíos sin precedentes en la protección de sus activos críticos de información. A continuación, se realiza una comparación estructurada de los marcos de referencia ISO/IEC 27001, NIST SP 800-53 y COBIT 2019 la cual presenta una visión de las fortalezas que cada estándar aporta a la gestión de seguridad.

Este análisis examina la orientación principal y la relevancia específica para instituciones financieras, controles relacionados con activos críticos, aplicabilidad sectorial, componentes esenciales, ventajas comparativas y aplicación práctica de cada marco.

Es importante indicar que la selección e implementación adecuada de estos estándares no representa necesariamente un ejercicio de cumplimiento normativo, sino una decisión estratégica que impacta directamente en la resiliencia operativa, la protección de datos sensibles y la continuidad del negocio en un sector donde la confianza del cliente y la integridad de las transacciones son los principales tópicos de estas entidades.

2.1.2.1 ISO/IEC 27001

El estándar ISO/IEC 27001 es un referente global para sistemas de gestión de seguridad de la información (SGSI), el cual se encuentra enfocado la identificación de riesgos. Este marco proporciona una metodología estructurada para la identificación, valoración y tratamiento de riesgos de seguridad, estableciendo un ciclo de mejora continua particularmente valioso para instituciones financieras que operan en entornos regulatorios complejos y con altas exigencias de protección de datos sensibles y activos críticos. en la tabla se identifican los componentes más importantes del estándar enfocados en las entidades financieras (ISO/IEC, 2022).

Tabla N°. 1

Contexto ISO /IEC 27001

Estándar	**ISO/IEC 27001**
Planteamiento principal	• Gestión de seguridad de la información basada en riesgos.
Relevancia para IFAS	• Proporciona un marco estructurado para identificar, clasificar y proteger activos críticos mediante un SGSI.
Principales controles relacionados con activos críticos	• A.5: Políticas de seguridad de la Información • A.8: Gestión de activos. • A.12: Seguridad en operaciones.
Aplicabilidad en Instituciones Financieras	• Ampliamente adoptado en el sector financiero para garantizar la seguridad y cumplimiento regulatorio.
Componentes Esenciales	• Estructura de Alto Nivel (HLS) • Política de Seguridad de la Información • Evaluación y Tratamiento de Riesgos • Declaración de Aplicabilidad (SOA) • Objetivos de Control y Controles (Anexo A) • Sistema de Métricas y Medición • Gestión de Documentación

Estándar	ISO/IEC 27001
Ventaja	• Reconocimiento internacional • Orientación metodológica • Flexibilidad en la implementación • Compatibilidad con otros sistemas de gestión • Certificación por terceros
Aplicación Practica	• Establecer el contexto organizacional • Definir el alcance del SGSI • Realizar evaluación de riesgos • Implementar controles seleccionados • Monitorear y medir efectividad • Mejora continua del sistema •

Nota: en la tabla se identifican los componentes más importantes del estándar enfocados en las entidades financieras (ISO/IEC, 2022).

2.1.2.2 NIST SP 800-53

El marco NIST SP 800-53, desarrollado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos, se enfoca en los controles de seguridad, este fue diseñado inicialmente para agencias federales, pero ampliamente adoptado en el sector privado. Este estándar se distingue por su meticulosa categorización de controles de seguridad y privacidad, el cual implementa un modelo de defensa en profundidad que resulta particularmente de importancia para instituciones financieras que requieren protecciones detalladas para sus sistemas de procesamiento de transacciones y repositorios de información sensible.

Tabla N°. 2

Contexto NIST SP 800-53

Estándar	NIST SP 800-53
Planteamiento principal	• Controles de seguridad para sistemas de información y organizaciones federales de EE.UU.
Relevancia para IFAS	• Ofrece un catálogo de controles de seguridad aplicables a la protección de activos críticos.

Estándar	NIST SP 800-53
Principales controles relacionados con activos críticos	• AC-6: Separación de funciones. • CM-6: Configuración de seguridad. • RA-2: Evaluaciones de riesgos de seguridad.
Aplicabilidad en instituciones financieras	• Es una referencia muy útil para mejorar la postura de seguridad.
Componentes esenciales	• Familias de controles de seguridad • Proceso de Selección de Controles • Conjunto de controles base • Esquema de gestión de riesgos
Ventajas	• Muy detallado y específico • Actualizaciones frecuentes • Integración con otros estándares NIST
Aplicación practica	• Planteamiento basado en riesgos • Categorizar el sistema de información • Seleccionar controles base o principales • Implementar controles complementarios • Documentar controles • Evaluar efectividad • Monitorear cambios

Nota: en la tabla se identifican los componentes más importantes o necesarios del estándar aterrizados a las entidades financieras (NIST SP 800-53, 2020).

2.1.2.3 COBIT 2019

COBIT 2019 representa una evolución significativa como marco de gobierno y gestión de la información y tecnología, trascendiendo el ámbito exclusivo de la seguridad para abarcar el alineamiento estratégico entre TI y objetivos de negocio. Este marco, desarrollado por ISACA, adopta una orientación que permite la identificación de valor, optimización de riesgos y optimización de recursos, proporcionando a las instituciones financieras una metodología estructurada para establecer un sistema de gobierno que garantice la protección de activos críticos mientras facilita la innovación y la transformación digital en un entorno altamente competitivo y regulado.

Tabla N°. 3

Contexto COBIT 2019

Estándar	COBIT 2019
Planteamiento Principal	• Gobernanza y gestión de TI para la alineación con los objetivos del negocio.
Relevancia para IFAS	• Permite identificar y gestionar activos críticos desde la gobernanza y cumplimiento.
Principales Controles Relacionados con Activos Críticos	• EDM03: Asegurar la optimización del riesgo. • APO12: Gestión del riesgo de seguridad. • DSS05: Seguridad de los servicios.
Aplicabilidad en Instituciones Financieras	• Aplicable a instituciones financieras para asegurar la alineación entre TI y los objetivos del negocio.
Componentes Esenciales	• Objetivos de gobierno • Procesos habilitadores • Estructura organizacional • Cultura y comportamiento • Información y tecnología • Servicios e infraestructura
Ventajas	• Alineación TI-negocio • Adaptabilidad • Integración con otros marcos
Aplicación Practica	• Planteamiento sobre el valor empresarial • Identificar necesidades de stakeholders • Definir alcance del sistema de gobierno • Construir modelo de objetivos con una hoja de ruta. • Implementar las soluciones definidas en el proceso.

Nota: en la siguiente tabla se identifican los componentes más importantes del estándar enfocados en las entidades financieras (COBIT, 2019).

2.1.2.4 Conclusión análisis marcos

Tras un análisis de los marcos ISO/IEC 27001, NIST SP 800-53 y COBIT 2019, resulta evidente que cada uno aporta conceptos complementarios esenciales para la protección de activos críticos en instituciones financieras. La constitución particular de cada uno proporciona estructuras sistemáticas para abordar las complejas exigencias regulatorias del sector financiero el cual es objeto de este análisis, estableciendo parámetros de defensa contra amenazas en un entorno donde los ciberataques son cada vez más específicos y persistentes. El estándar ISO/IEC 27001 aporta un sentido muy completo de gestión de riesgos, el cual es reconocido internacionalmente, NIST

SP 800-53 ofrece controles puntuales y de defensa, y COBIT 2019 comprende el aseguramiento y alineación estratégica entre seguridad y objetivos de negocio. La implementación estratégica de estos estándares no solo fortalece la postura de seguridad de las entidades financieras, sino que también fomenta la confianza de clientes e inversionistas, lo que es necesario para ser sostenibles y competitivos en el sector financiero donde la protección de datos y la integridad de las transacciones son el fundamento principal de su propuesta de valor.

2.1.3 *Análisis de Normativas Locales para Instituciones Financieras*

Las regulaciones locales se encuentran en un continuo cambio, por lo que las entidades financieras deben estar alineadas contantemente con estas a nivel local lo que representa un desafío en la gestión de sus activos de información críticos. El presente análisis evalúa detalladamente el marco normativo que rige a las entidades financieras, identificando requisitos explícitos e implícitos asociados a la identificación, clasificación y protección de activos de información. Las regulaciones locales, caracterizadas por su precisión contextual y sus constantes actualizaciones, definen lineamientos obligatorios en algunos casos alineados con los marcos internacionales de referencia, integrando consideraciones especificas adaptadas al ecosistema financiero de la región. Adoptar estas normativas no implica únicamente un ejercicio de cumplimiento, sino una decisión estratégica que impacta directamente en la capacidad institucional para gestionar riesgos, proteger información sensible de clientes y mantener la continuidad operativa en un sector donde la confianza del público y la estabilidad de sus sistemas están asociadas a prácticas de gobierno de la información.

2.1.3.1 **Circular Externa 007 de 2018**

La Circular Externa 007 de 2018, establece los lineamientos para la gestión y clasificación de los activos de información dentro de las organizaciones organización. Esta normativa, emitida por la Superintendencia Financiera de Colombia, define los parámetros obligatorios para la adecuada identificación, categorización y protección de la información según su nivel de sensibilidad, criticidad e importancia para los procesos institucionales.

Tabla N°. 4

Circular Externa 007 de 2018

Estándar/Normativa	Circular Externa 007 de 2018
Planteamiento principal	• Gestión de la ciberseguridad en entidades vigiladas. • Protección de activos digitales críticos. • Prevención y respuesta a incidentes cibernéticos. • Aseguramiento de la continuidad operativa digital.
Relevancia para IFAS	• Define requisitos específicos para protección de infraestructura crítica. • Establece lineamientos para la gestión de riesgos cibernéticos. • Determina responsabilidades en materia de seguridad digital. • Orienta la protección de datos financieros sensibles.
Principales controles relacionados con activos críticos	**Protección de Infraestructura:** • Segmentación de redes críticas • Sistemas de detección y prevención de intrusiones. • Control de acceso basado en roles. • Cifrado de datos sensibles. **Monitoreo y Detección:** • Sistemas SIEM para activos críticos. • Monitoreo 24/7 de infraestructura core del negocio. • Análisis de vulnerabilidades. • Gestión de logs centralizada
Aplicabilidad en instituciones financieras	• Implementación obligatoria para entidades vigiladas. • Requisitos escalonados según tamaño y complejidad. • Fusión con sistemas de gestión de riesgos existentes. • Alineación con estrategias digitales institucionales.
Componentes esenciales	• Gobierno de ciberseguridad. • Gestión de riesgos de ciberseguridad. • Programas de ciberseguridad. • Infraestructura tecnológica. • Monitoreo y detección. • Respuesta a incidentes.
Ventajas	• Específica para sector financiero. • Alineada con estándares. • Internacionales. • Orientación en ciberseguridad. • Clara en requerimientos.

Estándar/Normativa	Circular Externa 007 de 2018
Aplicación practica	• Actualizada a amenazas actuales. • Establecer gobierno de ciberseguridad. • Implementar controles requeridos. • Desarrollar programas de concientización. • Establecer monitoreo continuo. • Crear procedimientos de respuesta. • Reportar a la Superfinanciera.

Nota: la tabla detallada de clasificación de activos de información que contiene los criterios establecidos en dicha circular, incluyendo la identificación del activo, su propietario, la clasificación de confidencialidad, integridad y disponibilidad, así como las medidas de seguridad correspondientes a cada nivel de protección requerido (Supertintendencia Financiera de Colombia, 2018).

2.1.3.2 Circular Externa 029 de 2014

La Circular Externa 029 de 2014, expone los elementos esenciales para la implementación del Sistema de Administración de Riesgo Operativo (SARO). Esta circular, expedida por la Superintendencia Financiera de Colombia como parte de la Circular Básica Jurídica, indica las directrices obligatorias para la identificación, medición, control y monitoreo de los riesgos operativos inherentes a los procesos y actividades institucionales.

Tabla N°. 5

Contexto Circular Externa 029 de 2014

Estándar/Normativa	Circular Externa 029 de 2014
Planteamiento principal	• Sistema de Control Interno. • Gestión de riesgos. • Gobierno corporativo.
Relevancia para IFAS	• Establece marco de control para activos críticos. • Define niveles de responsabilidad en control interno. • Estructura la gestión de riesgos operativos.

Estándar/Normativa	Circular Externa 029 de 2014
	• Garantiza la protección de activos institucionales.
Principales controles relacionados con activos críticos	• Controles Operativos: • Segregación de funciones críticas • Documentación de procesos core del negocio. • Gestión de cambios en sistemas críticos. • Controles duales para operaciones sensibles. • Controles de Acceso: • Gestión de identidades y accesos • Revisión periódica de privilegios. • Control de acceso físico a áreas críticas. • Monitoreo de actividades privilegiadas.
Aplicabilidad en instituciones financieras	• Implementación mandatorio en todas las áreas. • Adaptación según estructura organizacional. • Incorporación con otros sistemas de gestión. • Base para auditorías internas y externas.
Componentes esenciales	• Sistema de Control Interno. • Ambiente de Control. • Gestión de Riesgos. • Actividades de Control. • Información y Comunicación. • Monitoreo.
Ventajas	• Marco de control. • Planteamiento en gestión de riesgos. • Claridad en responsabilidades. • Alineación con gobierno corporativo. • Base para otros sistemas.
Aplicación practica	• Establecer gobierno de ciberseguridad. • Implementar controles requeridos. • Desarrollar programas de concientización. • Establecer monitoreo continuo. • Crear procedimientos de respuesta. • Reportar a la Superfinanciera.

Nota: la tabla detallada que recoge los componentes principales establecidos en la mencionada circular, incluyendo la identificación de eventos de riesgo, factores de riesgo asociados, controles implementados, planes de acción y los indicadores de gestión que permiten evaluar la efectividad

del sistema conforme a los requerimientos regulatorios vigentes (Superintendencia Financiera de Colombia, Circular Externa 029 de 2014, 2014).

2.1.3.3 Circular Básica Jurídica

La Circular Básica Jurídica, expedida por la Superintendencia Financiera de Colombia, desarrolla un análisis de las disposiciones normativas que rigen las operaciones de las entidades vigiladas en el sistema financiero colombiano. Esta Circular establece los lineamientos, procedimientos y obligaciones que deben cumplir las instituciones financieras en materia de gobierno corporativo, protección al consumidor financiero, administración de riesgos y cumplimiento normativo.

Tabla N°. 6

Contexto circular básica jurídica

Estándar/Normativa	Circular Básica Jurídica
Planteamiento principal	• Marco regulatorio • Gobierno corporativo • Gestión de riesgos • Protección al consumidor financiero
Relevancia para IFAS	• Define estructura de gobierno para gestión de activos • Establece responsabilidades en protección de información • Determina requisitos de reportería regulatoria • Orienta la gestión de riesgos asociados a activos críticos
Principales controles relacionados con activos críticos	• Controles de Gobierno: • Políticas de gestión de activos críticos • Estructura de comités especializados • Asignación de responsabilidades • Reportes a la alta dirección • Controles de Cumplimiento: • Monitoreo de requisitos regulatorios • Gestión de reportes obligatorios • Evaluación periódica de cumplimiento • Actualización de políticas y procedimientos
Aplicabilidad en instituciones financieras	• Marco regulatorio base • Base para políticas institucionales • Guía para desarrollo de procedimientos • Referencia para auditorías regulatorias

Estándar/Normativa	Circular Básica Jurídica
Componentes esenciales	• Gobierno Corporativo • Gestión de Riesgos • Control Interno • Revisoría Fiscal • Defensor del Consumidor • Reportes Regulatorios
Ventajas	• Marco regulatorio completo • Claridad normativa • Unificación de requisitos • Orientado en protección al consumidor • Base legal sólida
Aplicación practica	• Implementar estructura de gobierno • Establecer sistemas de gestión de riesgos • Desarrollar controles internos • Cumplir requisitos de reportería • Mantener documentación • Realizar auditorías periódicas

Nota: la tabla detalla los principales componentes establecidos en la Circular Básica Jurídica, incluyendo algunos de los requerimientos específicos, las responsabilidades de los órganos de administración y los mecanismos de control interno que deben implementarse para garantizar la adecuada gestión y transparencia en las operaciones financieras conforme al marco regulatorio vigente (Super financiera de colombia, 2014).

2.1.3.4 Conclusión análisis de normativas locales para instituciones financieras

En conclusión, el análisis de las Circulares Externas 007 de 2018, 029 de 2014 y la Circular Básica Jurídica revela un marco regulatorio evolutivo diseñado específicamente para fortalecer la gestión de riesgos y la protección de activos de información en las instituciones financieras colombianas. Estas normativas establecen directrices precisas y complementarias que abarcan desde los requisitos técnicos de ciberseguridad hasta las responsabilidades de gobierno corporativo, conformando un ecosistema regulatorio que responde a las amenazas emergentes y las particularidades del sector financiero nacional. La Circular 007 de 2018, con su orientación en ciberseguridad, la Circular 029 de 2014, centrada en la gestión de riesgos operativos, y la Circular Básica Jurídica, que establece el marco general de gobernanza, dan los parámetros base que las entidades financieras deben integrar en sus técnicas frente a la protección de activos críticos

objeto de este estudio. El cumplimiento efectivo de estas regulaciones contribuye significativamente a la construcción de un sistema financiero resiliente, confiable y preparado para enfrentar los desafíos y amenazas en un entorno que se encuentra en constante cambio.

2.1.4 *Metodología de Mapeo de Procesos Críticos*

La identificación de procesos core en las entidades financieras representan un ejercicio crítico que requiere un análisis detallado y dedicado de la cadena de valor dentro una entidad. Debido a que estos procesos son el marco operativo que soporta la prestación de servicios financieros y determina la capacidad de la organización para cumplir con sus objetivos estratégicos y obligaciones regulatorias.

El proceso de identificación se desarrolla mediante una metodología estructurada que comienza con el mapeo de la arquitectura empresarial, identificando las interconexiones entre los diferentes componentes del negocio: desde las operaciones transaccionales básicas hasta los servicios financieros más complejos. En este proceso se consideran múltiples dimensiones, incluyendo el impacto en el cliente, la criticidad operativa, los requisitos regulatorios y la correlación tecnológica.

Los procesos core identificados no solo representan las operaciones principales de la institución, sino que también son aquellos cuya interrupción podría generar un impacto importante en la continuidad del negocio, la satisfacción del cliente y el cumplimiento normativo. Por lo tanto, su identificación precisa es esencial para la gestión de riesgos, la asignación de recursos y el diseño de controles adecuados que garanticen la resiliencia operativa de la institución financiera.

En el marco de esta investigación, se han identificado y documentado los procesos considerados críticos y principales para una institución financiera. Es importante destacar que la siguiente catalogación de procesos core representa una base referencial que puede adaptarse según las características específicas de cada entidad. El alcance y la complejidad de estos procesos pueden cambiar dependiendo de diversos factores tales como el tamaño de la institución, su modelo de negocio, los servicios ofrecidos, su presencia geográfica y sus objetivos estratégicos particulares. Los procesos presentados en siguiente tabla se aplica un marco base que puede ser expandido o simplificado según los procesos misionales específicos de cada entidad financiera. Algunas organizaciones podrían requerir procesos complementarios debido a líneas de negocio especializadas.

Tabla N°. 7

Procesos Core generales de entidades financieras

Proceso	Descripción	Componentes Críticos	Activos Relacionados
Core Bancario	Procesos que soportan las operaciones bancarias diarias.	• Gestión de cuentas y saldos. • Procesamiento de transacciones. • Cierre contable diario • Conciliación automática.	• Sistema Core Bancario. • Base de datos transaccional. • Servidores de procesamiento. • Sistemas de respaldo.
Gestión de créditos	Procesos relacionados con el ciclo de vida crediticio.	• Evaluación de riesgo crediticio. • Motor de decisión. • Gestión de desembolsos. • Seguimiento de cartera.	• Sistema de scoring. • Base de datos de clientes. • Sistema de gestión. • documental. • Herramientas de análisis de riesgo.
Sistema de pagos	Procesos que gestionan la transferencia de fondos.	• Procesamiento de ACH. • Transferencias internacionales. • Compensación y liquidación. • Gestión de corresponsales.	• Gateway de pagos. • Sistemas de mensajería SWIFT. • Plataforma de compensación. • Infraestructura de seguridad.
Gestión de tesorería	Procesos de gestión de liquidez e inversiones.	• Gestión de posición de liquidez. • Trading. • Control de riesgos. • Reportería regulatoria.	• Sistema de tesorería. • Plataformas de trading. • Herramientas de análisis. • Sistema de reportes.
Banca Digital	Procesos que soportan los canales digitales.	• Autenticación y autorización. • Procesamiento de transacciones. • Gestión de sesiones • Seguridad digital.	• Plataforma de banca en línea. • Aplicaciones móviles. • Sistemas de autenticación. • Infraestructura de seguridad digital.

Nota: la tabla contiene la catalogación de procesos core base referencial.

2.1.5 *Método de Análisis*

Para garantizar una adecuada gestión de los procesos críticos en una entidad financiera, se ha estructurado un análisis que permite identificar los elementos clave involucrados en cada

operación. A través de las siguientes tablas, se presentan los procesos críticos junto con su descripción, los actores que intervienen, las actividades principales que los componen, los activos críticos que soportan su ejecución y los riesgos asociados que pueden comprometer su integridad, disponibilidad y confidencialidad. Esta información servirá como base para la implementación de controles adecuados y técnicas de mitigación de riesgos, fortaleciendo la seguridad y continuidad del negocio.

2.1.5.1 Proceso Crítico: core bancario

A continuación, se describen los subprocesos asociados a proceso macro Core bancario que nos permite evidenciar un detalle más amplio de la estructura de cada proceso.

Tabla N°. 8

Análisis core bancario

Proceso crítico: core bancario		
Gestión de Cuentas y Saldos	**Descripción**	• Administración de cuentas bancarias.
	Actores Involucrados	• Cliente, sistema de core bancario, oficial de servicio, base de datos de clientes.
	Actividades Principales	• Solicitud de apertura y cierre de cuenta. • Validación de identidad y cumplimiento normativo. • Registro de datos en el sistema bancario. • Consulta y actualización de saldos.
	Activos Críticos	• BD de clientes, sistema de core bancario, App de consulta de saldos.
	Riesgos Asociados	• Robo de identidad, alteración de saldos, acceso no autorizado.
Procesamiento de Transacciones	**Descripción**	• Ejecución de transferencias, pagos, depósitos y retiros, asegurando la integridad de las operaciones.
	Actores Involucrados	• Cliente, cajero/ATM, sistema de pagos, red interbancaria.

Proceso crítico: core bancario		
	Actividades Principales	• Validación de disponibilidad de fondos. • Registro de la transacción en el sistema. • Confirmación al cliente y auditoría del movimiento.
	Activos Críticos	• Sistema de pagos, bases de datos de transacciones, infraestructura de red segura.
	Riesgos Asociados	• Fraude financiero, denegación de servicio, manipulación de registros.
Cierre Contable Diario	**Descripción**	• Consolidación de operaciones del día, conciliación de cuentas y generación de reportes regulatorios.
	Actores Involucrados	• Área contable, sistemas de conciliación, reguladores.
	Actividades Principales	• Revisión y validación de transacciones del día. • Generación de balances y reportes financieros. • Envío de reportes regulatorios y auditoría de registros. • Respaldo y almacenamiento seguro de la información contable.
	Activos Críticos	Sistemas contables, bases de datos transaccionales, servidores de almacenamiento.
	Riesgos Asociados	Inconsistencias en reportes, pérdida de datos, incumplimiento normativo.

Nota: descripción de los subprocesos asociados a proceso macro del Core bancario.

2.1.5.2 Proceso crítico: gestión de créditos

A continuación, en siguiente tabla se describen los subprocesos asociados a proceso macro gestión de créditos que nos permite evidenciar un detalle más amplio de la estructura de cada proceso.

Tabla N°. 9

Análisis gestión de créditos

Proceso Crítico: Gestión de Créditos		
Evaluación de Riesgo Crediticio	**Descripción**	• Análisis del perfil financiero del solicitante para determinar la viabilidad de otorgar crédito.
	Actores Involucrados	• Cliente, analista de crédito, sistema de evaluación de riesgo, burós de crédito.
	Actividades Principales	• Recepción de solicitud de crédito. • Validación de datos y documentos del cliente. • Consulta en burós de crédito. • Análisis de capacidad de pago y perfil de riesgo. • Generación de informe y puntuación de riesgo.
	Activos Críticos	• Base de datos de clientes, sistema de scoring de crédito, APIs de consulta en burós.
	Riesgos Asociados	• Fraude documental, errores en la evaluación, acceso no autorizado a información financiera.
Motor de Decisión	**Descripción**	• Aplicación de reglas automatizadas para la aprobación o rechazo de solicitudes de crédito.
	Actores Involucrados	• Sistema de reglas de negocio, analista de crédito, core bancario.
	Actividades Principales	• Ingreso de solicitud al motor de decisión. • Aplicación de reglas de negocio y criterios de aprobación. • Validación de cumplimiento normativo. • Generación de respuesta automática. • Notificación de aprobación/rechazo al cliente.
	Activos Críticos	• Motor de reglas de negocio, sistemas de aprobación de crédito, algoritmos de decisión.
	Riesgos Asociados	• Sesgo en los criterios de evaluación, vulnerabilidades en la lógica de decisión, manipulación indebida del motor de reglas.

Proceso Crítico: Gestión de Créditos		
Gestión de Desembolsos	**Descripción**	• Administración del proceso de entrega de los fondos aprobados a los beneficiarios.
	Actores Involucrados	• Cliente, sistema de pagos, tesorería, banco corresponsal.
	Actividades Principales	• Validación de aprobación del crédito. • Programación del desembolso. • Transferencia de fondos a la cuenta destino. • Registro contable y generación de evidencias. • Confirmación del desembolso al cliente.
	Activos Críticos	• Sistema de pagos, cuentas de tesorería, registros contables, infraestructura de red bancaria.
	Riesgos Asociados	• Fraude financiero, errores en transferencias, fallos en la conciliación de pagos.

Nota: descripción de los subprocesos asociados a proceso macro gestión de créditos

2.1.5.3 Proceso Crítico: sistema de pagos

A continuación, se describen los subprocesos asociados a proceso macro sistemas de pagos que nos permite evidenciar un detalle más amplio de la estructura de cada proceso.

Tabla N°. 10

Análisis sistemas de pagos

Proceso Crítico: sistema de pagos		
Procesamiento de ACH	**Descripción**	• Gestión de pagos y transferencias interbancarias a través de la Cámara de Compensación Automatizada (ACH).
	Actores Involucrados	• Cliente, banco emisor, banco receptor, operador ACH, sistema de pagos.
	Actividades Principales	• Recepción de órdenes de débito/crédito. • Validación de disponibilidad de fondos. • Envío de instrucciones a la red ACH. • Liquidación y confirmación de transacción. • Generación de reportes y conciliación.
	Activos Críticos	• Sistema de pagos ACH, base de datos de transacciones, infraestructura de red interbancaria.

Proceso Crítico: sistema de pagos		
	Riesgos Asociados	• Retrasos en procesamiento, fraudes en transferencias, fallos en la conciliación de pagos.
Transferencias Internacionales	**Descripción**	• Procesamiento de pagos transfronterizos mediante redes SWIFT o sistemas alternativos.
	Actores Involucrados	• Cliente, banco emisor, banco receptor, red SWIFT, bancos intermediarios.
	Actividades Principales	• Recepción y validación de solicitud de transferencia. • Conversión de divisas y aplicación de tarifas. • Envío de instrucciones vía SWIFT u otro canal. • Verificación de cumplimiento regulatorio. • Confirmación de la transacción y conciliación.
	Activos Críticos	• Sistema de pagos internacionales, red SWIFT, motor de conversión de divisas, registros contables.
	Riesgos Asociados	• Cumplimiento de normativas AML (Anti-Money Laundering), errores en tasas de cambio, fraude en transacciones transfronterizas.
Compensación y Liquidación	**Descripción**	• Proceso de conciliación de operaciones financieras entre instituciones, garantizando la integridad de los pagos.
	Actores Involucrados	• Cámara de compensación, bancos participantes, reguladores, sistema de liquidación.
	Actividades Principales	• Registro y conciliación de operaciones interbancarias. • Cálculo de saldos netos y compensación de pagos. • Validación de cumplimiento de garantías y colaterales. • Liquidación final de fondos entre entidades. • Reporte y auditoría de operaciones liquidadas.
	Activos Críticos	• Sistemas de compensación, bases de datos de transacciones, plataformas de monitoreo de riesgo.
	Riesgos Asociados	• Errores en conciliación, incumplimiento normativo, fallos en la liquidación que afecten estabilidad financiera.
Gestión de Corresponsales	**Descripción**	• Administración de acuerdos con bancos corresponsales para la ejecución de operaciones internacionales.
	Actores Involucrados	• Banco local, bancos corresponsales, área de cumplimiento, reguladores.

Proceso Crítico: sistema de pagos		
	Actividades Principales	• Selección y formalización de acuerdos con corresponsales. • Monitoreo de operaciones y cumplimiento de regulaciones. • Validación de tarifas y costos operativos. • Gestión de riesgos asociados a corresponsales. • Auditoría y optimización de relaciones corresponsales.
	Activos Críticos	• Base de datos de bancos corresponsales, sistemas de monitoreo de riesgo, registros contractuales.
	Riesgos Asociados	• Riesgo reputacional, incumplimiento regulatorio, problemas de liquidez por fallos en corresponsalía.

Nota: describen los subprocesos asociados a proceso macro sistemas de pagos.

2.1.5.4 Proceso crítico: gestión de tesorería

A continuación, se describen los subprocesos asociados a proceso macro gestión de tesorería que nos permite evidenciar un detalle más amplio de la estructura de cada proceso.

Tabla N°. 11

Análisis gestión de tesorería

Proceso Crítico: gestión de tesorería		
Gestión de Posición de Liquidez	**Descripción**	• Administración de la disponibilidad de fondos para cumplir con obligaciones diarias y optimización del uso de recursos financieros.
	Actores Involucrados	• Tesorería, áreas de negocio, sistemas de monitoreo de liquidez, reguladores.
	Actividades Principales	• Toma de decisiones sobre financiamiento. • Ajuste de técnicas para mantener liquidez óptima. • Generación de reportes para la alta gerencia y reguladores.
	Activos Críticos	• Sistema de monitoreo de liquidez, bases de datos de flujo de caja, infraestructura de red bancaria.
	Riesgos Asociados	• Riesgo de iliquidez, incumplimiento de requerimientos regulatorios, errores en cálculos de exposición.
Trading	**Descripción**	• Ejecución de operaciones en mercados financieros para optimizar rentabilidad y cobertura de riesgos.
	Actores Involucrados	• Mesa de dinero, brókers, plataformas de negociación, reguladores.

Proceso Crítico: gestión de tesorería		
	Actividades Principales	• Análisis de mercados y tendencias. • Ejecución de órdenes de compra y venta. • Monitoreo de posiciones y exposición. • Aplicación de técnicas de cobertura. • Reporte y conciliación de operaciones.
	Activos Críticos	• Sistemas de trading, plataformas electrónicas de negociación, bases de datos de posiciones.
	Riesgos Asociados	• Volatilidad del mercado, errores en ejecución de órdenes, incumplimiento normativo.
Control de Riesgos	**Descripción**	• Evaluación y mitigación de riesgos financieros, operacionales y de mercado en la entidad.
	Actores Involucrados	• Área de riesgo, auditoría interna, reguladores, alta gerencia.
	Actividades Principales	• Identificación de riesgos en procesos financieros. • Evaluación de impacto y probabilidad. • Implementación de controles y mitigaciones. • Monitoreo y reporte de métricas de riesgo. • Coordinación con áreas de cumplimiento y auditoría.
	Activos Críticos	• Sistemas de gestión de riesgos, modelos de evaluación, bases de datos de incidentes.
	Riesgos Asociados	• Subestimación de riesgos, fallos en modelos de evaluación, incumplimiento de normativas.
Reportería Regulatoria	**Descripción**	• Generación y presentación de informes financieros y operacionales requeridos por entes supervisores.
	Actores Involucrados	• Área de cumplimiento, reguladores, auditoría interna, sistemas contables.
	Actividades Principales	• Recopilación de datos financieros y operativos. • Validación de consistencia y cumplimiento normativo. • Elaboración de reportes para entes de supervisión. • Presentación de informes en plazos establecidos. • Archivo y respaldo de documentación reportada.
	Activos Críticos	• Sistemas de reportería regulatoria, bases de datos de cumplimiento, infraestructura de almacenamiento de información.
	Riesgos Asociados	• Errores en reportes, sanciones por incumplimiento, inconsistencias en la información presentada.

Nota: descripción de los subprocesos asociados a proceso macro gestión de tesorería.

2.1.5.5 Proceso crítico: banca digital

A continuación, se describen los subprocesos asociados a proceso macro banca digital que nos permite evidenciar un detalle más amplio de la estructura de cada proceso.

Tabla N°. 12

Análisis banca digital

Proceso Crítico: banca digital		
Autenticación y Autorización	**Descripción**	• Validación de identidad de usuarios y asignación de permisos para acceder a sistemas financieros.
	Actores Involucrados	• Cliente, sistema de autenticación, administradores de seguridad, servidores de acceso.
	Actividades Principales	• Registro y gestión de credenciales de usuario. • Implementación de autenticación multifactor (MFA). • Validación de accesos en tiempo real. • Aplicación de controles de autorización por roles. • Monitoreo de intentos de acceso y generación de alertas.
	Activos Críticos	• Servidores de autenticación, bases de datos de usuarios, tokens de acceso, infraestructura de identidad digital.
	Riesgos Asociados	• Robo de credenciales, accesos no autorizados, ataques de fuerza bruta.
Procesamiento de Transacciones	**Descripción**	• Ejecución segura de operaciones financieras, asegurando integridad y disponibilidad.
	Actores Involucrados	• Cliente, sistema de pagos, banco emisor y receptor, redes interbancarias.
	Actividades Principales	• Validación de identidad y autenticación del usuario. • Verificación de saldo y disponibilidad de fondos. • Procesamiento y liquidación de la transacción. • Registro de la operación en bases de datos transaccionales. • Notificación al usuario y generación de evidencia de la operación.
	Activos Críticos	• Plataforma de pagos, bases de datos transaccionales, infraestructura de red bancaria.
	Riesgos Asociados	• Fraude financiero, manipulación de registros, denegación de servicio (DoS).
	Descripción	• Administración segura de sesiones de usuario en plataformas digitales bancarias.

Proceso Crítico: banca digital		
Gestión de Sesiones	**Actores Involucrados**	• Cliente, sistema de autenticación, plataforma web/móvil, servidores de sesión.
	Actividades Principales	• Creación y control de sesiones activas. • Implementación de tiempos de expiración y reautenticación. • Registro de actividad y detección de anomalías. • Cierre automático de sesiones inactivas. • Auditoría y gestión de logs de acceso.
	Activos Críticos	• Servidores de sesión, tokens de sesión, bases de datos de actividad de usuarios.
	Riesgos Asociados	• Secuestro de sesión, ataques de reautenticación, acceso indebido por sesiones no cerradas.
Seguridad Digital	**Descripción**	• Protección de información y sistemas frente a amenazas cibernéticas y fraudes digitales.
	Actores Involucrados	• Área de ciberseguridad, administradores de TI, SOC (Security Operations Center), reguladores.
	Actividades Principales	• Monitoreo de amenazas y detección de intrusos. • Implementación de cifrado en datos sensibles. • Gestión de vulnerabilidades y aplicación de parches. • Pruebas de penetración y auditorías de seguridad. • Capacitación en concienciación de seguridad para empleados.
	Activos Críticos	• Firewalls, SIEM (Security Information and Event Management), herramientas de cifrado, bases de datos de amenazas.
	Riesgos Asociados	• Phishing, ransomware, explotación de vulnerabilidades, filtración de datos.

Nota: descripción de los subprocesos asociados a proceso macro banca digital.

2.1.6 *Análisis de riesgos de los procesos*

El análisis de riesgos en los procesos core de una institución financiera es un elemento primordial para garantizar la continuidad operativa y la protección de los activos críticos. Este proceso sistemático de identificación, evaluación y tratamiento de riesgos debe considerar las amenazas comunes y los desafíos emergentes en un entorno financiero cada vez más digital. El análisis de riesgos se basa en una metodología que permita comprender las vulnerabilidades existentes, evaluar su impacto potencial y establecer controles adecuados para su mitigación. Es

importante que este proceso sea adaptativo y permita cambios según la evolución de las amenazas (Industrial mintset, 2025).

2.1.6.1 Pasos del análisis de riesgos de los procesos

El proceso de análisis de riesgos en entidades financieras requiere identificar, evaluar y gestionar las amenazas potenciales que pueden afectar los activos críticos de la organización. La implementación ordenada de estos pasos es requerida para garantizar que todos los aspectos críticos sean evaluados, así mismo que las medidas de control sean proporcionales a los riesgos identificados.

Esta metodología se desarrolla a través de una serie de etapas asociadas que comienzan con la identificación detallada de puntos de fallo, seguida por una evaluación de los controles existentes, un análisis del impacto en la organización, y finalmente con la definición de planes de contingencia. Cada paso en este proceso está diseñado con el fin de construir sobre los resultados del análisis anterior, creando así un marco de gestión de riesgos que identifica las vulnerabilidades actuales y prepara a la organización para posibles amenazas emergentes. La efectividad de este análisis depende en gran medida de la adaptabilidad de los pasos a cada una de las organizaciones y la capacidad para adaptar el proceso a las características específicas y el contexto operativo de cada institución financiera (Industrial mintset, 2025).

2.1.6.2 Identificación de puntos de fallo

La identificación de puntos de fallo son una de las fases críticas en el marco del análisis de riesgos, donde se examinan sistemáticamente todas las vulnerabilidades, debilidades y condiciones que podrían comprometer la seguridad de los activos (UnnOtec, 2025). Este proceso debe ser metódico abarcando los siguientes elementos definidos en la siguiente tabla:

Tabla N°. 13

Pasos identificación puntos falla Fuente

	Pasos identificación puntos fallo
Vulnerabilidades Técnicas	• Análisis de infraestructura: identificación de configuraciones incorrectas, parches faltantes y debilidades en servidores, redes y aplicaciones. • Escaneo automatizado: utilización de herramientas especializadas para detectar vulnerabilidades conocidas en los sistemas. • Revisión de código: análisis de aplicaciones para detectar defectos de programación que podrían ser explotados. • Pruebas de penetración: simulación de ataques controlados para identificar vulnerabilidades explotables. • Análisis de arquitectura: evaluación de debilidades inherentes al diseño de los sistemas.
Vulnerabilidades Procedimentales	• Análisis de procesos: identificación de pasos redundantes, omisiones o secuencias incorrectas. • Revisión de procedimientos de emergencia: evaluación de la efectividad ante situaciones no previstas. • Análisis de segregación de funciones: verificación de controles duales y principio de mínimo privilegio. • Evaluación de procedimientos de cambio: identificación de debilidades en gestión de cambios. • Análisis de procedimientos de backup y recuperación: detección de fallas en procesos de respaldo.
Vulnerabilidades Organizativas	• Análisis de estructura: identificación de responsabilidades no asignadas o superpuestas. • Evaluación de competencias: detección de brechas en conocimientos y habilidades del personal. • Análisis de comunicación: identificación de fallos en canales de comunicación críticos. • Evaluación de cultura de seguridad: medición de la concienciación y comportamiento del personal. • Análisis de dependencias de terceros: evaluación de riesgos introducidos por proveedores.

Pasos identificación puntos fallo	
Puntos Únicos de Fallo (SPOF)	• Identificación de componentes críticos: determinación de elementos sin redundancia. • Análisis de dependencias: mapeo de relaciones entre sistemas para identificar cascadas de fallos. • Evaluación de alta disponibilidad: verificación de mecanismos de continuidad y tolerancia a fallos. • Análisis de concentración de conocimiento: Identificación de personas clave sin respaldo. • Evaluación de proveedores únicos: detección de dependencias críticas de proveedores específicos.
Metodologías de Identificación	• Análisis de modo y efecto de fallas (FMEA): evaluación sistemática de cómo pueden fallar los componentes. • Análisis de árbol de fallos (FTA): identificación deductiva de combinaciones que pueden causar fallos. • Análisis de causa raíz (RCA): aplicado a incidentes previos para identificar vulnerabilidades sistemáticas. • Modelado de amenazas: identificación de vulnerabilidades desde el punto de vista del atacante. • Revisiones por pares: evaluación cruzada por expertos para detectar puntos ciegos.
Documentación y Priorización	• Registro detallado: documentación estructurada de cada punto de falla identificado. • Clasificación: categorización según tipo, ubicación y potencial impacto. • Evaluación de criticidad: valoración basada en facilidad de explotación e impacto potencial. • Mapeo de controles: identificación de medidas existentes que mitigan cada vulnerabilidad. • Priorización: ordenamiento según nivel de riesgo para planificar remediación.
Obs. especiales entidades financieras	• Análisis de interfaces: evaluación de puntos de conexión con sistemas externos (pasarelas de pago, corresponsales). • Evaluación de cumplimiento: verificación de adherencia a requisitos regulatorios. • Análisis de segregación: evaluación de la separación entre ambientes productivos y no productivos.

Nota: Pasos identificación puntos falla Fuente: *(UnnOtec, 2025)*

2.1.7 *Evaluación de controles existentes en la organización*

La evaluación de controles existentes es necesaria en el análisis de procesos críticos de la entidad financiera. Esta etapa permite determinar la efectividad, madurez y capacidad de los

mecanismos de protección implementados actualmente para proteger la integridad, disponibilidad y confidencialidad de los activos críticos que soportan las operaciones del negocio.

2.1.7.1 Metodología de Evaluación de controles

En el marco del análisis de seguridad de la información y gestión de riesgos operativos en entidades financieras, a continuación se encuentra la metodología para la evaluación de controles, componente crítico para garantizar la protección de los activos de información. Esta metodología establece un esquema medible que permite identificar brechas de seguridad en los controles implementados y priorizar las acciones correctivas según el nivel de exposición al riesgo, optimizando así la asignación de recursos y fortaleciendo el sistema de protección en concordancia con los requerimientos regulatorios y las mejores prácticas de la industria financiera (Auditool, 2025).

2.1.7.1.1 Inventario de Controles

Se realiza un levantamiento de todos los controles existentes asociados a cada proceso crítico, clasificándolos según su naturaleza. A continuación, la tabla 14 presenta una clasificación de controles de seguridad según su naturaleza funcional. Esta taxonomía facilita una habilidad de defensa en profundidad que aborda las vulnerabilidades en múltiples capas de protección.

Tabla N°. *14*

Clasificación controles según su naturaleza Fuente

Clasificación controles según su naturaleza	
Controles Preventivos	Diseñados para evitar la materialización de riesgos.
Controles Detectivos	Orientados a identificar eventos de riesgo una vez ocurridos.
Controles Correctivos	Enfocados en mitigar los impactos tras la materialización de un riesgo.
Controles Disuasivos	Destinados a desalentar acciones que puedan materializar riesgos

Nota: clasificación de controles según su naturaleza *(NIST SP 800-53, 2020)*

2.1.7.1.2 Criterios de evaluación controles

El presente marco de evaluación de controles ha sido desarrollado tomando como base las mejores prácticas internacionales en gestión de seguridad de la información y riesgo operativo, incorporando elementos de los estándares ISO 27001, COBIT, el Marco de Ciberseguridad del NIST y las recomendaciones específicas de la Superintendencia Financiera de Colombia en sus circulares externas. Los criterios seleccionados representan dimensiones complementarias que

permiten una valoración de cada control, facilitando así la identificación de oportunidades de mejora y la priorización de acciones correctivas.

Tabla N°. *15*

Criterios de evaluación controles Fuente

Criterio	Descripción	Escala de Valoración
Diseño	Evaluación de la estructura y concepción del control.	1 (Deficiente) a 5 (Óptimo)
Implementación	Grado en que el control se ha puesto en práctica.	1 (No implementado) a 5 (Totalmente implementado)
Efectividad	Capacidad del control para mitigar el riesgo específico.	1 (Inefectivo) a 5 (Altamente efectivo)
Eficiencia	Relación entre recursos empleados y resultados obtenidos.	1 (Ineficiente) a 5 (Altamente eficiente)
Cumplimiento Normativo	Conformidad con regulaciones aplicables.	1 (Incumplimiento) a 5 (Conformidad total)
Automatización	Nivel de automatización vs. intervención manual.	1 (Manual) a 5 (Totalmente automatizado)
Madurez	Grado de evolución y refinamiento del control.	1 (Incipiente) a 5 (Optimizado)

Nota: A continuación, en la siguiente tabla se identifica la valoración conforme a los siguientes criterios (ISO/IEC, 2022) (COBIT, 2019) (NIST, Cybersecurity Framework | NIST, 2013).

2.1.7.1.3 Esquema matriz por riesgo

A continuación, en la siguiente tablase presenta un esquema general de levantamiento de riesgos el cual debería ser diligenciado por cada uno de los riesgos identificados.

Tabla N°. 16

Esquema matriz por riesgo

Criterio	Campo
Proceso Critico	Nombre proceso
Riesgo Asociado	Riesgo 1
Control Existente	Control 1
Descripción del control	Descripción
Tipo de control	Tipo

Criterio	Campo
Diseño	1-5
Implementación	1-5
Efectividad	1-5
eficiencia	1-5
Cumplimiento	1-5
Automatización	1-5
Madurez	1-5
Valoración Global	Promedio
Brecha identificada	Descripción

Nota: esquema de levantamiento de riesgo.

2.1.7.1.4 Matriz de evaluación de controles

Para cada proceso crítico se desarrolla una matriz que relaciona los riesgos identificados con los controles existentes. Estableciendo una evaluación del nivel de cobertura que los controles existentes lo que proporciona una valoración frente a los riesgos identificados en la siguiente tabla.

Tabla N°. *17*

Evaluación de nivel de cobertura del riego

Nivel de Cobertura	Descripción	Rango de Valoración Global
Óptimo	El control mitiga completamente el riesgo.	4.5 - 5.0
Adecuado	El control mitiga significativamente el riesgo	3.5 - 4.4
Parcial	El control mitiga moderadamente el riesgo.	2.5 - 3.4
Limitado	El control mitiga mínimamente el riesgo.	1.5 - 2.4
Insuficiente	El control no mitiga efectivamente el riesgo.	1.0 - 1.4

Nota: cuadro descriptivo nivel de cobertura

2.1.7.1.5 Análisis de Brechas frente a los controles

Una vez evaluados los controles existentes, se identifican las brechas entre el nivel de protección actual y el nivel requerido para una gestión óptima de riesgos. A continuación, en la siguiente tabla se encuentra una descripción de las brechas más importantes a evaluar (ISO/IEC, 2022).

Tabla N°. *18*

Análisis de brechas autor Fuente

Análisis de brechas	
Brechas de Diseño	Deficiencias en la concepción o estructura del control.
Brechas de Implementación	Falencias en la puesta en práctica del control.
Brechas de Efectividad	Insuficiencia en la capacidad del control para mitigar el riesgo.
Brechas Normativas	Incumplimiento de requisitos regulatorios aplicables.
Brechas de Cobertura	Riesgos sin controles asociados o con controles insuficientes

Nota: análisis de la descripción de brechas *(ISO/IEC 27002:2022, 2022)*

2.1.7.1.6 Ejemplo de aplicación de control a proceso critico

A continuación, se ejecuta un ejemplo práctico que permite evidenciar de forma más sencilla los pasos descritos con anterioridad.

- **Proceso Crítico:** aprobación de Créditos Corporativos.
    - **Ejercicio 1:** riesgo 1 fraude en la documentación del solicitante

Tabla N°. 19

Ejercicio riesgo 1 fraude en la documentación del solicitante

Riesgo 1	
Criterio	**Descripción**
Proceso Critico	Aprobación de Créditos Corporativos
Riesgo Asociado	Fraude en la documentación del solicitante
Control Existente	Verificación documental
Descripción del control	Revisión manual de documentos contra fuentes originales.
Tipo de control	Preventivo
Diseño	4
Implementación	3
Efectividad	3
eficiencia	2

Riesgo 1	
Criterio	**Descripción**
Cumplimiento	4
Automatización	1
Madurez	3
Valoración Global	2.9
Brecha identificada	Baja automatización y eficiencia

Nota: ejercicio 1 fraude en la documentación del solicitante

- **Ejercicio 1:** riesgo 2 fraude en la documentación del solicitan

Tabla N°. 20

Riesgo 2 Incumplimiento políticas de riego crediticio

Riesgo 2	
Criterio	**Descripción**
Proceso Critico	Aprobación de Créditos Corporativos.
Riesgo Asociado	Incumplimiento de políticas de riesgo crediticio
Control Existente	Comité de Aprobación
Descripción del control	Evaluación colegiada de solicitudes que exceden límites predefinidos
Tipo de control	Preventivo
Diseño	5
Implementación	4
Efectividad	4
eficiencia	3
Cumplimiento	5
Automatización	2
Madurez	4

Riesgo 2	
Criterio	**Descripción**
Valoración Global	3.9
Brecha identificada	Proceso con tiempos de respuesta extendidos

Nota: incumplimiento de riesgo crediticio.

- **Ejercicio 1:** riesgo 3 concentración excesiva de cartera

Tabla N°. 21

Riego 3 Concentración excesiva de cartera

Riesgo 3	
Criterio	**Descripción**
Proceso Critico	Aprobación de Créditos Corporativos.
Riesgo Asociado	Concentración excesiva de cartera
Control Existente	Sistema de alertas de concentración
Descripción del control	Notificaciones automáticas cuando se supera umbral por sector económico.
Tipo de control	Detectivo
Diseño	3
Implementación	2
Efectividad	2
eficiencia	4
Cumplimiento	3
Automatización	4
Madurez	2
Valoración Global	2.9
Brecha identificada	Implementación parcial y baja efectividad

Nota: concentración excesiva de cartera.

2.1.7.1.7 Conclusiones y recomendaciones ejemplo de aplicación.

Las siguientes conclusiones y recomendaciones son de carácter explicativo, basadas en los criterios definidos para el ejemplo 1 y los tres riesgos asociados.

- Conclusiones:
    - La mayoría de los controles evaluados presenta un nivel de cobertura "Parcial" frente a los riesgos identificados.
    - Los controles preventivos muestran mayor madurez, que el detectivo.
    - Los procesos de mayor criticidad muestran una cobertura de controles insuficiente en relación con su nivel de riesgo.
- Recomendaciones para el fortalecimiento de controles ejemplo de aplicación
    - **Priorización de mejoras**: enfocar esfuerzos en el fortalecimiento de controles asociados a los procesos de mayor criticidad y con brechas significativas.
    - **Automatización progresiva**: implementar un programa de automatización para controles manuales de alta frecuencia.
    - **Revisión de diseño**: rediseñar controles con valoración de diseño inferior a 3.0.
    - **Monitoreo continuo**: establecer indicadores de desempeño para evaluar la efectividad de los controles en el tiempo.
    - **Capacitación**: fortalecer la formación del personal en la ejecución y monitoreo de controles.

Esta evaluación contribuye a los fundamentos para el diseño e implementación de un plan de acción orientado a fortalecer el sistema de control interno, garantizando una gestión adecuada de los riesgos asociados a los procesos críticos en una entidad financiera.

2.1.8 *Análisis de impacto en el negocio (BIA)*

El Análisis de Impacto en el Negocio (BIA) es una metodología estructurada que permite identificar y evaluar los efectos que la interrupción de los procesos críticos tendría sobre la operación, finanzas y reputación de una entidad financiera. El marco conceptual del Análisis de Impacto en el Negocio (BIA) (BSI, 2019) presentado se ha desarrollado con base en los estándares internacionales de gestión de continuidad de negocio, principalmente la norma ISO 22301, complementada con las directrices específicas de la norma NIST SP 800-34 (SP 800-34) y las recomendaciones del Business Continuity Institute (The Business Continuity Institute (BCI, 2025).

Es necesario incorporar requerimientos establecidos por la Superintendencia Financiera de Colombia en su Circular Externa 042 de 2012, que define los requisitos mínimos de seguridad y calidad para la gestión de la información, incluyendo las disposiciones específicas para entidades financieras en materia de continuidad operativa.

- Objetivos del Análisis de Impacto:
    - Identificar los procesos críticos de una entidad financiera y sus relaciones internas entre cada uno de ellos.
    - Determinar los impactos cualitativos y cuantitativos de la interrupción de estos procesos.
    - Establecer prioridades de recuperación y tiempos máximos tolerables de interrupción.
    - Identificar recursos mínimos necesarios para la operación y recuperación de procesos.
    - Sentar las bases para el desarrollo de técnicas de continuidad y planes de recuperación.

2.1.8.1 Metodología de evaluación

La metodología de evaluación del análisis de impacto en el negocio (BIA), se enfoca principalmente en la identificación y valoración objetiva de los procesos críticos una entidad financiera. El marco metodológico presentado define lineamientos generales que permitan determinar con precisión las consecuencias operativas, financieras y reputacionales derivadas de posibles interrupciones, así como los tiempos máximos tolerables de indisponibilidad; lo anterior entendiendo que es necesario para la construcción de esquemas de continuidad y la asignación eficiente de recursos de protección según el verdadero nivel de criticidad de cada proceso de una organización.

- **Identificación de Procesos Críticos**: se evalúa cada proceso de la entidad para determinar su criticidad en función de:
    - Impacto directo en los objetivos estratégicos
    - Relación con la generación de ingresos

- Cumplimiento de obligaciones regulatorias
- Servicio a clientes estratégicos
- Interdependencias con otros procesos críticos

- **Parámetros de evaluación de impacto:** para cada proceso crítico identificado, se evalúan los siguientes parámetros:

Tabla N°. 22

Parámetros de evaluación de impacto

Parámetro	Descripción	Escala de Medición
Impacto Financiero	Pérdidas económicas directas e indirectas	• Bajo (<$X Cop) • Medio ($XX Cop -$XX Cop) • Alto ($XX Cop -$X Cop) ▪ Crítico (>$X Cop)
Impacto Operacional	Afectación a las operaciones de la entidad	Bajo, Medio, Alto, Crítico
Impacto Reputacional	Daño a la imagen y confianza institucional	Bajo, Medio, Alto, Crítico
Impacto Regulatorio	Incumplimientos normativos y sanciones potenciales	Bajo, Medio, Alto, Crítico
Impacto en Clientes	Afectación a servicios y satisfacción de clientes	Bajo, Medio, Alto, Crítico

Nota: evaluación de impacto.

- **Métricas Temporales Críticas:** se establecen los siguientes parámetros temporales para cada proceso (Work, 2015):
  - **RTO (Recovery Time Objective)**: tiempo máximo tolerable de interrupción.
  - **RPO (Recovery Point Objective)**: pérdida máxima tolerable de datos.
  - **MTD (Maximum Tolerable Downtime)**: tiempo máximo absoluto de interrupción antes de daños irreparables.

- **WRT (Work Recovery Time)**: tiempo necesario para recuperar operaciones normales tras restaurar sistemas.

2.1.8.2 Matriz de Análisis de impacto en el negocio (BIA)

La Matriz de Análisis de Impacto en el Negocio (BIA) es la herramienta central de documentación que presenta los resultados del proceso evaluativo de criticidad de procesos la cual se puede identificar con los principales ítems en la siguiente tabla. Es un instrumento, basado en las mejores prácticas del estándar ISO 22301 y las directrices específicas de la Circular Externa 042 de 2012 de la Superintendencia Financiera de Colombia, la cual facilita la toma de decisiones estratégicas que permitan la priorización de recursos en materia de continuidad del negocio de una entidad financiera (Norma ISO 22301 BSI, 2019).

Tabla N°. *23*

Matriz de Análisis de impacto en el negocio (BIA) Fuente

Proceso crítico	**Descripción**	**Nivel de criticidad**	**Impacto financiero**	**Impacto operacional**	**Impacto reputacional**	**Impacto regulatorio**	**Impacto en clientes**	**RTO**	**RPO**	**MTD**	**Recursos críticos**	**Dependencias**
Nombre proceso	Descripción	Nivel	Impacto	Impacto	Impacto	Impacto	Impacto	Tiempo	Tiempo	Tiempo	Recursos	Dependencias

Nota: matriz de análisis de impacto*(Norma ISO 22301 BSI, 2019)*

2.1.8.3 Clasificación de Criticidad de Procesos

En esta sección se encuentra las herramientas para categorizar los procesos organizacionales según su relevancia estratégica y operativa. Esta taxonomía, desarrollada con base en los lineamientos del Disaster Recovery Institute International (DRI International) y adaptada a los requerimientos específicos de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia en su Parte I (Super financiera de colombia, 2014), establece niveles diferenciados que reflejan el impacto potencial que la interrupción de cada proceso tendría sobre las operaciones, finanzas y reputación de la entidad. A continuación, en la siguiente tabla se presenta el esquema

de clasificación según su criticidad, considerando el impacto acumulativo en todas las dimensiones evaluadas:

Tabla N°. *24*

Clasificación de criticidad de procesos Fuente

Nivel de Criticidad	Descripción	Prioridad de Recuperación
Crítico	Procesos vitales para la supervivencia de la organización	Inmediata (0-4 horas)
Alto	Procesos esenciales que no pueden interrumpirse por más de 24 horas	Alta (4-24 horas)
Medio	Procesos importantes que pueden tolerarse interrupciones de hasta 72 horas	Media (24-72 horas)
Bajo	Procesos que pueden interrumpirse por más de 72 horas sin impactos severos	Baja (>72 horas)

Nota: clasificación de criticidad *(DRI International)*

2.1.8.4 Ejemplos de aplicación impacto de proceso critico

A continuación, se documenta el nivel de impacto y nivel de criticidad de dos procesos críticos de una entidad financiera de manera general asociado en los siguientes ejemplos:

- **Ejemplo 1:** proceso de gestión de pagos interbancarios

Tabla N°. 25

Ejemplo 1: proceso de gestión de pagos interbancarios

Proceso Crítico	Gestión de Pagos Interbancarios
Descripción	Proceso que gestiona transferencias de alto valor entre instituciones financieras
Nivel de Criticidad	Crítico
Impacto Financiero	Crítico ($2M diarios)
Impacto Operacional	Crítico
Impacto Reputacional	Alto
Impacto Regulatorio	Crítico
Impacto en Clientes	Crítico
RTO	2 horas

Proceso Crítico	Gestión de Pagos Interbancarios
RPO	0 (zero data loss)
MTD	4 horas
Recursos Críticos	Sistema de pagos SWIFT, Servidor principal, Personal especializado, Conexiones de red redundantes.
Dependencias	Proceso de autenticación, Sistema de validación, Liquidez interbancaria.

Nota: proceso que gestiona transferencias de alto valor entre instituciones financieras

- **Análisis de impacto por tiempo de interrupción:** los valores presentados en la siguiente tabla son de referencia y generales no representan un valor real, si no una adaptación para el ejercicio.

Tabla N°. 26

Análisis de impacto por tiempo de interrupción

Tiempo de Interrupción	Impacto Financiero	Impacto Operacional	Impacto Reputacional	Impacto Regulatorio	Acciones Requeridas
0-2 horas	$170Cop	Acumulación de transacciones pendientes	Mínimo	Notificación preventiva al regulador	Activación de comunicación con clientes
2-4 horas	$340Cop	Imposibilidad de cumplir con liquidaciones diarias	Moderado, primeras quejas de clientes	Reporte obligatorio de incidente	Activación de procedimientos alternos
4-24 horas	$2MCop	Paralización de operaciones relacionadas	Severo, posible cobertura mediática	Supervisión directa del regulador	Activación del Plan de Recuperación de Desastres
>24 horas	>$2MCop + penalizaciones	Afectación sistémica a otras operaciones	Crítico, pérdida de confianza institucional	Intervención regulatoria, multas	Activación del BIA corporativo

Nota: análisis de impacto de interrupción

- **Ejemplo 2:** proceso de Aprobación de Créditos Corporativos

Tabla N°. 27

Ejemplo 2 :proceso de a probación de créditos corporativos

Proceso Crítico	**Aprobación de Créditos Corporativos**
Descripción	Evaluación y aprobación de solicitudes de financiamiento a empresas
Nivel de Criticidad	Alto
Impacto Financiero	Alto ($500M cop diarios)
Impacto Operacional	Alto
Impacto Reputacional	Medio
Impacto Regulatorio	Medio
Impacto en Clientes	Alto
RTO	8 horas
RPO	4 horas
MTD	24 horas
Recursos Críticos	Sistema de scoring crediticio, Base de datos de clientes, Comité de crédito, Analistas de riesgo
Dependencias	Proceso de validación de información, Sistema de evaluación financiera, Servicio de verificación documental

Nota: Evaluación y aprobación de solicitudes de financiamiento a empresas.

- **Análisis de Impacto por Tiempo de Interrupción**: los valores presentados siguiente tabla son de referencia y generales no representan un valor real si no una adaptación para el ejercicio.

Tabla N°. 28

Análisis de impacto por tiempo de interrupción

Tiempo de Interrupción	**Impacto Financiero**	**Impacto Operacional**	**Impacto Reputacional**	**Impacto Regulatorio**	**Acciones Requeridas**
0-8 horas	$170 Cop	Retraso en el procesamiento de solicitudes	Mínimo	Ninguno	Comunicación preventiva a clientes afectados
8-24 horas	$500 Cop	Acumulación significativa de solicitudes	Moderado, clientes	Registro del incidente	Activación de procedimientos

Tiempo de Interrupción	Impacto Financiero	Impacto Operacional	Impacto Reputacional	Impacto Regulatorio	Acciones Requeridas
			estratégicos afectados		manuales de evaluación
24-72 horas	$1.5MCop	Imposibilidad de cumplir con tiempos comprometidos	Alto, posible pérdida de oportunidades de negocio	Notificación obligatoria	Asignación de recursos necesarios para recuperación
>72 horas	>$3MCop	Pérdida de clientes potenciales	Crítico, afectación de relaciones comerciales	Posibles sanciones por incumplimiento	Revisión y reestructuración de procesos

Nota: Análisis de impacto de interrupción.

- **Análisis de Interdependencias:** se identifican las relaciones y dependencias entre los procesos críticos, determinando el efecto cascado que la interrupción de un proceso puede tener sobre otros:
- **Recursos Críticos para la Continuidad**: para cada proceso crítico se identifican.

Tabla N°. 29

Recursos críticos para la continuidad

Recursos críticos para la continuidad	
Recursos tecnológicos	• Sistemas de información. • Infraestructura de red y comunicaciones. • Servidores y bases de datos. • Aplicaciones específicas.
Recursos humanos	• Personal clave con conocimientos especializados. • Roles críticos para la operación. • Equipos de respuesta y recuperación.
Recursos físicos	• Instalaciones primarias y alternas. • Equipamiento especializado. • Documentación crítica.
Proveedores y servicios externos	• Servicios críticos tercerizados. • Proveedores de los que depende la operación. • Acuerdos de nivel de servicio.

Nota: Recursos críticos para la continuidad

2.1.8.5 Estrategias de continuidad recomendadas sobre los ejemplos planteados

La siguiente tabla presenta basado en el análisis de impacto, una propuesta de técnicas diferenciadas según el nivel de criticidad.

Tabla N°. 30

Estrategias de continuidad para los ejemplos planteados

Estrategias de continuidad	
Para Procesos Críticos	• Redundancia completa de sistemas e infraestructura. • Personal alternativo capacitado para asumir funciones. • Sitios alternos de operación totalmente equipados. • Acuerdos de nivel de servicio con tiempos de respuesta inferiores al RTO. • Pruebas frecuentes de recuperación (trimestrales).
Para Procesos de Alta Criticidad	• Redundancia parcial de sistemas críticos. • Procedimientos alternos manuales documentados. • Capacidad de operación remota o distribuida. • Pruebas semestrales de recuperación.
Para Procesos de Media Criticidad	• Capacidad de procesamiento por lotes en sistemas alternos. • Procedimientos manuales temporales. • Pruebas anuales de recuperación.

Nota: análisis de impacto

2.1.8.6 Conclusiones y recomendaciones del ejercicio practico

- Conclusiones
    - Los procesos analizados clasifican como "Críticos" y requieren medidas de continuidad.
    - Los impactos financieros potenciales por interrupción de procesos críticos deberán ser estimados conforme a la tabla definida por días.
    - Los procesos con mayor relación representan riesgos sistémicos que deben ser prioritarios.
- Recomendaciones estratégicas del ejercicio práctico

- **Inversión Prioritaria**: asignar recursos para fortalecer la resiliencia de los procesos críticos identificados
- **Redundancia Sistémica**: implementar arquitecturas redundantes para los sistemas que soportan procesos críticos
- **Automatización de Recuperación**: desarrollar capacidades de recuperación automatizada para reducir los RTO
- **Capacitación Cruzada**: formar personal alternativo capaz de ejecutar funciones críticas
- **Revisión Periódica**: actualizar el BIA semestralmente o ante cambios significativos al interno de la organización

Este análisis de impacto establece la base para la construcción de un plan de continuidad del negocio, que permita a la entidad financiera responder eficazmente ante eventos disruptivos, minimizando el impacto operacional, financiero y reputacional.

2.1.9 *Definición de planes de contingencia*

Los planes de contingencia representan un conjunto de procedimientos y acciones que permiten a una entidad financiera responder de manera oportuna y eficaz ante eventos que le afecten en su operación. Estos planes representan la materialización operativa de las tecnicas de continuidad se definen en el análisis de impacto en el negocio (BSI, 2019) y la evaluación de controles existentes previamente desarrollados.

- Objetivos de los Planes de Contingencia
  - Establecer procedimientos claros para la respuesta inmediata ante incidentes
  - Minimizar el tiempo de interrupción de los procesos críticos
  - Reducir el impacto operacional, financiero y reputacional de los eventos disruptivos
  - Asegurar la continuidad de los servicios esenciales a clientes y stakeholders
  - Cumplir con los requisitos regulatorios en materia de continuidad del negocio
  - Preservar la confianza de clientes, inversionistas y reguladores

2.1.9.1 Estructura General del Plan de Contingencia

La Estructura General del Plan de Contingencia es un marco que permite organizar las medidas preventivas, reactivas y de recuperación ante posibles incidentes que se puedan presentar en la organización. A continuación, se presentan los componentes para la construcción del plan de contingencia (IBM, Ejemplos de planes de contingencia empresarial: prepararse para lo inesperado | IBM, 2023).

2.1.9.1.1 Componentes Principales

En la siguiente tabla se define los componentes principales que debería contener un plan de contingencia para procesos críticos.

Tabla N°. 31

Componentes principales del plan de contingencia

Componente	Descripción
Alcance	Delimitación precisa del proceso crítico cubierto por el plan.
Objetivos	Resultados esperados de la implementación del plan.
Escenarios de Activación	Circunstancias específicas que desencadenan el plan.
Roles y Responsabilidades	Asignación clara de funciones durante la contingencia.
Procedimientos de Activación	Pasos secuenciales para iniciar la respuesta.
Procedimientos de Operación Alterna	Métodos para mantener la funcionalidad mínima.
Procedimientos de Recuperación	Acciones para restaurar la operación normal.
Estrategia de Comunicación	Protocolos de notificación a stakeholders internos y externos.
Recursos Necesarios	Elementos requeridos para ejecutar el plan.

Componente	Descripción
Criterios de Desactivación	Condiciones para retornar a la operación normal.
Mecanismos de Prueba	Metodología para validar la efectividad del plan.
Procedimientos de Actualización	Proceso para mantener el plan vigente.

Nota: información tomada de las siguientes fuentes (IBM, Ejemplos de planes de contingencia empresarial: prepararse para lo inesperado | IBM, 2023)

2.1.9.1.2 Niveles de activación plan de contingencia

En la siguiente tabla se establecen los diferentes niveles de activación según la severidad del incidente presentado.

Tabla N°. 32

Niveles de activación plan de contingencia

Nivel	Descripción	Ejemplos de Escenarios	Autoridad de Activación
Nivel 1 - Alerta	Incidente menor que no afecta significativamente la operación.	Falla temporal de sistemas no críticos, indisponibilidad parcial de recursos.	Jefe de Área
Nivel 2 - Contingencia Operativa	Afectación moderada que requiere activación de procedimientos alternos.	Falla extendida de sistemas de soporte, indisponibilidad de personal clave.	Gerente de Área
Nivel 3 - Crisis	Interrupción severa que compromete múltiples procesos críticos.	Desastres naturales localizados, ciberataques, fallas mayores en infraestructura.	Comité de Crisis
Nivel 4 - Desastre	Evento catastrófico que amenaza la continuidad del negocio.	Destrucción de instalaciones principales, eventos de	CEO/Comité Ejecutivo

Nivel	Descripción	Ejemplos de Escenarios	Autoridad de Activación
		impacto regional, pandemias.	

Nota: información tomada de las siguientes fuentes**:** *(IBM, Ejemplos de planes de contingencia empresarial: prepararse para lo inesperado | IBM, 2023)*

2.1.9.2 Ejemplo práctico: plan de contingencia para proceso de gestión de pagos Interbancarios

A continuación, se encuentra la información general para el ejemplo práctico como insumo base para la construcción de el plan de contingencia para una entidad bancaria.

Tabla N°. 33

Información general plan de contingencia

Plan de contingencia para proceso de gestión de pagos Interbancarios	
Nombre del Proceso	Gestión de Pagos Interbancarios
Nivel de Criticidad	Crítico
RTO	2 horas
RPO	0 (zero data loss)
MTD	4 horas
Propietario del Plan	Director de Operaciones Financieras
Custodio del Plan	Jefe de Transferencias Interbancarias
Fecha de Última Actualización	15/02/2025
Versión	3.2

Nota: contiene información básica de actualización plan de contingencia

- **Escenarios de Activación plan de contingencia**

Los Escenarios de activación del plan de contingencia representan situaciones críticas previamente identificadas que pueden comprometer la operatividad normal de los sistemas de pago interbancario. Cada escenario ha sido definido según su naturaleza, estableciendo niveles de activación que determinan la urgencia y alcance de la respuesta necesaria, así como una evaluación del impacto potencial sobre las operaciones financieras. Esta matriz de escenarios permite a la

organización implementar respuestas proporcionadas y eficaces, facilitando la toma de decisiones durante situaciones de crisis y garantizando la continuidad de los servicios financieros core. La siguiente tabla presenta un ejemplo ilustrativo sobre cómo construir un esquema de contingencia con la definición desde la nomenclatura hasta la definición del impacto potencial.

Tabla N°. 34

Planteamiento de escenarios plan de contingencia ejemplo

Escenario	Descripción	Nivel de Activación	Impacto Potencial
ESC-PI-01	Falla del sistema principal de procesamiento SWIFT	Nivel 2	Imposibilidad de procesar transferencias interbancarias de alto valor
ESC-PI-02	Caída de enlaces de comunicación con redes financieras	Nivel 2	Incapacidad para enviar/recibir mensajes de autorización
ESC-PI-03	Indisponibilidad del personal clave	Nivel 1	Retrasos en aprobaciones y resolución de excepciones
ESC-PI-04	Ataque cibernético a los sistemas de pago	Nivel 3	Compromiso de integridad/disponibilidad de la infraestructura de pagos
ESC-PI-05	Destrucción/inaccesibilidad del centro de procesamiento principal	Nivel 4	Pérdida total de capacidad operativa en la ubicación principal

Nota: planteamiento de escenarios plan de contingencia a modo de ejemplo

- **Roles y responsabilidades en ejecución plan de contingencia**: en la siguiente tabla se definen los roles y responsabilidades para la ejecución del plan de contingencia.

Tabla N°. 35

Roles y responsabilidades ejecución plan de contingencia

Rol	Responsable Titular	Responsable Alterno	Responsabilidades Clave
Coordinador de Contingencia	Jefe de Transferencias Interbancarias	Supervisor de Operaciones	Activar/coordinar el plan, reportar avances al Comité de Crisis.

Rol	Responsable Titular	Responsable Alterno	Responsabilidades Clave
Equipo de Operación Alterna	Especialistas de Transferencias (4)	Analistas de Operaciones Financieras (4)	Ejecutar procedimientos alternos de procesamiento de pagos.
Equipo de Recuperación Tecnológica	Especialistas de Infraestructura (2)	Ingenieros de Sistemas (2)	Restablecer sistemas y conexiones afectadas.
Enlace con Entidades Externas	Gerente de Relaciones Interbancarias	Jefe de Corresponsalía	Comunicación con bancos corresponsales y entidades del sistema financiero.
Oficial de Comunicaciones	Gerente de Comunicación Corporativa	Coordinador de Comunicación Interna	Gestionar comunicaciones oficiales a stakeholders.

Nota: definición de definen los roles y responsabilidades para la ejecución del plan de contingencia.

- Procedimientos de activación plan de contingencia: la siguiente tabla presenta un esquema general del procedimiento para la activación del plan de contingencia.

Tabla N°. 36

Procedimientos de activación plan de contingencia

Procedimientos de activación plan de contingencia	
Detección y notificación	• Identificación del incidente por monitoreo automático o reporte manual. • Notificación al Coordinador de Contingencia. • Evaluación preliminar del impacto y clasificación del nivel de activación.
Declaración de contingencia	• Validación de criterios de activación según nivel. • Declaración formal de la contingencia por la autoridad. correspondiente. • Registro de la hora exacta de declaración (T0).

Procedimientos de activación plan de contingencia	
Convocatoria de equipos de respuesta	• Activación de la cadena de llamadas o sistema de notificación automatizado. • Confirmación de disponibilidad de los recursos humanos requeridos. • Instrucciones para el desplazamiento hacia sitios alternos si aplica.
Establecimiento de centro de comando	• Configuración de sala de crisis física o virtual según el escenario. • Habilitación de canales de comunicación dedicados. • Inicio de registro cronológico de eventos y decisiones.

Nota: procedimiento activación plan de contingencia

2.1.9.2.1 Procedimientos de Operación Alterna para escenarios propuestos

- **Escenario ESC-PI-01: falla del sistema principal SWIFT:** la siguiente tabla presenta el procedimiento de activación de plan de contingencia para el procedimiento PROC-ALT-SWIFT-01.

Tabla N°. 37

Procedimiento PROC-ALT-SWIFT-01

Procedimiento PROC-ALT-SWIFT-01	
Objetivo	Mantener la capacidad de procesamiento de pagos interbancarios críticos durante la indisponibilidad del sistema SWIFT principal.
Tiempo estimado de implementación	60-90 minutos
Activación de terminal SWIFT de contingencia	• Acceder a la terminal SWIFT alternativa ubicada en el sitio de respaldo. • Verificar conectividad y funcionamiento. • Validar sincronización de datos y configuraciones. •
Priorización de operaciones	• Identificar pagos críticos con vencimiento inminente (≤ 2 horas). • Clasificar operaciones según su importancia sistémica. • Comunicar a las áreas de negocio el esquema de procesamiento durante la contingencia. •
Procesamiento manual asistido	• Para volúmenes pequeños, utilizar procedimiento manual controlado con doble verificación. • Documentar cada transacción procesada por vía alterna. • Implementar controles adicionales de validación.
Establecimiento de canales	• Activar protocolo de comunicación con bancos corresponsales principales. • Establecer mecanismos alternativos de confirmación de operaciones.

Procedimiento PROC-ALT-SWIFT-01	
alternos con contrapartes críticas	• Implementar controles de conciliación especiales para el período de contingencia.
Monitoreo reforzado	• Incrementar frecuencia de conciliaciones (cada 30 minutos) • Verificar liquidez interbancaria en cuentas corresponsales. • Reportar regularmente el estado de operaciones al Comité de Crisis.

Nota: procedimiento de operacional terna para activación de escenarios.

- **Escenario ESC-PI-04 ataque cibernético a sistemas de pago:** la siguiente tabla presenta el procedimiento de activación de plan de contingencia para el procedimiento PROC-ALT-CIBER-01.

Tabla N°. 38

Procedimiento PROC-ALT-CIBER-01

Procedimiento PROC-ALT-CIBER-01	
Objetivo	Garantizar la integridad y seguridad de las operaciones de pago ante un compromiso de seguridad digital.
Tiempo estimado de implementación	30-45 minutos
Aislamiento de Sistemas Comprometidos	• Desconectar inmediatamente sistemas afectados de la red. • Activar barreras adicionales de seguridad en perímetro de red. • Implementar controles de acceso de emergencia.
Activación de Plataforma Segura Aislada	• Desconectar inmediatamente sistemas afectados de la red. • Activar barreras adicionales de seguridad en perímetro de red. • Implementar controles de acceso de emergencia.
Implementación de Protocolo de Verificación Reforzada	• Activar requisitos adicionales de autenticación para todas las operaciones. • Implementar verificación telefónica para transacciones superiores a $500,000. • Aplicar reglas temporales más restrictivas de validación.
Coordinación con Equipos de Ciberseguridad	• Mantener canal directo con equipo de respuesta a incidentes. • Implementar recomendaciones tácticas inmediatas. • Colaborar en la preservación de evidencias digitales.

Nota: procedimiento de operacional terna para activación de escenarios.

2.1.9.2.2 Procedimientos de Recuperación

- **Recuperación de Sistemas Críticos:** en la siguiente tabla se encontrará las especificaciones para la recuperación de los sistemas críticos.

Tabla N°. 38

Recuperación de sistemas críticos

Recuperación de Sistemas Críticos	
Evaluación de Daños	• Diagnóstico técnico de sistemas afectados. • Estimación de tiempo de recuperación. • Determinación de la habilidad de recuperación más adecuada.
Restauración de Infraestructura	• Recuperación de servidores y bases de datos desde respaldos validados. • Reconstrucción de configuraciones y parametrizaciones. • Verificación de integridad de datos y funcionalidades.
Pruebas de Validación	• Ejecución de pruebas funcionales en ambiente aislado. • Verificación de integridad de datos mediante conciliaciones cruzadas. • Validación de conectividad con sistemas externos.
Transición Controlada	• Sincronización de datos entre sistema alterno y principal recuperado. • Transición gradual por grupos de funcionalidad. • Monitoreo intensivo durante las primeras horas post-recuperación.

Nota: recuperación de sistemas críticos

- **Retorno a la Operación Normal:** en la siguiente tabla se encontrará las especificaciones para el proceso de retorno a la operación normal.

Tabla N°. 39

Retorno a la operación normal

Retorno a la operación normal	
Verificación Previa	• Confirmación de estabilidad de sistemas recuperados durante 4 horas. • Validación cruzada de datos entre sistemas alternos y principales. • Autorización formal para el retorno por parte del Comité de Crisis.
Secuencia de Retorno	• Establecimiento de secuencia ordenada de transición. • Comunicación del plan de retorno a todas las partes involucradas. • Ejecución por fases con puntos de control.

Retorno a la operación normal	
Procesamiento de Acumulación de Transacciones	• Plan para gestionar el backlog de operaciones. • Asignación de recursos complementarios si es necesario. • Priorización de transacciones críticas.
Verificación Post-Implementación	• Monitoreo reforzado durante las primeras 24 horas. • Validación de procesamiento correcto del 100% de operaciones críticas. • Confirmación con contrapartes externas.

Nota: retorno a la operación normal

2.1.9.2.3 Estrategia de Comunicación

- **Comunicación Interna:** en la siguiente tabla se encontrará las especificaciones para el proceso de comunicación interna.

Tabla N°. 40

Comunicación interna

Audiencia	Responsable	Mensaje Clave	Canal	Frecuencia
Comité Ejecutivo	Coordinador de Contingencia	Estado de la contingencia, impacto financiero, estimación de recuperación	Videoconferencia segura, informes ejecutivos	Cada 2 horas
Áreas de Negocio	Oficial de Comunicaciones	Limitaciones operativas, tiempos estimados, procedimientos temporales	Correo electrónico seguro, intranet, SMS	Inicial + cada 4 horas
Personal Operativo	Jefes de Departamento	Instrucciones específicas, reasignación de funciones, protocolos alternativos	Reuniones de equipo, mensajería interna	Inicial + cada turno

Nota: mecanismos de comunicación interna.

- **Comunicación Externa:** en la siguiente tabla se encontrará las especificaciones para el proceso de comunicación externa.

Tabla N°. 41

Comunicación externa

Audiencia	Responsable	Mensaje Clave	Canal	Frecuencia
Reguladores	Director de Cumplimiento	Naturaleza del incidente, medidas implementadas, cumplimiento normativo	Canales oficiales, reportes regulatorios	Según normativa + actualización diaria
Clientes Corporativos	Gerentes de Relación	Impacto en servicios, canales alternos, estimaciones de normalización	Comunicación directa personalizada	Inicial + actualizaciones significativas
Bancos Corresponsales	Enlace con Entidades Externas	Protocolos alternos, instrucciones especiales, requerimientos de cooperación	Red financiera segura, contacto directo	Inmediata + cada 6 horas
Medios/Público	Dpto. Comunicación Corporativa	Mensaje institucional controlado (si aplica)	Comunicados oficiales, web corporativa	Según táctica aprobada por Comité de Crisis

Nota: mecanismos de comunicación externa.

2.1.9.2.4 Recursos Necesarios

- **Recursos tecnológicos:** en la siguiente tabla se encontrará las especificaciones de los recursos necesarios a nivel tecnológico, así como el responsable de cada uno de ellos.

Tabla N°. 42

Recursos tecnológicos

Recurso	Ubicación	Responsable de Provisión	Tiempo de Disponibilidad
Plataforma SWIFT alterna	Centro de procesamiento secundario	Gerencia de Infraestructura Tecnológica	Inmediato (siempre activo en modo pasivo)
Servidores de procesamiento de contingencia	Sitio alterno	Gerencia de Infraestructura Tecnológica	30 minutos

Recurso	Ubicación	Responsable de Provisión	Tiempo de Disponibilidad
Enlaces de comunicación redundantes	Múltiples proveedores	Gerencia de Telecomunicaciones	Inmediato (conmutación automática)
Estaciones de trabajo preconfiguradas	Centro de contingencia	Soporte Técnico	15 minutos
Sistema de mensajería segura	Nube privada	Seguridad Informática	Inmediato

Nota: recursos necesarios a nivel tecnológico

- **Recursos humanos:** en la siguiente tabla se encontrará las especificaciones de los recursos necesarios a nivel humano, así como la cantidad requerida para cada uno de los equipos.

Tabla N°. 43

Recursos humanos

Equipo	Composición Mínima	Competencias Requeridas	Movilización
Operación de Contingencia	4 especialistas + 1 supervisor	Certificación en operativa interbancaria, conocimiento del sistema alterno	60 minutos
Soporte Técnico	2 especialistas	Administración de sistemas SWIFT, redes financieras	30 minutos
Seguridad de la Información	1 oficial	Gestión de incidentes, controles de seguridad	45 minutos
Conciliación	2 analistas	Experiencia en conciliación bancaria, gestión de excepciones	90 minutos

Nota: recursos necesarios a nivel humano

2.1.9.2.5 Documentación Crítica

A continuación, se tiene en la tabla una lista de los documentos requeridos para la correcta ejecución de plan de contingencia.

Tabla N°. 44

Lista documentación crítica

Documento	Formato	Ubicación	Responsable de Actualización
Manual de procedimientos de contingencia	Digital y físico	Repositorio seguro + caja de contingencia	Jefe de Transferencias Interbancarias
Directorio de contactos clave	Digital y físico	Sistema de gestión documental + dispositivos móviles	Asistente de Dirección
Guías técnicas de sistemas alternos	Digital	Repositorio técnico seguro	Analista de Documentación Técnica
Plantillas de reporting regulatorio	Digital	Sistema de gestión documental	Oficial de Cumplimiento

Nota: lista de los documentos requeridos

2.1.9.2.6 Criterios de desactivación

A continuación, se tiene en la tabla una lista de los documentos requeridos para la correcta desactivación del plan de contingencia.

Tabla N°. 45

Criterios de desactivación:

Criterio	Descripción	Método de Verificación	Autoridad para Desactivación
Recuperación de Sistemas	Sistemas principales operativos con funcionalidad completa.	Pruebas funcionales completas, certificación técnica.	Director de Tecnología
Estabilidad Operativa	Procesamiento normal durante al menos 4 horas sin incidentes.	Monitoreo de transacciones, reportes de operación.	Director de Operaciones
Conciliación Completa	100% de transacciones del período de	Reporte de conciliación sin excepciones.	Contralor

Criterio	Descripción	Método de Verificación	Autoridad para Desactivación
	contingencia conciliadas.		
Normalización de Recursos	Disponibilidad completa de personal, instalaciones y sistemas.	Verificación de disponibilidad.	Coordinador de Contingencia

Nota: desactivación plan de contingencia

2.1.9.2.7 Mecanismos de prueba del plan

Tabla N°. 46

Mecanismos de prueba del plan

Tipo de Prueba	Frecuencia	Alcance	Método de Evaluación
Revisión Documental	Trimestral	Verificación de actualización y completitud del plan	Lista de verificación, control de versiones
Simulación de Escritorio	Semestral	Ejercicio teórico con los equipos de respuesta	Evaluación de decisiones y tiempos estimados
Prueba Parcial	Anual	Activación de componentes específicos del plan	Medición de tiempos reales, funcionalidad
Prueba completa	Anual	Simulacro completo de activación y recuperación	Evaluación frente a objetivos RTO/RPO

2.1.10 *Mantenimiento y Mejora Continua de los Planes*

- **Ciclo de Actualización:** a continuación, la tabla contiene los parámetros necesarios para el ciclo de actualización.

Tabla N°. 47

Ciclo de actualización

Actividad	Periodicidad	Responsable	Entregable
Revisión de contexto.	Semestral	Propietario del Plan.	Informe de cambios.
Actualización de información.	Trimestral	Custodio del Plan.	Plan actualizado.

Actividad	Periodicidad	Responsable	Entregable
Revisión post-incidente.	Después de cada activación.	Coordinador de Contingencia.	Lecciones aprendidas.
Revisión post-prueba.	Después de cada prueba.	Coordinador de Pruebas.	Oportunidades de mejora.
Revisión completa.	Anual	Comité de Continuidad de Negocio.	Plan de acción de mejoras.

Nota: parámetros ciclo de actualización

- **Gestión de Cambios:** todos los cambios propuestos a los planes de contingencia seguirán un proceso formal.

Tabla N°. 48

Gestión de cambios

Gestión de cambios	
Solicitud de Cambio	• Documentación de la modificación propuesta. • Justificación técnica o de negocio. • Evaluación preliminar de impacto.
Evaluación	• Análisis por parte del Custodio del Plan. • Validación con áreas involucradas. • Aprobación por el Propietario del Plan.
Implementación	• Actualización de la documentación. • Comunicación a las partes interesadas. • Capacitación si es necesario.
Verificación	• Prueba del cambio implementado. • Registro en el historial de cambios. • Certificación de la nueva versión.

Nota: gestión de cambios plan de contingencia.

2.1.11 *Documentación Asociada*

A continuación, se encuentra la tabla donde se encontrará la documentación asociada al proceso de plan de continuidad.

Tabla N°. 49

Documentación asociada

Documentación Asociada	
Registros de Actividad: para cada activación del plan se mantendrán registros detallados	• Bitácora cronológica de eventos • Decisiones tomadas y su justificación • Desviaciones respecto al plan y razones • Efectividad de las acciones implementadas • Tiempos reales vs. tiempos objetivo • Lecciones aprendidas
Informes Post-Incidente: después de cada activación real se elaborará un informe detallado	• Causa raíz del incidente • Eficacia de la respuesta • Cumplimiento de objetivos (RTO/RPO) • Impacto final en la operación • Recomendaciones de mejora • Plan de acción para implementar mejoras

Nota: documentos de apoyo plan de continuidad.

2.1.12 *Integración con el Marco de Gestión de Continuidad*

Los Planes de Contingencia para procesos críticos se integran en el marco general de Gestión de Continuidad del Negocio de la entidad financiera, alineándose con:

- Política de Continuidad del Negocio.
- Plan de Recuperación de Desastres (DRP).
- Política de Gestión de Crisis.
- Marco de Gestión de Riesgos.
- Requerimientos regulatorios aplicables.

2.1.13 *Conclusiones y recomendaciones implementación plan de contingencia*

- **Conclusiones sobre los ejemplos asociados**
    - Los Planes de Contingencia son herramientas operativas esenciales para garantizar la continuidad de los procesos críticos en las entidades financieras.
    - La efectividad de estos planes depende de su actualización, prueba regular y mejora continua.

- El planteamiento debe ser progresivo, priorizando los procesos de mayor criticidad identificados en el BIA.

- **Recomendaciones sobre los ejemplos asociados**
  - **Integración Tecnológica**: implementar herramientas de automatización para la activación y seguimiento de planes
  - **Cultura de Resiliencia**: desarrollar programas de concienciación y capacitación continua
  - **Gestión de Interdependencias**: fortalecer la visión de la continuidad considerando relaciones entre procesos
  - **Alineación Estratégica**: revisar periódicamente la alineación entre planes de contingencia y objetivos estratégicos
  - **Colaboración Externa**: establecer acuerdos de cooperación con entidades del sector para respuesta coordinada ante eventos sistémicos

Los Planes de Contingencia representan la materialización del compromiso de la entidad financiera con la resiliencia operacional, contribuyendo a la estabilidad del sistema financiero y a la protección de los intereses de los clientes y demás partes interesadas.

2.1.13.1 Aplicabilidad y Adaptación del marco identificación y tratamiento de riesgo

La metodología presentada para el análisis de riesgos establece un marco referencial que proporciona las bases necesarias para la identificación y evaluación de riesgos en entidades financieras. Es importante destacar que estos lineamientos generales deben ser adaptados y profundizados según las características específicas de cada proceso y subproceso dentro de la organización. La efectividad del análisis dependerá de la capacidad de la institución para contextualizar estas directrices generales en función de sus necesidades particulares, su estructura operativa y sus objetivos estratégicos.

2.1.13.1.1 Granularidad y profundidad del análisis de riesgos

Al aplicar esta metodología, es el principio para comprender que cada proceso core identificado requerirá un análisis detallado y específico que considere sus propias particularidades y desafíos.

Los pasos descritos deben ser ejecutados de manera recursiva y detallada para cada componente del proceso, considerando no solo los riesgos evidentes sino también aquellos que pueden surgir de las interrelaciones entre subprocesos. Este nivel de granularidad en el análisis permite identificar vulnerabilidades que podrían no ser evidentes en una evaluación más general y asegura que los controles implementados sean verdaderamente efectivos para el contexto específico de cada proceso.

2.1.13.1.2 Evolución y mejora continua

La identificación y análisis de riesgos debe entenderse como un proceso dinámico y en constante evolución. Los tópicos generales presentados proporcionan un punto de partida sólido, pero deben ser continuamente revisados y actualizados para reflejar tanto los cambios en el entorno operativo como la aparición de nuevas amenazas y vulnerabilidades. Esta adaptabilidad y flexibilidad del marco permite a las instituciones financieras mantener una orientación proactiva en la gestión de riesgos, asegurando que sus procesos de evaluación y control evolucionen al mismo ritmo que los desafíos del sector financiero.

2.1.14 *Identificación de activos IFAS*

Para identificar la problemática que poseen las entidades en el levantamiento de activos de información, se realizó la implementación de una encuesta centrada en identificar los **"Desafíos en la identificación y clasificación de activos críticos en entidades financieras"** representa un esquema de metodología que permite establecer una base sólida en el proceso de identificación de activos IFAS. Esta herramienta permitió capturar diversos puntos de vista multidisciplinarios, revelando brechas críticas y oportunidades de mejora mediante métodos tradicionales de análisis. Al involucrar directamente a los colaboradores que interactúan cotidianamente con estos activos de información, se obtiene una visión más amplia de la problemática que existe al interno de las entidades para identificar los activos de información asociados a las IFAS. A continuación, se presentan los resultados obtenidos de esta encuesta, los cuales han sido la base principal para estructurar un marco robusto de identificación de activos críticos identificando algunas especificaciones operativas y los desafíos específicos que enfrenta una organización en el ecosistema financiero actual (Microsoft Defender for Endpoint, 2025). Anexo 1

Es importante indicar que la encuesta fue aplicada a 25 especialistas de tres entidades bancarias privadas de primer y segundo nivel en Colombia, incluyendo roles como Gerentes de TI, Oficiales

de Seguridad de la Información, Gerentes de Riesgos, líderes de áreas de negocio y auditores de TI. El objetivo principal fue identificar y catalogar las dificultades para el mapeo de los activos críticos que soportan las operaciones bancarias del core.

En el Anexo 2 se podrán identificar los resultados asociados a cada una de las preguntas realizadas a la muestra de expertos en la encuesta: desafíos en la Identificación y Clasificación de Activos Críticos en Entidades Financieras (25 participantes)

2.1.14.1 Conclusiones principales de la encuesta realizada

Según los resultados obtenidos de la encuesta aplicada a 25 especialistas en seguridad de la información y ciberseguridad, se identificaron desafíos críticos en el proceso de levantamiento y gestión de activos de información. La problemática principal se centra en la dificultad para mantener una actualización continua de los activos (88% de los encuestados), situación que se agrava por las limitaciones en las herramientas disponibles (80%) y la falta de participación de los usuarios finales en la clasificación de activos según su confidencialidad (76%). Es notable que pocas son las organizaciones que utilizan software especializado para esta labor, mientras que un 28% aún depende de hojas de cálculo, lo que dificulta la gestión eficiente y el seguimiento adecuado. La complejidad de las interdependencias entre activos y la resistencia organizativa se suman como obstáculos de importancia. Además, la frecuencia de actualización del inventario de activos muestra una brecha importante, donde solo el 16% realiza actualizaciones mensuales, mientras que la mayoría (60%) lo hace trimestral o semestralmente, lo que puede resultar insuficiente en entornos tecnológicos en continuo cambio. Esta situación se agrava por la falta de criterios claros de clasificación y la diversidad de metodologías utilizadas, donde si bien predominan los estándares internacionales como ISO 27001 y NIST, existe una división significativa en los planteamientos adoptados por las entidades.

- **Perfil Dominante**: la mayoría de los encuestados son Oficiales de Seguridad de la Información con 5-10 años de experiencia.
- **Metodologías**: predomina el uso de estándares internacionales (ISO 27001 y NIST) sobre metodologías propias.
- **Desafíos Críticos**:
    - La actualización continua es el mayor desafío (88%)
    - Las limitaciones de herramientas afectan al 80%
    - La clasificación por usuarios finales es problemática para el 76%

- **Herramientas**:
    - Solo un tercio usa software especializado
    - Existe una dependencia significativa de hojas de cálculo (28%)
    - Hay una fragmentación en las soluciones utilizadas
- **Actualización de Activos**:
    - La mayoría (60%) actualiza trimestral o semestralmente
    - Solo 16% mantiene actualizaciones mensuales
    - Un pequeño porcentaje (8%) actualiza solo por cambios significativos
- **Áreas de Mejora Identificadas**:
    - Necesidad de herramientas más especializadas
    - Automatización de procesos de actualización
    - Mejora en criterios de clasificación
    - Mayor participación de usuarios finales

Basado en la encuesta de apoyo sobre los desafíos en la identificación y clasificación de activos críticos en entidades financieras, se construirá la fase asociada con la identificación de activos IFAS.

2.1.14.2 Metodología para la identificación de activos IFAS

A continuación, se presenta tres etapas principales para la iniciación del levantamiento de identificación de activos de información (Microsoft Defender for Endpoint, 2025).

Tabla N°. 50

Metodología para la identificación de activos IFAS

Metodología para la identificación de activos IFAS	
Etapa preparatoria	
Conformación de equipos multidisciplinarios	• Representantes de TI (infraestructura, desarrollo, seguridad). • Personal de gestión de riesgos. • Líderes de áreas de negocio clave (banca personal, corporativa, inversiones). • Oficiales de cumplimiento y protección de datos.
Definición de criterios de criticidad	• Impacto en la continuidad del negocio. • Sensibilidad de la información. • Requisitos regulatorios aplicables. • Valor financiero directo e indirecto.
Proceso de identificación	

Metodología para la identificación de activos IFAS	
Sesiones de trabajo colaborativas	• Talleres de identificación por dominio funcional • Entrevistas estructuradas con custodios de información • Sesiones de mapeo de flujos de datos y procesos críticos
Catalogación de activos por categorías	
Información	• Datos de clientes (información personal, financiera, transaccional) • Información sobre productos y servicios • Información financiera interna • Registros regulatorios y de cumplimiento
Funciones	• Procesos de negocio críticos (préstamos, depósitos, inversiones) • Funciones de servicio al cliente • Procesos de conciliación y compensación • Funciones de administración de riesgo
Aplicaciones	• Core bancario • Sistemas de procesamiento de pagos • Plataformas de banca digital • Herramientas de análisis de riesgo crediticio • Aplicaciones de cumplimiento normativo
Sistemas	• Infraestructura de servidores críticos • Redes y comunicaciones • Sistemas de almacenamiento • Mecanismos de copia de respaldo • Sistemas de control de acceso
Validación cruzada	• Entre áreas para asegurar que no existan activos no identificados

Nota: método para la identificación de activos IFAS

2.1.14.2.1 Herramientas de apoyo en el levantamiento e identificación de activos IFAS

A continuación, se encuentra una serie de parámetros y herramientas que apoyan el levantamiento e identificación de activos IFAS en las organizaciones financieras.

- **Matrices de responsabilidad** (RACI) para cada activo identificado.
- **Inventario centralizado** de activos con metadatos importantes:
    - Propietario/custodio del activo
    - Clasificación de confidencialidad
    - Ubicación física/lógica
    - Interrelaciones con otros activos
    - Medidas de protección actuales

2.1.14.3 Consideraciones específicas basadas en la encuesta

Según los resultados de la encuesta realizada "Desafíos en la Identificación y Clasificación de Activos Críticos en Entidades Financieras", es importante tener en cuenta los siguientes parámetros para realizar el proceso de identificación y documentación de los activos de información IFAS:

- **Mecanismos para la identificación de "activos ocultos"** no documentados formalmente, pero críticos para operaciones.

- **Mapeo de dependencias entre activos** para entender cascadas de impacto.
- **Evaluación periódica de la criticidad** de los activos, no solo durante la identificación inicial.
- **Documentación estandarizada** que facilite la comunicación entre áreas técnicas y de negocio.
- Los siguientes documentos serían los esperados al finalizar las actividades anteriores:
    - **Inventario de activos IFAS** clasificados por criticidad
    - **Matrices de responsabilidad y custodia** para cada activo identificado
    - **Documentación de criterios aplicados** para la clasificación de criticidad

Este planteamiento colaborativo no solo permite una identificación más completa de los activos críticos, sino que promueve una cultura organizacional donde la protección de estos activos es una responsabilidad compartida entre todas las áreas.

2.1.14.4 Clasificación de activos

La clasificación de activos de información son la base principal para la gestión de la seguridad de la información, siendo la Tríada CIA (Confidencialidad, Integridad y Disponibilidad) el marco de referencia más ampliamente adoptado para este propósito. Esta taxonomía propone una estructura de cuatro niveles para cada dimensión de la tríada, permitiendo una categorización de los activos de información (COBIT, 2019). El modelo está diseñado para facilitar la identificación de controles de seguridad apropiados, asegurar una protección adecuada según la criticidad del activo y optimizar la asignación de recursos de seguridad (ISO/IEC 27002:2022, 2022).

La clasificación adecuada de los activos IFAS permite establecer controles proporcionales a su criticidad y sensibilidad, optimizando los recursos de seguridad en el sector financiero:

Tabla N°. 51

Taxonomía basada en la Tríada CIA

Taxonomía basada en la Tríada CIA	
Confidencialidad	• Propiedad que garantiza que la información no esté disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Niveles de clasificación	• Público: información que puede ser conocida por cualquier persona sin restricciones. • Uso interno: información para uso exclusivo dentro de la entidad financiera. • Confidencial: información sensible cuya divulgación podría afectar negativamente a la entidad. • Altamente confidencial: información crítica cuya divulgación podría tener graves consecuencias legales, reputacionales o financieras.
Integridad	• Propiedad que garantiza que los datos sean exactos y completos, y que no hayan sido alterados sin autorización.
Niveles de clasificación	• Baja: la alteración de los datos no tendría impacto significativo. • Media: la alteración podría causar inconvenientes operativos subsanables. • Alta: la alteración tendría impactos financieros o reputacionales significativos. • Crítica: la alteración comprometería gravemente las operaciones, finanzas o cumplimiento normativo.
Disponibilidad **Niveles de clasificación**	• Propiedad que garantiza que la información sea accesible y utilizable cuando sea requerida por los usuarios autorizados. • Baja: tolerancia a interrupciones de días o más. • Media: tolerancia a interrupciones de horas. • Alta: tolerancia a interrupciones de minutos. • Crítica: requerimiento de disponibilidad casi continua (99.99% o superior).

Nota: información tomada de la fuente *(NIST SP 800-53, 2020)*

2.1.14.5 Metodología de Clasificación

A continuación, se presenta un esquema para el proceso de evaluación y sus criterios cada uno asociado a la triada (CIA).

Tabla N°. 52

Metodología de clasificación

Metodología de clasificación	
Proceso de evaluación	
Valoración inicial	• Aplicación de cuestionarios estructurados a los propietarios de los activos. • Evaluación por expertos en seguridad y riesgos.
Criterios de evaluación	
Para Confidencialidad	• Sensibilidad legal/regulatoria de la información • Valor competitivo de los datos • Impacto reputacional ante divulgación • Requisitos de privacidad aplicable
Para Integridad	• Criticidad para decisiones financieras • Impacto financiero de datos incorrectos • Necesidad de evidencia forense o auditable • Requisitos regulatorios de precisión
Para Disponibilidad	• Tiempos máximos de recuperación (RTO) • Puntos objetivos de recuperación (RPO) • Ventanas de servicio requeridas • Dependencias de procesos críticos
Mecanismo de consenso	• Revisión por comité multidisciplinario • Aprobación formal por oficiales de seguridad y riesgos.

Nota: información tomada de la fuente: *(NIST SP 800-53, 2020)*

2.1.14.6 **Matriz de Clasificación Combinada**

Se recomienda la implementación de una matriz combinada que asigne un nivel general de criticidad basado en los valores individuales de C-I-A (ISO/IEC, 2022) (COBIT, 2019):

Tabla N°. 53

Matriz de Clasificación Combinada

Matriz de Clasificación Combinada		
Nivel combinado	**Definición**	**Criterios**
Nivel 1 - Bajo	Activos no críticos para operaciones diarias	Todos los valores C-I-A son bajos
Nivel 2 - Medio	Activos importantes, pero con alternativas disponibles	Al menos un valor C-I-A es medio
Nivel 3 - Alto	Activos esenciales para procesos clave	Al menos un valor C-I-A es alto
Nivel 4 - Crítico	Activos vitales para la continuidad del negocio	Al menos un valor C-I-A es crítico

Nota: información tomada de la fuente: *(ISO/IEC 27002:2022, 2022)*

- Documentación de resultado de la clasificación debe quedar formalizado en:
    - Registro de clasificación: por activo con valores asignados para C-I-A
    - Etiquetado: físico/lógico de activos según su clasificación
    - Matrices de responsabilidad: según nivel de criticidad
    - Políticas de manejo: específicas por nivel de clasificación
- Alineación con políticas de seguridad de los resultados de la identificación y clasificación de activos de información:
    - Políticas de gestión de acceso y autenticación
    - Requisitos de cifrado según nivel de confidencialidad
    - Tácticas de continuidad según valores de disponibilidad
    - Controles de integridad proporcionales a la clasificación
- Proceso de revisión y actualización mediane la implementación del siguiente ciclo continuo.
    - Revisión periódica (mínimo anual) de la clasificación
    - Actualización ante cambios significativos (fusiones, nuevos productos)
    - Verificación del cumplimiento de políticas derivadas de la clasificación
    - Auditorías internas para validar la adecuación de la clasificación

Esta clasificación sistemática permitirá focalizar los esfuerzos de seguridad en los activos verdaderamente críticos, optimizando la asignación de recursos y garantizando el cumplimiento normativo en el sector financiero (National Institute of Standards and Technology, 2004).

2.2 Fase 2: Metodología de identificación y clasificación de vulnerabilidades y brechas de seguridad en entidades financieras

La Fase 2 desarrolla el proceso de aseguramiento de las Internet Facing Applications (IFAs), aplicaciones expuestas directamente a internet que son una superficie de ataque crítica para cualquier entidad. Esta metodología permite identificar con precisión las vulnerabilidades que podrían comprometer la integridad y confidencialidad de los activos de información expuestos al exterior. Mediante la aplicación del marco NIST SP (NIST SP 800-53, 2020) para el análisis de riesgos, la ejecución de Gap Analysis contrastando controles implementados contra estándares internacionales de seguridad, y la realización de ejercicios de Red Team que simulan escenarios de ataque reales, se logra una evaluación defensiva, fortaleciendo así la postura de seguridad de la información en la entidad ante amenazas cibernéticas cada vez más sofisticadas.

2.2.1 *Análisis de riesgos*

El análisis de riesgos es una de las actividades principales para la identificación de vulnerabilidades que puedan comprometer la integridad y confidencialidad de los activos IFAS en entidades del sector financiero. A continuación, se desarrolla un esquema de metodología completa basada en el marco NIST SP 800-30 complementada con escenarios de ataque del framework.

2.2.2 *Metodología NIST SP 800-30 para Evaluación de Riesgos*

- **Etapa 1:** a continuación, se encuentran algunos parámetros generales para la definición de la evaluación de riesgos.

  Tabla N°. 54

  Preparación para la evaluación de riesgos

Preparación para la evaluación de riesgos	
Definición del propósito	• Establecimiento de objetivos claros alineados con las necesidades de protección de activos IFAS • Determinación del alcance (sistemas, aplicaciones, infraestructura, información) • Definición de los límites temporales y organizacionales
Identificación de supuestos y restricciones	• Limitaciones regulatorias específicas del sector financiero • Restricciones operativas y tecnológicas • Consideraciones presupuestarias y de recursos

Preparación para la evaluación de riesgos	
Establecimiento de fuentes de información	• Inventario de activos IFAS previamente identificados • Documentación técnica de sistemas y aplicaciones • Registros históricos de incidentes de seguridad • Auditorías previas e informes de cumplimiento • Análisis de vulnerabilidades anteriores
Selección de la metodología de evaluación	• Planteamiento cuantitativo con métricas financieras específicas • Métodos cualitativos para factores difíciles de cuantificar • Combinación híbrida para un análisis completo

Nota: tomado de la fuente: *(NIST, Cybersecurity Framework | NIST, 2013)*

- **Etapa 2:** a continuación, se presentan 6 pasos generales para llevar a cabo la evaluación de riegos asociados a las IFAS.
    - **Paso 1:** identificación de amenazas
        - Categorización de fuentes de amenazas:

Tabla N°. 55

Fuentes de amenazas

Fuentes de amenazas	
Fuentes de amenazas adversariales	• Actores externos: ciberdelincuentes, hacktivistas, grupos APT (Advanced Persistent Threats) • Actores internos: empleados descontentos, contratistas, personal temporal • Proveedores y terceros: cadena de suministro, socios tecnológicos
Fuentes de amenazas adversariales	• Estructurales: fallos de hardware, obsolescencia tecnológica • Ambientales: desastres naturales, fallas de energía, pandemias • Humanas: errores accidentales, omisiones, configuraciones incorrectas

Nota: Fuentes de amenazas frente a su procedencia

- Integración con MITRE ATT&CK (MITRE ATT&CK, 2025):
    - Mapeo de actores de amenazas primordiales para el sector financiero:
        - APT38 (Lazarus Group): enfocado en fraude bancario
        - FIN7: especializado en ataques a sistemas de pagos
        - Carbanak: dirigido a infraestructuras bancarias
- Identificación de tácticas, técnicas y procedimientos (TTPs) aplicables:

Tabla N°. 56

Técnicas y procedimientos (TTPs)

Identificación de tácticas		
Táctica ATT&CK	**Técnicas principales para activos IFAS**	**Impacto potencial**
Acceso Inicial	Phishing (T1566), Explotación de aplicaciones (T1190)	Phishing (T1566), Explotación de aplicaciones (T1190)
Ejecución	Scripts (T1059), Tareas programadas (T1053)	Scripts (T1059), Tareas programadas (T1053)
Persistencia	Cuentas válidas (T1078), Modificación de registro (T1112)	Cuentas válidas (T1078), Modificación de registro (T1112)
Evasión de Defensas	Ofuscación (T1027), Evasión de EDR (T1562)	Ofuscación (T1027), Evasión de EDR (T1562)
Acceso a Credenciales	Keylogging (T1056), Robo de credenciales (T1555)	Keylogging (T1056), Robo de credenciales (T1555)
Movimiento Lateral	Pass-the-Hash (T1550), Uso de RDP (T1021)	Pass-the-Hash (T1550), Uso de RDP (T1021)
Exfiltración de Datos	Transferencia por canales alternativos (T1048)	Transferencia por canales alternativos (T1048)

Nota: tomado de la fuente: *(MITRE ATT&CK, 2025)*

- **Paso 2:** a continuación, se presentan algunos parámetros generales para realizar la identificación de vulnerabilidades.

Tabla N°. 57

Identificación de vulnerabilidades

Identificación de Vulnerabilidades		
Análisis técnico de vulnerabilidades	**Vulnerabilidades de aplicaciones**	• Revisión de código para detectar fallos de seguridad (SAST) • Pruebas dinámicas de aplicaciones (DAST) • Análisis de composición de software (SCA) para detectar dependencias vulnerables • Revisión de configuraciones de seguridad
	Vulnerabilidades de infraestructura	• Escaneo de puertos y servicios expuestos • Revisión de configuraciones de servidores y dispositivos de red • Análisis de parches pendientes y versiones de software • Evaluación de seguridad en entornos cloud y virtualizados
	Vulnerabilidades organizacionales	• Análisis de políticas y procedimientos • Evaluación de programas de concienciación • Revisión de controles de acceso y segregación de funciones • Evaluación de gestión de identidades y privilegios
Pruebas de penetración enfocadas	• Pruebas de penetración de caja negra/gris/blanca • Ejercicios de red team simulando APTs financieros • Pruebas de ingeniería social (phishing, vishing) • Revisión de seguridad física para activos críticos	
Documentación estandarizada	• Catalogación según Common Vulnerabilities and Exposures (CVE) • Clasificación por Common Weakness Enumeration (CWE) • Calificación mediante Common Vulnerability Scoring System (CVSS)	

Nota: tomado de la fuente:*(MITRE ATT&CK, 2025)*

- **Paso 3:** en este paso se debe realizar una evaluación y análisis específicos a los controles existentes, así como a las brechas de seguridad que se pueden encontrar en el mapeo de riesgo.
    - **Evaluación de controles existentes**:
        - **Preventivos**: firewalls, sistemas DLP, gestión de accesos privilegiados
        - **Detectivos**: el SIEM, monitorización de comportamiento, EDR

        - **Correctivos**: respuesta a incidentes, recuperación de desastres
        - **Disuasivos**: políticas, procesos disciplinarios, auditorías
    - **Análisis de brechas de control**:
        - Mapeo contra marcos regulatorios financieros aplicables
        - Comparación con estándares
        - Identificación de controles ausentes o insuficientes
- **Paso 4:** determinación de Probabilidad
    - **Factores de probabilidad**:
        - Historial de ocurrencia de eventos similares
        - Facilidad de explotación de vulnerabilidades (complejidad técnica)
        - Exposición de los activos (interna, externa, híbrida)
        - Existencia de exploits públicos o herramientas automatizadas
        - Motivación y capacidades de los atacantes
    - **Escala de probabilidad**:

Tabla N°. 58

Tabla de escala de probabilidad

Nivel	Descripción	Criterios cualitativos	Criterios cuantitativos
Muy Alto	Casi cierto	Explotación inminente	>95% probabilidad anual
Alto	Muy probable	Explotación altamente probable	70-95% probabilidad anual
Moderado	Probable	Explotación posible	30-70% probabilidad anual
Bajo	Improbable	Explotación poco probable	5-30% probabilidad anual
Muy Bajo	Raro	Explotación muy improbable	<5% probabilidad anual

Nota: tomado de la fuente:*(MITRE ATT&CK, 2025)*

- **Paso 5:** determinación de Impacto

- **Categorías de impacto para activos IFAS**:

Tabla N°. 59

Esquema de categorización de impacto IFA

Esquema de categorización de impacto IFAS	
Impacto financiero directo	• Pérdidas monetarias por fraude • Costos de investigación y recuperación • Sanciones regulatorias y multas
Impacto operacional	• Interrupción de servicios críticos • Afectación a procesos de negocio clave • Tiempos de inactividad y degradación del servicio
Impacto reputacional	• Daño a la confianza de clientes e inversores • Cobertura mediática negativa • Afectación a relaciones comerciales
Impacto legal y de cumplimiento	• Incumplimiento de obligaciones regulatorias • Litigios y demandas de clientes/accionistas • Responsabilidades fiduciarias comprometidas

Nota: esquema de categorización por el impacto en las IFAS.

- **Escala de impacto**:

Tabla N°. 60

Esquema de escala de impacto

Nivel	Descripción	Impacto financiero	Impacto operacional	Impacto reputacional	Impacto de cumplimiento
Crítico	Catastrófico	>5% del ingreso anual	Interrupción total >24h	Cobertura mediática internacional	Pérdida de licencias
Alto	Severo	1-5% del ingreso anual	Interrupción parcial >8h	Cobertura mediática nacional	Sanciones significativas

Nivel	Descripción	Impacto financiero	Impacto operacional	Impacto reputacional	Impacto de cumplimiento
Moderado	Significativo	0.1-1% del ingreso anual	Interrupción limitada <8h	Cobertura regional	Multas moderadas
Bajo	Menor	<0.1% del ingreso anual	Degradación del servicio	Conocimiento limitado	Hallazgos menores
Muy Bajo	Insignificante	Despreciable	Sin efectos perceptibles	Sin impacto externo	Sin consecuencias

Nota: ejemplo esquema de impacto

- **Paso 6:** determinación del Riesgo
  - **Matriz de riesgo**: combinación sistemática de los valores de probabilidad e impacto para determinar el nivel de riesgo general:

Tabla N°. 61

Matriz de riesgo

Probabilidad/Impacto	Muy Bajo	Bajo	Moderado	Alto	Crítico
Muy Alto	Moderado	Alto	Alto	Crítico	Crítico
Alto	Bajo	Moderado	Alto	Alto	Crítico
Moderado	Bajo	Moderado	Moderado	Alto	Alto
Bajo	Muy Bajo	Bajo	Moderado	Moderado	Alto
Muy Bajo	Muy Bajo	Muy Bajo	Bajo	Moderado	Moderado

Nota: tomado de la fuente:*(MITRE ATT&CK, 2025)*

  - **Priorización de riesgos**:
    - Ordenamiento de escenarios de riesgo por nivel de severidad
    - Agrupación de riesgos relacionados
    - Identificación de cadenas de riesgo y efectos cascada

- **Etapa 3:** en la siguiente tabla se encuentra una recomendación de las comunicaciones y los documentos asociados a los resultados.

Tabla N°. 62

Comunicación y documentos requeridos

Comunicación y documentos requeridos	
Informe ejecutivo	• Resumen de hallazgos críticos • Visualización de riesgos principales • Recomendaciones estratégicas
Informe técnico detallado	• Metodología aplicada • Inventario completo de vulnerabilidades • Escenarios de ataque detallados • Análisis de controles existentes y propuestos • Evidencias y pruebas técnicas
Registro estructurado de riesgos	• Código único de identificación • Descripción detallada • Activos IFAS afectados • Valoración (probabilidad, impacto, nivel) • Propietario del riesgo • Controles mitigantes (existentes y recomendados) • Estado actual y plan de acción

Nota: tomado de la fuente:*(MITRE ATT&CK, 2025)*

2.2.3 *Ejemplos: escenarios de Ataque MITRE ATT&CK para Activos IFAS*

A continuación, se presentan escenarios específicos de ataque modelados con el framework MITRE ATT&CK, enfocados en los activos IFAS críticos del sector financiero (MITRE ATT&CK, 2025):

2.2.3.1 Escenario 1: compromiso de Sistema Core Bancario

- **Perfil de amenaza**: grupo APT financieramente motivado (tipo Carbanak)
- **Activos IFAS objetivo**: sistema core bancario, bases de datos de clientes, interfaces de pago
- **Cadena de ataque**: en la siguiente tabla se encuentra la taxonomía asociada a la cadena de ataque propuesta conforme al escenario definido.

Tabla N°. 63

Esquema de cadena de ataque escenario 1

Cadena de ataque	
Acceso Inicial [TA0001]:	• Spear phishing con documento malicioso [T1566.001] • Objetivo: personal de operaciones bancarias
Ejecución [TA0002]	• Macro malicioso [T1204.002] • PowerShell [T1059.001]
Persistencia [TA0003]	• Modificación de tareas programadas [T1053.005] • Abuso de WMI [T1047]
Escalación de Privilegios [TA0004]:	• Explotación de vulnerabilidad local [T1068] • Robo de credenciales de administrador [T1078.002]
Evasión de Defensas [TA0005]:	• Ofuscación de código [T1027] • Evasión de detección mediante inyección de procesos [T1055]
Movimiento Lateral [TA0008]:	• Pass-the-Hash [T1550.002] • RDP a sistemas críticos [T1021.001]
Acceso a Datos [TA0009]:	• Consultas SQL no autorizadas [T1059.005] • Extracción de información sensible
Impacto [TA0040]:	• Manipulación de transacciones [T1565] • Transferencias fraudulentas a cuentas controladas por atacantes

Nota: tomado de la fuente:*(MITRE ATT&CK, 2025)*

- **Vulnerabilidades potenciales**:
  - Falta de autenticación multifactor en sistemas críticos
  - Configuraciones inadecuadas de segmentación de red
  - Monitorización insuficiente de actividades privilegiadas
  - Ausencia de validaciones en procesos de transferencia

2.2.3.2 Escenario 2: compromiso de Plataforma de Banca Digital

- **Perfil de amenaza**: grupo cibercriminal organizado (tipo FIN7)
- **Activos IFAS objetivo**: aplicación web/móvil de banca, APIs de servicios financieros
- **Cadena de ataque**: en la siguiente tabla se encuentra la taxonomía asociada a la cadena de ataque propuesta conforme al escenario definido.

Tabla N°. 64

Cadena de ataque escenario 2

Cadena de ataque	
Reconocimiento [TA0043]	• OSINT sobre infraestructura web [T1592] • Escaneo de vulnerabilidades [T1595]
Acceso Inicial [TA0001]	• Explotación de vulnerabilidad en aplicación web [T1190] • Inyección SQL [CWE-89]
Credenciales [TA0006]	• Captura de credenciales en tránsito [T1556] • Ataque de fuerza bruta a cuentas [T1110]
Descubrimiento [TA0007]:	• Enumeración de sistemas internos [T1082] • Descubrimiento de servicios de red [T1046]
Exfiltración [TA0010]:	• Exfiltración mediante canal encriptado [T1048.002] • Transferencia por protocolo alternativo [T1048.003]
Impacto [TA0040]:	• Manipulación de cuentas de usuario [T1531] • Fraude de transacciones

Nota: tomado de la fuente: *(MITRE ATT&CK, 2025)*

- **Vulnerabilidades potenciales**:
  - Falta de validación de entrada en campos de formulario
  - Exposición de información sensible en respuestas de API
  - Gestión inadecuada de sesiones
  - Ausencia de mecanismos anti-automatización

2.2.3.3 Escenario 3: compromiso de Sistemas de Tesorería

- **Perfil de amenaza**: insider malintencionado (empleado o contratista)
- **Activos IFAS objetivo**: sistema de gestión de tesorería, datos de mercado, configuraciones de límites
- **Cadena de ataque**: en la siguiente tabla se encuentra la taxonomía asociada a la cadena de ataque propuesta conforme al escenario definido.

Tabla N°. 65

Cadena de ataque escenario 3

Cadena de ataque	
Acceso Inicial [TA0001]:	• Uso de acceso legítimo [T1078] • Credenciales válidas [T1078.001]
Persistencia [TA0003]:	• Creación de cuenta [T1136] • Modificación de reglas de acceso [T1222]
Evasión [TA0005]:	• Borrado de logs [T1070.001] • Actividad en horarios inusuales [T1562.001]
Acceso a Datos [TA0009]:	• Acceso autorizado a información fuera de rol [T1530] • Consultas excesivas [T1213]
Exfiltración [TA0010]:	• Transferencia por correo electrónico personal [T1048] • Uso de dispositivos extraíbles [T1052.001]
Impacto [TA0040]:	• Manipulación de configuraciones de límites [T1565.001] • Alteración de datos financieros

Nota: tomado de la fuente: *(MITRE ATT&CK, 2025)*

- **Vulnerabilidades potenciales**:
  - Exceso de privilegios en cuentas de usuario
  - Falta de monitorización de acciones privilegiadas
  - Ausencia de segregación de funciones
  - Deficiencias en la gestión de cambios

2.2.4 *Controles de Mitigación Recomendados según NIST SP 800-53*

Para cada escenario de amenaza identificado, se recomienda implementar controles específicos alineados con NIST SP 800-53 (NIST, Cybersecurity Framework | NIST, 2013):

Tabla N°. 66

Controles propuestos

Controles propuestos basados en NIST SP 800-53	
Para Escenario 1 (Compromiso de Sistema Core Bancario)	• AC-2: gestión de cuentas • AC-3: cumplimiento de control de acceso • AC-6: privilegio mínimo • AU-2: eventos auditables • AU-6:revisión, análisis y reporte de auditoría • IA-2:identificación y autenticación de usuarios organizacionales • IA-5: gestión de autenticadores • SC-7: protección de límites • SI-4: monitorización del sistema
Para Escenario 2 (Compromiso de Plataforma de Banca Digital):	• SA-11: pruebas de seguridad y evaluación • SA-15: desarrollo de sistemas, aplicaciones e integración • SC-8: confidencialidad e integridad de la transmisión • SC-23: autenticidad de la sesión • SI-10: validación de entradas • SI-11: manejo de errores • SI-7: integridad del software, firmware y la información
Para Escenario 3 (Compromiso de Sistemas de Tesorería)	• AC-5: separación de funciones • AC-17: acceso remoto • AT-2: concienciación en seguridad • AU-10: no repudio • AU-12: generación de auditoría • CM-5: restricciones de acceso para cambios • PS-4: terminación de personal • PS-7: seguridad de personal externo

Nota: tomado de la fuente:*(NIST SP 800-53, 2020)*

2.2.5 *Plan de Remediación y Gestión Continua de Riesgos*

Tabla N°. 67

Plan de Remediación y Gestión continua de Riesgos

Plan de Remediación y Gestión Continua de Riesgos	
Estrategia de tratamiento	• Mitigación: implementación de controles • Transferencia: seguros cibernéticos • Aceptación: documentación formal • Evitación: rediseño de procesos
Priorización de acciones	• Plan inmediato (0-30 días): riesgos críticos • Plan a corto plazo (30-90 días): riesgos altos • Plan a medio plazo (90-180 días): riesgos moderados • Plan a largo plazo (>180 días): riesgos bajos
Monitorización y gestión continua	• Revisión periódica del registro de riesgos • Actualización ante cambios en amenazas o vulnerabilidades • Unificación con procesos operativos • Reportes regulares a la alta dirección
Indicadores clave de riesgo (KRIs	• Intentos fallidos de autenticación • Vulnerabilidades críticas no parchadas • Incidentes de seguridad relacionados • Tiempo de exposición a vulnerabilidades • Eficacia de controles implementados

Nota: plan de remediación y gestión continua de riesgos

La implementación sistemática de este planteamiento de análisis de riesgos basado en NIST SP 800-30 (NIST, Cybersecurity Framework | NIST, 2013) y MITRE ATT&CK (MITRE ATT&CK, 2025)permitirá a las entidades financieras identificar, evaluar y gestionar las vulnerabilidades que amenazan sus activos IFAS críticos, fortaleciendo la postura general de seguridad y cumplimiento regulatorio.

2.2.5.1 **Detección de brechas**

El Gap Analysis o análisis de brechas es una metodología esencial para identificar las diferencias existentes entre el estado actual de los controles de seguridad de la información y el estado sugerido por estándares internacionales. Este proceso sistemático permite a las entidades financieras detectar vulnerabilidades críticas y subsanarlas para mejorar su postura de seguridad.

2.2.6 *Metodología de Gap Analysis para activos IFAS*

- **Selección de marcos de referencia**

La primera etapa del análisis de brechas implica la selección de los estándares internacionales más importantes para el sector financiero:

Tabla N°. 68

Marcos de referencia análisis de brechas

Marcos de referencia	
Marcos regulatorios y estándares primarios	• ISO/IEC 27001:2022: estándar internacional para sistemas de gestión de seguridad de la información • NIST Cybersecurity Framework (CSF): marco completo con funciones de identificar, proteger, detectar, responder y recuperar • PCI DSS v4.0: estándar específico para la protección de datos de tarjetas de pago • SWIFT Customer Security Controls Framework (CSCF): controles específicos para entidades que utilizan la red SWIFT.
Marcos complementarios	• COBIT 2019: marco de gobernanza y gestión de TI con énfasis en seguridad • CIS Controls v8: conjunto de controles de seguridad priorizados • NIST SP 800-53 Rev.5: controles de seguridad detallados para sistemas de información • Marco FFIEC para exámenes de TI: específico para instituciones financieras en EE.UU.

Nota: Análisis de brechas

- **Desarrollo de la matriz de evaluación**

La efectividad del Gap Analysis depende de una matriz estructurada que permita una evaluación sistemática:

Tabla N°. 69

Desarrollo de matriz de evaluación Gap Análisis

Desarrollo de matriz de evaluación Gap Análisis		
Estructura de la matriz	A continuación, se expone la selección de campos de importancia que constituirán la matriz de evaluación para el desarrollo del gap análisis	• Dominio • Control • Descripción • Requisito del estándar • Estado actual

Desarrollo de matriz de evaluación Gap Análisis		
		• Nivel de cumplimiento • Brecha identificada • Impacto • Prioridad
Dominios clave para activos IFAS	Los siguientes los dominios a incluir en la matriz de gap análisis.	• Gestión de accesos e identidades • Seguridad de infraestructura • Seguridad de aplicaciones • Gestión de datos • Gestión de incidentes • Continuidad del negocio • Seguridad de terceros • Gobernanza y cumplimiento
Escala de evaluación de cumplimiento	Nivel 1 - No implementado (0%)	• Ausencia total del control
	Nivel 2 - Implementación inicial (25%)	• Implementación ad-hoc o parcial.
	Nivel 3 - Implementación definida (50%)	• Proceso documentado, pero con implementación inconsistente.
	Nivel 4 - Implementación gestionada (75%)	• Proceso implementado y monitorizado regularmente.
	Nivel 5 - Optimizado (100%)	• Proceso completamente implementado con mejora continua.

Nota: información tomada de fuente: *(ISO/IEC, 2022)*

- **Proceso de evaluación**

A continuación, se presenta una propuesta de la metodología a seguir en la ejecución del proceso de evaluación:

Tabla N°. 70

Metodología de implementación Gap Análisis

Metodología de implementación Gap Análisis	
Preparación	• Definición del alcance (activos IFAS específicos) • Selección de los marcos de referencia más importantes • Identificación de los participantes clave (equipos de seguridad, TI, cumplimiento)

Metodología de implementación Gap Análisis	
	• Recopilación de documentación existente (políticas, procedimientos, resultados de auditorías)
Recolección de evidencias	• Entrevistas estructuradas con responsables de controles • Revisión documental de políticas y procedimientos • Observación directa de implementación de controles • Pruebas técnicas de efectividad • Revisión de registros y logs de actividad
Análisis comparativo	• Evaluación sistemática control por control • Determinación del nivel actual de implementación • Análisis de causas raíz para brechas identificadas • Determinación del impacto potencial • Asignación de prioridades

Nota: información tomada de fuente: *(ISO/IEC, 2022)*

2.2.6.1 Ejemplo de gap analysis para controles críticos

A continuación, se expone un ejemplo práctico de la implementación del gap analysis para controles del basados en el estándar ISO 27001 y aplicados a una muestra de activos IFAS identificados en el sector financiero:

Tabla N°. 71

Ejemplo de controles aplicados a IFAS

Ejemplo de controles aplicados a IFAS		
Dominio: Gestión de accesos	Control	A.9.2.3 Gestión de derechos privilegiados
	Requisito del estándar	Los privilegios de acceso deben ser asignados según el principio de mínimo privilegio
	Estado actual	Existen cuentas administrativas compartidas para sistemas críticos
	Nivel	2 (25%)
	Brecha identificada	Ausencia de gestión individualizada de cuentas privilegiadas

Ejemplo de controles aplicados a IFAS		
	Impacto	Alto: imposibilidad de atribución de acciones
	Prioridad	Alta
Dominio: Seguridad de aplicaciones	Control	A.14.2.5 Principios de ingeniería de sistemas seguros
	Requisito del estándar	Los principios de seguridad deben incorporarse en el desarrollo de aplicaciones
	Estado actual	Se realizan pruebas de seguridad post-desarrollo, no existe un SDL formalizado
	Nivel	3 (50%)
	Brecha identificada	Falta combinacion de seguridad en SDLC
	Impacto	Medio: vulnerabilidades detectadas tardíamente
	Prioridad	Media
Dominio: Gestión de datos	Control	A.8.2.3 Manejo de activos
	Requisito del estándar	Procedimientos para manejo de información según su clasificación
	Estado actual	Clasificación de datos implementada, pero sin controles técnicos
	Nivel	3 (50%)
	Brecha identificada	Ausencia de DLP y cifrado para datos críticos

Ejemplo de controles aplicados a IFAS		
Dominio: gestión de incidentes	Impacto	Alto: riesgo de filtración de información sensible
	Prioridad	Alta
	Control	A.16.1.5 Respuesta a incidentes
	Requisito del estándar	Procedimientos definidos para respuesta a incidentes de seguridad
	Estado actual	Plan documentado, pero sin pruebas regulares
	Nivel	3 (50%)
	Brecha identificada	Falta de simulacros y métricas de eficacia
	Impacto	Medio: tiempo de respuesta potencialmente prolongado
	Prioridad	Media

Nota: ejemplo de controles que son referencia para las IFAS

- **Visualización y análisis de resultados:** la representación visual de los resultados facilita la comprensión y toma de decisiones:
    - **Mapa de calor de brechas**: matriz que combina impacto y nivel de cumplimiento para destacar áreas críticas.
    - **Gráfico radar de madurez**: visualización del nivel de madurez por dominio de control**.**
    - **Diagrama de Pareto de brechas**: identificación del 20% de brechas que generan el 80% del riesgo.
- **Plan de remediación:** el análisis de brechas debe traducirse en un plan de acción concreto:

Tabla N°. 72

Estructura plan de remediación para las brechas identificadas

Estructura plan de remediación para las brechas identificadas	
Estructura del plan	• Brecha identificada • Acción correctiva recomendada • Responsable • Recursos requeridos • Plazo de implementación • Métricas de éxito • Dependencias
Priorización de remediaciones	• Críticas: implementación inmediata (0-30 días) • Altas: implementación a corto plazo (30-90 días) • Medias: implementación a mediano plazo (90-180 días) • Bajas: implementación a largo plazo (>180 días)
Estrategias de remediación	• Implementación de nuevos controles • Fortalecimiento de controles existentes • Rediseño de procesos • Adopción de nuevas tecnologías • Capacitación y concienciación

Nota: plan de remediación

- **Monitorización continua:** el Gap Analysis no debe ser un ejercicio puntual, ya que requiere que sea ejecutado continuamente para identificar el estado tanto de las brechas identificadas como si se presentan nuevas brechas a tratar:
    - **Ciclo de evaluación periódica**: definición de actividades de revisión.
        - Revisión trimestral de brechas críticas
        - Evaluación semestral de progreso general
        - Actualización anual completa
    - **Integración con gestión de riesgos**: actualización de identificación asociada al mapa de riesgos.
        - Vinculación de brechas con registro de riesgos
        - Actualización de perfil de riesgo al remediar brechas
        - Métricas de reducción de riesgo
    - **Reporte a la alta dirección**: definición de KPIS en función de medir el avance y progreso.

- Dashboard ejecutivo de estado de brechas
- Indicadores de progreso de remediación
- Análisis de tendencias de madurez

2.2.7 *Simulación de ataques*

Los ejercicios de Red Team representan una metodología de evaluación de seguridad que simula ataques reales para probar la resiliencia para el objeto de este documento de los activos IFAS (MITRE ATT&CK, 2025). En contraste a las pruebas de penetración convencionales, estas actividades adoptan una visión muy completa, emulando las tácticas, técnicas y procedimientosTTPs (Técnicas, Tácticas y Procedimientos) de amenazas reales específicas para entidades del sector financiero (CSRC, SP 800-115, Technical Guide to Information Security Testing and Assessment | , 2008).

2.2.7.1 **Metodología de Red Team para activos IFAS**

La implementación de una metodología de Red Team especializada para activos IFAS (Internet Facing Applications) representa una orientación importante en la protección de sistemas expuestos a internet frente a amenazas cibernéticas avanzadas. Este marco metodológico propone procedimientos organizados y adaptados a las particularidades de aplicaciones con exposición pública, permitiendo emular con precisión las técnicas, tácticas y procedimientos (TTPs) empleados por adversarios. A diferencia de las evaluaciones convencionales, esta metodología ofrece una vista completa de la postura de seguridad de la entidad, abordando tanto vulnerabilidades técnicas como procedimentales y del factor humano, lo que resulta primordial para identificar y remediar rechas de seguridad en las aplicaciones apoyando la primera línea de defensa contra potenciales atacantes externos (CSRC, SP 800-115, Technical Guide to Information Security Testing and Assessment | , 2008).

A continuación, se presenta el esquema metodológico propuesto para realizar la planeación y diseño de in ejercicio Red Team.

Tabla N°. 73

Planificación y diseño del ejercicio Red Team

Planificación y diseño del ejercicio Red Team	
Definición de objetivos	• **Objetivos tácticos:** validar controles específicos. • **Objetivos estratégicos**: evaluar la postura de seguridad de manera completa y precisa. • **Objetivos de detección:** medir capacidades de monitorización y respuesta.
Establecimiento del alcance	• **Definición de límites:** sistemas y aplicaciones incluidos/excluidos. • **Reglas de compromiso:** restricciones operativas y éticas. • **Ventanas de tiempo:** períodos permitidos para ataques activos. • **Comunicaciones:** protocolos para situaciones de emergencia.
Selección de escenarios realistas	• **Basados en inteligencia de amenazas:** TTPs de grupos APT que apuntan al sector financiero. • **Alineados con perfil de riesgo:** escenarios de mayor impacto potencial. • **Diversidad metodológica:** combinación de vectores técnicos, físicos y de ingeniería social.
Formación del equipo	• **Red Team:** especialistas en ofensiva con experiencia en sector financiero. • **Blue Team:** defensores responsables de detección y respuesta. • **White Team:** árbitros que supervisan el ejercicio. • **Observadores:** Stakeholders que analizan el proceso y resultados.
Preparación logística	• **Infraestructura de comando y control:** sistemas seguros para operaciones. • **Herramientas y recursos:** software especializado, equipamiento físico. • **Documentación:** plantillas para reportes, registro de actividades. • **Comunicaciones seguras:** canales cifrados para coordinación del equipo.

Nota: planificación y diseño red time.

2.2.7.2 Ejecución del ejercicio de Red Team

El ejercicio de Red Team para activos IFAS se estructura en fases alineadas con el Cyber Kill Chain y MITRE ATT&CK:

Tabla N°. 74

Fases del ejercicio Red Team

Fases del ejercicio Red Team	
Fase de reconocimiento (Reconnaissance)	• OSINT financiero: recopilación de información pública sobre la entidad. • Análisis de presencia digital: evaluación de huella digital y posibles filtraciones. • Mapeo de infraestructura: identificación de sistemas expuestos • Ingeniería social pasiva: recopilación de información sobre empleados clave.
Fase de armamento y entrega (Weaponization & Delivery)	• Construcción de payloads específicos: malware adaptado para evadir defensas. • Infraestructura de ataque: configuración de servidores de comando y control. • Vectores de entrega: phishing personalizado, documentos maliciosos, dispositivos físicos. • Evasión de defensas: técnicas para eludir soluciones de seguridad.
Fase de explotación y establecimiento (Exploitation & Installation)	• Aprovechamiento de vulnerabilidades: explotación de fallos en sistemas y aplicaciones. • Escalada de privilegios: obtención de accesos elevados • Establecimiento de persistencia: mecanismos para mantener acceso.
Fase de comando y control(Command & Control)	• Movimiento lateral: propagación a sistemas críticos IFAS • Canales encubiertos: comunicaciones ocultas con sistemas comprometidos • Exfiltración de datos: extracción simulada de información sensible • Mantenimiento de acceso: técnicas para permanencia en la red
Fase de acciones sobre objetivos (Actions on Objectives)	• Manipulación de datos financieros: alteración simulada de información crítica. • Compromiso de sistemas transaccionales: acceso a aplicaciones core. • Escenarios de impacto: simulación de fraudes o interrupciones operativas.

Nota: Fases del ejercicio de red times.

2.2.7.3 Escenarios específicos para activos IFAS

A continuación, se detallan escenarios específicos de Red Team diseñados para evaluar la seguridad de activos IFAS críticos en 5 escenarios propuestos:

Tabla N°. 75

Escenarios específicos de activos IFAS

Escenarios específicos de activos IFAS	
Escenario: Compromiso del sistema Core Banking	• **Objetivo:** evaluar la seguridad del sistema central bancario. • **Vector inicial:** phishing dirigido a personal de operaciones. • **Escalada:** movimiento lateral desde estaciones de trabajo. • **Acción final:** intento de manipulación de transacciones. • **Métricas clave:** tiempo hasta detección, capacidad de bloqueo, tiempo de respuesta.
Escenario: Ataque a infraestructura de pagos	• **Objetivo:** evaluar la seguridad de los sistemas de procesamiento de pagos. • **Vector inicial:** explotación de vulnerabilidad en aplicación expuesta. • **Escalada:** pivoteo a través de segmentos de red internos. • **Acción final:** intento de creación de transacciones fraudulentas. • **Métricas clave:** eficacia de segmentación, detección de anomalías transaccionales.
Escenario: Compromiso de banca digital	• **Objetivo:** evaluar la seguridad de plataformas de banca online. • **Vector inicial:** ataque a APIs y servicios web. • **Escalada:** explotación de fallos de lógica de negocio. • **Acción final:** intento de acceso a cuentas de clientes. • **Métricas clave:** robustez de autenticación, monitorización de actividad anómala.
Escenario: Ataque a infraestructura de datos	• **Objetivo:** evaluar la seguridad de bases de datos críticas. • **Vector inicial:** acceso a través de credenciales comprometidas. • **Escalada:** explotación de privilegios excesivos. • **Acción final:** intento de exfiltración de datos de clientes. • **Métricas clave:** eficacia de DLP, cifrado, monitorización de acceso a datos.
Escenario: Compromiso físico y digital combinado	• **Objetivo:** evaluar la seguridad integrada física-digital. • **Vector inicial:** acceso físico no autorizado. • **Escalada:** conexión a red interna, implantación de dispositivos. • **Acción final:** compromiso de sistemas desde interior del perímetro. • **Métricas clave:** controles de acceso físico, segmentación, detección de dispositivos no autorizados.

Nota: escenarios seguridad de activos IFAS

- **Documentación y medición:** un aspecto principal de los ejercicios de Red Team es la documentación detallada de cada una de las etapas propuestas:
    - **Registro detallado de actividades**:

        - Cronología precisa de acciones
        - Técnicas empleadas con referencia a MITRE ATT&CK
        - Evidencias técnicas (capturas, logs)
        - Decisiones y adaptaciones durante el ejercicio
    - **Métricas de detección**:
        - Tasa de detección: porcentaje de técnicas detectadas
        - Tiempo medio de detección (MTTD): rapidez de identificación
        - Precisión de alertas: relación alertas verdaderas vs. falsos positivos
    - **Métricas de respuesta**:
        - Tiempo medio de respuesta (MTTR): velocidad de contención
        - Efectividad de respuesta: capacidad para bloquear avance
        - Coordinación de equipos: eficacia de los protocolos de respuesta
    - **Métricas de resistencia**:
        - Profundidad de compromiso: nivel de acceso alcanzado
        - Impacto potencial: valoración del daño hipotético
        - Robustez de controles: eficacia de las medidas de seguridad
- **Matriz de técnicas y detección**: tabla que correlaciona cada técnica ATT&CK utilizada con:
    - ¿Fue detectada?
    - ¿Cómo fue detectada? (herramienta/proceso)
    - Tiempo hasta detección
    - Eficacia de la respuesta
- **Análisis y reporte de resultados**: el análisis post-ejercicio es necesario para definir el valor del Red Team:

Tabla N°. 76

Análisis y reporte de resultados

Análisis y reporte de resultados	
Sesión de lecciones aprendidas (Purple Team)	• Revisión conjunta Red Team y Blue Team • Análisis de técnicas acertadas y fallidas • Identificación de falsos negativos (ataques no detectados) • Revisión de respuestas eficaces y mejorables

Análisis y reporte de resultados	
Informe ejecutivo	• Resumen de hallazgos críticos • Valoración del nivel de riesgo • Recomendaciones estratégicas • Comparativa con ejercicios anteriores
Informe técnico detallado	• Descripción técnica de cada técnica empleada • Vulnerabilidades explotadas • Controles evadidos • Recomendaciones técnicas específicas • Evidencias y pruebas
Plan de remediación priorizado	• Acciones inmediatas (quick wins) • Mejoras a corto plazo • Iniciativas estratégicas a largo plazo • Asignación de responsabilidades y plazos

Nota: análisis post-ejercicio

- **Integración con el programa de seguridad:** los resultados del Red Team deben integrarse en el programa de seguridad más amplio:

Tabla N°. 77

Integración con el programa de seguridad

Integración con el programa de seguridad	
Actualización de métricas de postura de seguridad	• Incorporación de hallazgos al dashboard de seguridad • Actualización de indicadores de riesgo • Revisión de KPIs de seguridad
Vinculación con otras iniciativas	• Alimentación del programa de gestión de vulnerabilidades • Actualización de planes de respuesta a incidentes • Mejora de programas de concienciación
Ciclo de mejora continua	• Programación de verificaciones de remediación • Planificación de futuros ejercicios • Actualización de escenarios basada en amenazas emergentes
Formación de equipos internos	• Transferencia de conocimientos al Blue Team • Crecimiento de capacidades internas de simulación • Creación de escenarios de entrenamiento

Nota: integración con el programa de seguridad

2.2.7.4 Consideraciones especiales para entidades financieras

Las entidades financieras deben tener en cuenta aspectos particulares al realizar ejercicios de Red Team:

Tabla N°. 78

Consideraciones especiales para entidades financieras

Consideraciones especiales para entidades financieras	
Cumplimiento regulatorio	• Alineación con marcos como TIBER-EU para pruebas basadas en inteligencia • Documentación para satisfacer requisitos regulatorios. • Notificación a reguladores cuando sea necesario
Gestión de riesgos operativos	• Protocolos para evitar impacto en sistemas productivos • Mecanismos de reversión en caso de afectación no planeada • Ventanas de ejecución durante periodos de baja actividad
Confidencialidad	• Acuerdos de confidencialidad (NDAs) estrictos • Manejo seguro de hallazgos y documentación • Control de acceso a la información del ejercicio.
Tercerización vs. capacidades internas	• Evaluación de proveedores especializados • Construcción progresivo de capacidades internas • Modelo híbrido con transferencia de conocimiento

Nota: ejercicios propuestos de red times

2.2.7.5 Ejemplo de calendario de implementación

Un programa completo de Red Team para activos IFAS puede estructurarse de la siguiente manera:

Tabla N°. 79

Calendario propuesto de implementación de ejercicio Red Time

Calendario propuesto de implementación de ejercicio Red Time	
Trimestre 1: preparación y planificación	• Desarrollo de objetivos y alcance • Selección de escenarios • Preparación logística
Trimestre 2: ejecución de escenarios técnicos	• Escenario de compromiso de Core Banking • Escenario de ataque a infraestructura de pagos
Trimestre 3: ejecución de escenarios de aplicaciones y datos	• Escenario de compromiso de banca digital • Escenario de ataque a infraestructura de datos
Trimestre 4: escenario combinado y cierre	• Escenario físico-digital • Análisis global y planificación siguiente ciclo

Nota: Calendario red time

2.2.7.6 Tecnologías y herramientas recomendadas en entornos financieros

Para la ejecución satisfactoria de los ejercicios de Red Team en entornos financieros se recomienda:

- **Plataformas de emulación de adversarios**:
  - Breach and Attack Simulation (BAS)
  - Plataformas de automatización de Red Team
  - Frameworks como Atomic Red Team, Calder
- **Infraestructura segura**:
  - Entornos aislados para pruebas
  - Canales cifrados para comunicaciones
  - Sistemas seguros para almacenar hallazgos
- **Herramientas de análisis**:
- Plataformas de navegación ATT&CK
  - Sistemas de visualización de campañas
  - Herramientas de análisis de detección y respuesta

La implementación sistemática de ejercicios de Red Team proporciona una evaluación realista de la resiliencia de los activos IFAS críticos.

2.2.8 *Análisis final fase 2*

La aplicación de una metodología de Red Team para activos IFAS (Internet Facing Applications) es necesaria para evidenciar el avance de la seguridad al interno de la entidad. A través del análisis de riesgos tomados del marco NIST SP 800-30 (NIST, Cybersecurity Framework | NIST, 2013), se ha logrado categorizar y priorizar las amenazas potenciales según su impacto y probabilidad, facilitando así la asignación optima de recursos defensivos. La detección organizada de brechas mediante Gap Analysis apoya la identificación de oportunidades de mejora entre los controles implementados actualmente y los estándares internacionales de ciberseguridad, estableciendo una guía básica que permite el fortalecimiento progresivo de las defensas.

Los resultados al final del desarrollo del guía definido en la fase 2 están enfocados en la identificación de un activo intangible pero esencial para la organización. La identificación constante de vulnerabilidades en los activos IFAS proporciona una ventaja decisiva en un entorno en constante cambio con múltiples actores maliciosos, permitiendo la implementación de controles compensatorios antes de que estas debilidades sean explotadas en escenarios reales.

2.3 Fase 3: diseño de un modelo control de buenas prácticas de ciberseguridad implementando controles y procedimientos de contención y mitigación.

La ciberseguridad actualmente requiere un tratamiento preventivo no solamente reactivo. En esta fase se evidenciarán técnicas para la protección para activos IFAS, abordando desde la identificación de vulnerabilidades hacia la implementación de un marco defensivo y con actualización continua. Basándonos en los hallazgos de las fases previas de evaluación, este modelo establece una estructura de protección proactiva, detección temprana y respuesta eficiente, adaptada específicamente a las necesidades y riesgos identificados en el entorno de las IFAS. El objetivo primordial es desarrollar un ecosistema de seguridad resiliente que no solo responda a las amenazas actuales, sino que evolucione continuamente frente al continuo cambio de las ciberamenazas.

2.3.1 *Definición de controles*

La implementación de controles de seguridad son la primera línea de defensa en un modelo de buenas prácticas. Este componente establece algunos parámetros de protección técnicos y administrativos necesarios para proteger los activos IFAS contra amenazas conocidas y emergentes. Los controles presentados sé han identificado siguiendo un planteamiento de defensa, donde múltiples capas de seguridad complementarias ofrecen protección redundante en caso de que un sean comprometidos. La selección de estos controles responde directamente a las vulnerabilidades y brechas identificadas en las fases anteriores, priorizando aquellos que ofrecen la mayor reducción de riesgo con una implementación eficiente y sostenible. Cada control ha sido evaluado considerando su efectividad, impacto operacional, requisitos de recursos y alineación con estándares internacionales de seguridad**.**

Durante esta fase se busca establecer un modelo centrado en la protección proactiva y respuesta a incidentes para activos IFAS, estableciendo un marco de seguridad sostenible y adaptable a los contantes cambios de las amenazas.

2.3.2 *Definición de Controles*

2.3.2.1 **Controles técnicos**

- Encriptación: la implementación de controles de encriptación es uno de los principales componentes en la arquitectura de seguridad para la protección de activos digitales críticos. Este mecanismo de defensa transforma la información sensible mediante algoritmos criptográficos avanzados, convirtiendo datos legibles en formatos cifrados que resultan indescifrables sin las correspondientes claves de acceso. La correcta implementación de estos controles no solo satisface requisitos regulatorios cada vez más exigentes, sino que establece una capa de protección esencial frente a accesos no autorizados, interceptaciones y exfiltraciones de datos, incluso en escenarios donde otros mecanismos de seguridad perimetral hayan sido comprometidos.

Tabla N°. 80

Encriptación

Encriptación	
Implementación de encriptación en reposo	• Cifrado de bases de datos que contienen información sensible • Encriptación de dispositivos de almacenamiento (discos duros, backups) • Gestión de claves criptográficas con rotación periódica
Encriptación en tránsito	• Uso obligatorio de TLS 1.3 o superior para todas las comunicaciones web • Implementación de VPN para accesos remotos • Establecimiento de túneles cifrados para comunicaciones entre activos IFAS

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.2.2 Segmentación de redes

La segmentación de redes establece perímetros de seguridad internos que limitan el movimiento lateral de potenciales atacantes. Al crear segmentos basados en criterios funcionales, niveles de sensibilidad y requisitos de acceso, la segmentación proporciona una protección definida que dificulta la ejecución de amenazas y facilita la detección de actividades que presenten desviaciones en el proceso al interno de las entidades.

Tabla N°. 81

Segmentación de red

Segmentación de red	
Arquitectura de red por zonas	• Creación de zonas desmilitarizadas (DMZ) para servicios expuestos • Microsegmentación basada en funcionalidades y niveles de criticidad • Aislamiento de redes para sistemas IFAS críticos
Implementación de controles de perímetro	• Despliegue de firewalls de nueva generación (NGFW • Sistemas de prevención de intrusiones (IPS/IDS) • Filtrado avanzado de contenido en puntos de entrada/salida
Control de flujos de tráfico interno	• Establecimiento de listas de control de acceso (ACL) granulares • Implementación de tecnología Zero Trust Network Access (ZTNA) • Monitorización continua de comunicaciones entre segmentos

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.2.3 Protección de endpoints

La protección de endpoints es una línea de defensa crucial en la línea de ciberseguridad organizacional, enfocándose en proteger dispositivos finales como ordenadores, portátiles y

dispositivos móviles los cuales son accesos frecuentemente explotados por atacantes. Este control implementa soluciones que combinan antimalware avanzado, sistemas de prevención de intrusiones, control de aplicaciones y tecnologías de detección y respuesta (EDR), creando un escudo protector que identifica y neutraliza amenazas antes de que puedan comprometer activos críticos (Microsoft Defender for Endpoint, 2025).

Tabla N°. 82

Protección de Endpoints

Protección de Endpoints	
Soluciones de protección avanzada	• EDR (Endpoint Detection and Response) • Protección contra malware basada en comportamiento • Sistemas de prevención de pérdida de datos (DLP)
Control de dispositivos y aplicaciones	• Gestión de dispositivos móviles (MDM) • Listas blancas de aplicaciones permitidas • Control de medios extraíbles

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.2.4 Gestión de identidades y accesos

La gestión de identidades y accesos es un componente crítico del entorno de seguridad que regula quién puede acceder a qué recursos dentro de la estructura organizacional. Este control establece una base para el control de autenticación, autorización y auditoría de usuarios, implementando el principio del mínimo privilegio y la segregación de funciones para minimizar la superficie de ataque. Mediante sistemas centralizados de identidad, autenticación multifactor y políticas de acceso, se establece un equilibrio estratégico entre usabilidad y seguridad, previniendo accesos no autorizados y limitando el potencial impacto de credenciales comprometidas.

Tabla N°. 83

Gestión de identidades y accesos

Gestión de identidades y accesos	
Implementación de autenticación	• Autenticación multifactor (MFA) para todos los accesos críticos • Single Sign-On (SSO) con controles de seguridad reforzados • Autenticación biométrica donde sea aplicable

Gestión de identidades y accesos	
Gestión centralizada de identidades	• Directorio unificado con sincronización segura • Sistema de aprovisionamiento y desaprovisionamiento automatizado • Reconciliación periódica de identidades y permisos

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.3 *Controles Administrativos*

2.3.3.1 Políticas de acceso mínimo privilegio

El principio de acceso mínimo o representa establece que cada usuario, proceso o sistema debe operar únicamente con los privilegios necesarios para desempeñar sus funciones asignadas. Este control crítico minimiza los riegos asociados a la superficie de ataque al restringe los permisos asignados. Con el uso de estas políticas, se logra establecer medidas en la escalada de privilegios y el acceso no autorizado a los activos de información.

A continuación, se presentan los tres ítems a considerar en la implementación del control de mínimo privilegio.

Tabla N°. 84

Políticas de Acceso mínimo privilegio

Políticas de Acceso mínimo privilegio	
Matriz de accesos basada en roles	• Definición clara de perfiles de acceso alineados con funciones laborales • Revisión periódica de privilegios asignados (trimestralmente) • Procesos específicos para solicitud y aprobación de excepciones
Segregación de funciones (SoD)	• Identificación de funciones incompatibles • Implementación de controles preventivos y detectivos • Auditoría regular de cumplimiento
Gestión de cuentas privilegiadas	• Sistema de gestión de accesos privilegiados (PAM) • Registro detallado de actividades administrativas • Renovación automática de credenciales privilegiadas

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.3.2 Políticas y procedimientos

Las políticas y procedimientos de seguridad son la base del marco normativo y operacional de una organización y en ellas se definen las responsabilidades y procesos para la protección de activos de información. A través de una documentación completa, actualizada continuamente y socializada a todos los colaboradores dentro de la entidad, se logra garantizar el cumplimiento regulatorio y se crea en paralelo una cultura de seguridad.

A continuación, los ítems asociados a la construcción de un marco normativo y procedimental robusto.

Tabla N°. 85

Políticas y procedimientos

Políticas y procedimientos	
Desarrollo de política marco de seguridad	• Alineación con estándares ISO 27001 y NIST • Compromiso documentado de la alta dirección • Revisión anual obligatoria
Procedimientos operativos estandarizados	• Procedimientos de gestión de cambios • Protocolos de respuesta a incidentes • Procesos de gestión de vulnerabilidades
Normativas específicas para activos IFAS	• Clasificación y manejo de información • Requisitos de seguridad para desarrollo y adquisición • Directrices para transferencia de información

Nota: documento de políticas y procedimientos

2.3.3.3 Concientización y capacitación

La concientización y capacitación en ciberseguridad son esenciales en todas las entidades, ya que permite que todos los funcionarios tengan herramientas de seguridad y así mismo identificar más claramente si se encuentran bajo un ataque. Esta etapa se centra en entrenar el factor humano como primera línea defensiva mediante programas de capacitación ya sea técnica o de simulación. Al cultivar una cultura de seguridad de la información donde cada funcionario comprende su rol en la protección de activos digitales, reconoce indicadores de ataque y responde adecuadamente ante incidente, la organización establece una barrera cognitiva que complementa las defensas técnicas y mitiga eficazmente riesgos asociados a ingeniería social o phishing.

Tabla N°. 86

Concienciación y capacitaciones

Concienciación y capacitaciones	
Programa continuo de sensibilización	• Campañas periódicas sobre amenazas emergentes • Simulaciones de phishing con orientación educativa • Materiales adaptados a diferentes perfiles de usuario
Formación especializada	• Capacitación técnica para equipos de TI y seguridad • Entrenamiento específico para custodios de activos IFAS • Certificaciones según roles y responsabilidades

Concienciación y capacitaciones	
Cultura de seguridad	• Programa de reconocimiento para comportamientos seguros • Participación en comunidades de seguridad • Promoción de reportes de incidentes sin represalias

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.3.4 Estrategia de implementación y gestión de controles de seguridad

La estrategia de implementación y gestión de controles de seguridad es una guía de transformación de la teoría en herramientas defensivas totalmente funcionales. Conformando un esquema de implementación, configuración y actualización continua como medida de protección ante las diversas amenazas del entono, ya que define el orden de prioridad haciendo base en los análisis de riesgos previos, asignando responsabilidades claras y estableciendo indicadores de desempeño medibles.

Tabla N°. 87

Estrategia de implementación y gestión de controles de seguridad

Estrategia de implementación y gestión de controles de seguridad	
Priorización Basada en Riesgos	• Evaluación del impacto potencial y probabilidad de amenazas • Clasificación de controles por criticidad y eficiencia • Desarrollo de mapa de ruta de implementación por fases
Medición de Efectividad	• Definición de KPIs de seguridad alineados con objetivos • Establecimiento de línea base y métricas de mejora • Tableros de control para seguimiento de madurez
Actualización y mejora continua	• Ciclos regulares de revisión y actualización • Incorporación de lecciones aprendidas de incidentes • Adaptación proactiva ante nuevas amenazas y tecnologías

Nota: implementación de estrategias y gestión de controles de seguridad

2.3.4 *Gestión de incidentes de seguridad*

La gestión de incidentes de seguridad define la capacidad organizacional para detectar, analizar, contener, erradicar y recuperarse de eventos que comprometen la confidencialidad, integridad o disponibilidad de los activos de información. A continuación, se presentan los cuatro ítems principales a tener encuentra frente a la estructura de plan de gestión de incidentes.

Tabla N°. 88

Gestión de incidentes

Gestión de incidentes	
Preparación y Planificación	• Desarrollo de planes de respuesta a incidentes • Establecimiento de equipos de respuesta (CSIRT) • Creación de runbooks para escenarios más probables
Detección y Análisis	• Implementación de capacidades de monitoreo 24/7 • Correlación avanzada de eventos de seguridad • Procedimientos de escalamiento y clasificación de incidentes
Contención, Erradicación y Recuperación	• Protocolos de aislamiento de sistemas comprometidos • Procedimientos forenses y de preservación de evidencia • Planes de continuidad y recuperación ante desastres
Actividades Post-Incidente	• Análisis de causa raíz • Documentación de lecciones aprendidas • Actualización de controles basada en hallazgos

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.5 *Cumplimiento y gobernanza*

El cumplimiento y gobernanza en ciberseguridades el marco regulatorio que asegura la alineación defensiva en conjunto con requisitos legales, estándares y objetivos de la entidad. Mediante políticas bien definidas, roles y responsabilidades claramente asignados, y procesos de auditoría.

Tabla N°. 89

Cumplimiento y gobernanza

Cumplimiento y Gobernanza	
Marco Regulatorio	• Mapeo de requisitos legales y regulatorios aplicables • Procesos de evaluación periódica de cumplimiento • Gestión de relaciones con reguladores y auditores
Gobernanza de Seguridad	• Estructura de comités y roles de responsabilidad • Reportes ejecutivos de estado de seguridad • Integración con gobierno corporativo
Gestión de Terceros	• Evaluación de seguridad de proveedores y socios • Cláusulas contractuales de seguridad • Monitoreo continuo de riesgos de terceros

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.6 *Resiliencia operativa*

Esta fase establece los fundamentos para un modelo de buenas prácticas de ciberseguridad, el cual permite ser adaptable y enfocado en la protección constante de los activos IFAS, complementando las fases previas de evaluación y análisis con acciones concretas de implementación (BSI, 2019).

Tabla N°. 90

Resiliencia operativa

Resiliencia operativa	
Continuidad del Negocio	• Análisis de impacto al negocio (BIA) • Estrategias de recuperación por tipo de activo IFAS • Pruebas periódicas de planes de continuidad
Gestión de Crisis	• Protocolos de comunicación durante incidentes • Roles y responsabilidades del equipo de crisis • Simulacros y ejercicios de mesa
Documentación y Evidencias	• Repositorio centralizado de documentación • Registro auditable de actividades de seguridad • Trazabilidad de decisiones y acciones

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

2.3.7 *Procedimientos de respuesta a incidentes para activos IFAS*

A continuación, desarrollaré los procedimientos de respuesta a incidentes basados en NIST IR 8353 para activos IFAS, enfocándome en escenarios de ransomware y filtración de datos.

2.3.7.1 Fundamentos de los procedimientos de respuesta a incidentes

Los procedimientos que se presentan a continuación están basados en el marco de trabajo establecido en la publicación especial NIST IR (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021).

Los playbook para respuesta ante incidentes se definen a partir de establecer un protocolo completo en el que se establece procedimientos operativos básicos que permitan hacer frente a las amenazas qué sean de tipo disruptivo. A continuación, se definen una secuencia la de acciones o actividades, así como la asignación de responsabilidades y los medios de comunicación que se deben activar desde que se inicia el proceso de incidencia hasta la recuperación de los sistemas afectados.

2.3.7.2 Playbook para respuesta ante incidentes de ransomware

El playbook para respuesta ante incidentes de ransomware se define a partir de establecer un esquema desde la preparación, detección, contención erradicación, recuperación y lecciones aprendidas (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021).

- **Preparación**

Tabla N°. 91

Playbook preparación

Actividad	Descripción	Fuente
Inventario de activos IFAS	Mantener un inventario actualizado de todos los activos IFAS, incluyendo sistemas, aplicaciones y datos críticos.	NIST IR 8353, Sección 2.1 "Identify"
Evaluación de riesgos	Realizar evaluaciones periódicas de vulnerabilidades específicas para activos IFAS.	NIST IR 8353, Sección 2.1.2 "Risk Assessment"
Capacitación del personal	Entrenar al personal en la identificación y reporte de posibles incidentes de ransomware.	NIST IR 8353, Sección 2.2.3 "Awareness and Training"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Detección**

Tabla N°. 92

Playbook detección

Actividad	Descripción	Fuente
Monitoreo continuo	Implementar sistemas de detección de anomalías en la red y comportamientos sospechosos.	NIST IR 8353, Sección 2.3.1 "Anomalies and Events"
Alertas tempranas	Configurar alertas para actividades como cifrado masivo de archivos o comunicaciones con servidores de comando y control.	NIST IR 8353, Sección 2.3.2 "Security Continuous Monitoring"
Identificación de IOCs	Mantener actualizados los indicadores de compromiso (IOCs) asociados con ransomware.	NIST IR 8353, Sección 2.3.3 "Detection Processes"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Contención**

Tabla N°. 93

Playbook Contención

Actividad	Descripción	Fuente
Aislamiento de sistemas	Desconectar inmediatamente los sistemas IFAS comprometidos de la red.	NIST IR 8353, Sección 2.4.2 "Mitigation"
Bloqueo de tráfico malicioso	Implementar reglas de firewall para bloquear comunicaciones con infraestructura del atacante.	NIST IR 8353, Sección 2.4.1 "Response Planning"
Preservación de evidencia	Realizar copias forenses de los sistemas afectados antes de cualquier acción de recuperación.	NIST IR 8353, Sección 2.4.3 "Improvements"

- Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Erradicación**

Tabla N°. 94

Playbook erradicación

Actividad	Descripción	Fuente
Análisis de malware	Identificar la variante específica de ransomware para determinar vectores de eliminación.	NIST IR 8353, Sección 2.4.2 "Mitigation"
Eliminación del malware	Utilizar herramientas especializadas para eliminar el ransomware de los sistemas afectados.	NIST IR 8353, Sección 2.5.1 "Recovery Planning"
Verificación de limpieza	Confirmar que todos los componentes maliciosos han sido removidos.	NIST IR 8353, Sección 2.5.2 "Improvements"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Recuperación**

Tabla N°. 95

Playbook recuperación

Actividad	Descripción	Fuente
Restauración de datos	Restaurar datos desde copias de seguridad verificadas como no comprometidas.	NIST IR 8353, Sección 2.5.1 "Recovery Planning"

Actividad	Descripción	Fuente
Reconfiguración de sistemas	Reinstalar y reconfigurar sistemas IFAS siguiendo prácticas de seguridad.	NIST IR 8353, Sección 2.5.3 "Communications"
Verificación funcional	Probar la funcionalidad completa de los sistemas recuperados antes de reintegrarlos.	NIST IR 8353, Sección 2.5.2 "Improvements"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Lecciones aprendidas**

Tabla N°. 96

Playbook lecciones aprendidas

Actividad	Descripción	Fuente
Análisis post-incidente	Documentar detalladamente el incidente, incluyendo vectores de ataque y eficacia de la respuesta.	NIST IR 8353, Sección 2.4.3 "Improvements"
Actualización de controles	Reforzar controles de seguridad basados en las vulnerabilidades explotadas.	NIST IR 8353, Sección 2.5.2 "Improvements"
Mejora de playbooks	Actualizar los procedimientos de respuesta según las lecciones aprendidas.	NIST IR 8353, Sección 2.4.3 "Improvements"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

2.3.7.3 Playbook para respuesta ante incidentes de filtración de datos

- Preparación

Tabla N°. 97

Playbook preparación 2

Actividad	Descripción	Fuente
Clasificación de datos	Identificar y clasificar datos sensibles en los activos IFAS.	NIST IR 8353, Sección 2.1.1 "Asset Management"
DLP y monitoreo	Implementar soluciones de prevención de pérdida de datos para detectar transferencias anómalas.	NIST IR 8353, Sección 2.2.5 "Information Protection Processes and Procedures"

Actividad	Descripción	Fuente
Definición de umbrales	Establecer umbrales claros para activar la respuesta a incidentes de filtración.	NIST IR 8353, Sección 2.4.1 "Response Planning"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Detección**

Tabla N°. 98

Playbook detección 2

Actividad	Descripción	Fuente
Monitoreo de exfiltración	Implementar monitoreo de tráfico saliente para detectar transferencias sospechosas de datos.	NIST IR 8353, Sección 2.3.2 "Security Continuous Monitoring"
Alertas de acceso inusual	Configurar alertas para accesos anómalos a datos sensibles en los activos IFAS.	NIST IR 8353, Sección 2.3.1 "Anomalies and Events"
Monitoreo de repositorios	Vigilar la aparición de datos corporativos en repositorios públicos o dark web.	NIST IR 8353, Sección 2.3.3 "Detection Processes"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Contención**

Tabla N°. 99

Playbook contención 2

Actividad	Descripción	Fuente
Revocación de accesos	Revocar inmediatamente credenciales comprometidas y tokens de acceso.	NIST IR 8353, Sección 2.4.2 "Mitigation"
Aislamiento de sistemas	Aislar sistemas IFAS comprometidos para prevenir mayor exfiltración.	NIST IR 8353, Sección 2.4.2 "Mitigation"
Bloqueo de canales	Identificar y bloquear canales utilizados para la exfiltración de datos.	NIST IR 8353, Sección 2.4.1 "Response Planning"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Evaluación de impacto**

Tabla N°. 100

Playbook evaluación impacto 2

Actividad	Descripción	Fuente
Verificación de datos expuestos	Determinar qué datos específicos fueron comprometidos y su sensibilidad.	NIST IR 8353, Sección 2.4.1 "Response Planning"
Análisis forense	Realizar análisis forense para determinar el alcance y método de la filtración.	NIST IR 8353, Sección 2.4.3 "Improvements"
Evaluación de obligaciones legales	Determinar requisitos de notificación según regulaciones aplicables.	NIST IR 8353, Sección 2.4.3 "Improvements"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Notificación y comunicación**

Tabla N°. 101

Playbook comunicación 2

Actividad	Descripción	Fuente
Notificación interna	Notificar a la dirección ejecutiva y departamentos de la entidad.	NIST IR 8353, Sección 2.4.3 "Improvements"
Notificación a reguladores	Informar a las autoridades regulatorias según los requisitos aplicables.	NIST IR 8353, Sección 2.4.3 "Improvements"
Comunicación a afectados	Notificar a individuos afectados por la filtración de datos.	NIST IR 8353, Sección 2.5.3 "Communications"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Remediación**

Tabla N°. 102

Playbook remediación 2

Actividad	Descripción	Fuente
Eliminación de brechas	Corregir vulnerabilidades que permitieron la filtración.	NIST IR 8353, Sección 2.5.1 "Recovery Planning"
Protección adicional	Implementar controles adicionales para datos sensibles.	NIST IR 8353, Sección 2.5.2 "Improvements"
Monitoreo avanzado	Incrementar monitoreo de actividades relacionadas con los datos comprometidos.	NIST IR 8353, Sección 2.5.2 "Improvements"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

- **Lecciones aprendidas**

Tabla N°. 103

Playbook lecciones aprendidas 2

Actividad	Descripción	Fuente
Análisis de causa raíz	Identificar causas principales que permitieron la filtración.	NIST IR 8353, Sección 2.4.3 "Improvements"
Mejora de controles	Reforzar controles de seguridad para prevenir incidentes similares.	NIST IR 8353, Sección 2.5.2 "Improvements"
Actualización de políticas	Revisar y actualizar políticas de gestión de datos según lecciones aprendidas.	NIST IR 8353, Sección 2.5.2 "Improvements"

Nota: tomado de la fuente *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

2.3.7.4 Consideraciones específicas para activos IFAS

Las actividades descritas en ambos playbooks deben adaptarse considerando las características específicas de los activos IFAS propios de cada organización, incluyendo:

- Priorización de la continuidad operativa de servicios financieros críticos (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021).
- Coordinación con reguladores financieros durante la respuesta a incidentes (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021).
- Consideración del impacto reputacional en entidades financieras (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021).

Estos playbooks proporcionan una base para responder de manera eficaz a incidentes de ransomware y filtración de datos en activos IFAS, aplicando las mejores prácticas descritas por NIST.

2.3.8 *Integración de estándares: alineación del modelo con ISO 27001 y NIST CSF*

A continuación, se desarrollará la integración de estándares ISO 27001 (Anexo A) y NIS para el establecimiento de un modelo de buenas prácticas de ciberseguridad enfocado en activos IFAS, presentando la información en cuadros para facilitar su comprensión y aplicación práctica para cada uno de los ítems de las guías de buenas prácticas (ISO/IEC 27002:2022, 2022).

2.3.8.1 Marco de integración

La siguiente tabla muestra el planteamiento de integración utilizado para alinear ambos estándares:

Tabla N°. 104

Marco de integración

Marco de integración		
Aspecto	**Descripción**	**Fuente**
Planteamiento de integración	Mapeo cruzado de controles y funciones para crear un marco unificado	ISO 27001:2022, Introducción; NIST CSF v1.1, Sección 3.1
Beneficio principal	Cumplimiento regulatorio combinado con una orientación operativa práctica	ISO 27001:2022, Sección 0.1; NIST CSF v1.1, Resumen Ejecutivo
Aplicabilidad	Adaptado específicamente para protección de activos IFAS	Basado en análisis de requisitos del sector financiero

Nota: esquema de marco de integración

2.3.8.2 Alineación de funciones NIST CSF con dominios ISO 27001

2.3.8.2.1 Función: idenificar

La alineación estratégica entre la función "IDENTIFICAR" del Marco de Ciberseguridad del NIST (CSF) y los dominios correspondientes de ISO 27001 representa la necesidad de establecer una administración de riesgos completa. Esta incorporación vincula el concepto proactivo de identificación de activos con esta orientación en entornos operativos y amenazas potenciales propuesto por NIST con los requerimientos de la norma ISO para la gestión del contexto organizacional y evaluación de riesgos. Al mapear las categorías y subcategorías de la función "IDENTIFICAR" contra los controles específicos de ISO 27001 (ISO/IEC 27002:2022, 2022), las organizaciones establecen una base sólida para desarrollar un entendimiento contextualizado de sus activos críticos y del panorama de amenazas importantes que permitan facilitar la priorización de recursos defensivos y el cumplimiento simultáneo de ambos marcos de referencia sin redundancias o inconsistencias.

Tabla N°. 105

Alineación función Identificar con ISO 27001

Alineación función Identificar con ISO 27001			
Control ISO 27001	**Implementación para IFAS**	**Referencia cruzada NIST CSF**	**Fuente**
A.5.1 Políticas de seguridad	Desarrollo de políticas específicas para activos IFAS	ID.GV-1 Política de seguridad establecida	ISO 27001:2022, A.5.1; NIST CSF v1.1, Categoría ID.GV
A.8.1 Gestión de activos	Inventario detallado de activos IFAS con clasificación de criticidad	ID.AM-1 Inventario de dispositivos físicos	ISO 27001:2022, A.8.1; NIST CSF v1.1, Categoría ID.AM
A.5.7 Gestión de riesgos	Metodología de evaluación de riesgos adaptada para activos financieros	ID.RA-1 Vulnerabilidades identificadas	ISO 27001:2022, A.5.7; NIST CSF v1.1, Categoría ID.RA
A.5.23 Identificación de requisitos	Mapeo de requisitos regulatorios específicos del sector financiero	ID.GV-2 Cumplimiento de requisitos legales	ISO 27001:2022, A.5.23; NIST CSF v1.1, Categoría ID.GV
A.5.2 Roles y responsabilidades	Definición de roles para gestión de activos IFAS	ID.AM-6 Roles y responsabilidades	ISO 27001:2022, A.5.2; NIST CSF v1.1, Categoría ID.AM

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.2.2 Función: proteger

La función "PROTEGER" del Marco de Ciberseguridad del NIST (CSF) (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021) y su alineación estratégica con los dominios de ISO 27001. Esta colaboración metodológica agrupa las tecnicas defensivas estratégicas diseñadas por NIST —enfocadas en la producción y puesta en marcha de controles técnicos, administrativos y físicos— con las exigencias estructuradas de la norma ISO para la protección de los activos de información a lo largo de todo su ciclo de vida. A través del mapeo de categorías como la gestión de identidad, la concienciación, la seguridad de los datos y los procesos de protección contra las cláusulas y controles específicos de ISO 27001 (ISO/IEC, 2022), las entidades crean un marco unificado que no solo fortalece su estrategia defensiva sino que

también maximiza recursos al cumplir con varios requisitos de cumplimiento mediante controles unificados, incrementando de esta manera la eficiencia en las operaciones sin poner en riesgo la confiabilidad delas medidas implementadas.

Tabla N°. 106

Alineación función Proteger con ISO 27001

Alineación función Proteger con ISO 27001			
Control ISO 27001	**Implementación para IFAS**	**Referencia cruzada NIST CSF**	**Fuente**
A.5.14 Control de acceso	Implementación de acceso basado en roles para sistemas financieros	PR.AC-4 Gestión de permisos	ISO 27001:2022, A.5.14; NIST CSF v1.1, Categoría PR.AC
A.8.8 Gestión de secretos	Protección reforzada de credenciales para activos IFAS	PR.DS-5 Protección contra fugas de datos	ISO 27001:2022, A.8.8; NIST CSF v1.1, Categoría PR.DS
A.5.33 Protección de registros	Implementación de registros inalterables para transacciones financieras	PR.PT-1 Auditoría/registros de eventos	ISO 27001:2022, A.5.33; NIST CSF v1.1, Categoría PR.PT
A.8.9 Controles criptográficos	Cifrado de datos financieros en reposo y en tránsito	PR.DS-1 Datos en reposo protegidos	ISO 27001:2022, A.8.9; NIST CSF v1.1, Categoría PR.DS
A.8.29 Seguridad en desarrollo	Implementación de DevSecOps para aplicaciones financieras	PR.IP-2 Ciclo de vida de desarrollo seguro	ISO 27001:2022, A.8.29; NIST CSF v1.1, Categoría PR.IP

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.2.3 Función: detectar

La función "DETECTAR" del Marco de Ciberseguridad del NIST (CSF) (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021) conecta las prácticas de inspección constante, identificación de irregularidades y supervisión de la seguridad impulsadas por NIST con los controles particulares de ISO 27001 (ISO/IEC 27002:2022, 2022)vinculados con el seguimiento, registro y administración de eventos. A través de esta metodología se implementan procesos y tecnologías para gestionar la identificación temprana de actividades maliciosas,

estableciendo mecanismos de alerta que reducen el tiempo entre la ocurrencia de una brecha y su detección, factor determinante para minimizar el impacto de los incidentes de seguridad.

Tabla N°. 107

Alineación función Detectar con ISO 27001

Alineación función Detectar con ISO 27001			
Control ISO 27001	**Implementación para IFAS**	**Referencia cruzada NIST CSF**	**Fuente**
A.8.16 Monitoreo	Implementación de SIEM con reglas específicas para activos IFAS	DE.CM-1 Monitoreo de red	ISO 27001:2022, A.8.16; NIST CSF v1.1, Categoría DE.CM
A.8.15 Vulnerabilidades técnicas	Escaneo continuo de vulnerabilidades en sistemas financieros	DE.CM-8 Escaneos de vulnerabilidades	ISO 27001:2022, A.8.15; NIST CSF v1.1, Categoría DE.CM
A.5.20 Análisis de eventos	Análisis de comportamiento de usuarios en sistemas financieros	DE.AE-3 Datos de eventos agregados	ISO 27001:2022, A.5.20; NIST CSF v1.1, Categoría DE.AE
A.5.33 Auditoría	Implementación de auditorías automáticas de transacciones sospechosas	DE.CM-7 Monitoreo de actividades no autorizadas	ISO 27001:2022, A.5.33; NIST CSF v1.1, Categoría DE.CM
A.5.19 Detección proactiva	Uso de threat hunting para detectar amenazas avanzadas a IFAS	DE.DP-5 Proceso de mejora continua	ISO 27001:2022, A.5.19; NIST CSF v1.1, Categoría DE.DP

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.2.4 Función: responder

La función "RESPONDER" del Marco de Ciberseguridad del NIST (CSF) (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021) define la capacidad de la entidad para contener el impacto de incidentes de seguridad una vez detectados. Lo que logra vincular los procesos de planificación, comunicación, análisis, mitigación y mejora de respuesta establecidos por NIST con los controles específicos de ISO 27001 (ISO/IEC 27002:2022, 2022) relacionados con la gestión de incidentes y continuidad del negocio. Las entidades establecen protocolos estructurados y capacidades operativas para reaccionar de manera rápida ante eventos inesperados,

aplicando recursos técnicos y humanos para tratar de minimizar amenazas, mientras documentan lecciones aprendidas que fortalecen progresivamente la resiliencia operacional frente a eventos que puedan comprometer la seguridad de la información.

Tabla N°. 108

Alineación función Responder con ISO 27001

Alineación función Responder con ISO 27001			
Control ISO 27001	Implementación para IFAS	Referencia cruzada NIST CSF	Fuente
A.5.24 Gestión de incidentes	Implementación de procedimientos específicos para incidentes en IFAS	RS.RP-1 Plan de respuesta ejecutado	ISO 27001:2022, A.5.24; NIST CSF v1.1, Categoría RS.RP
A.5.25 Lecciones aprendidas	Análisis post-incidente y mejora continua	RS.IM-1 Incorporación de lecciones aprendidas	ISO 27001:2022, A.5.25; NIST CSF v1.1, Categoría RS.IM
A.5.26 Recopilación de evidencias	Procedimientos forenses para sistemas financieros	RS.AN-3 Análisis forense realizado	ISO 27001:2022, A.5.26; NIST CSF v1.1, Categoría RS.AN
A.5.30 Comunicación externa	Protocolos de comunicación con reguladores financieros	RS.CO-4 Coordinación con stakeholders	ISO 27001:2022, A.5.30; NIST CSF v1.1, Categoría RS.CO
A.5.28 Contención de incidentes	Estrategias de contención para minimizar impacto financiero	RS.MI-1 Incidentes contenidos	ISO 27001:2022, A.5.28; NIST CSF v1.1, Categoría RS.MI

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.2.5 Función: recuperar

La función "RECUPERAR" del Marco de Ciberseguridad del NIST (CSF) (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021) es el componente final del ciclo defensivo, enfocado en restablecer capacidades y servicios que hayan sido afectados por incidentes de seguridad. Esta agrupación de metodologías conecta los procesos de planificación de recuperación, mejoras continuas y comunicaciones post-incidente definidos por NIST con los controles de ISO 27001 (ISO/IEC 27002:2022, 2022) relacionados con gestión de continuidad del negocio y lecciones aprendidas. A través de esta asociación, las entidades desarrollan mecanismos de recuperación de la operación a un estado seguro, implementando sus experiencias previas y comunicando actividades de recuperación a las partes interesadas.

Tabla N°. 109

Alineación función Recuperar con ISO 27001

Alineación función Recuperar con ISO 27001			
Control ISO 27001	**Implementación para IFAS**	**Referencia cruzada NIST CSF**	**Fuente**
A.5.29 Continuidad de negocio	Planes de recuperación priorizados para servicios financieros críticos	RC.RP-1 Plan de recuperación ejecutado	ISO 27001:2022, A.5.29; NIST CSF v1.1, Categoría RC.RP
A.5.31 Planificación de continuidad	Pruebas regulares de planes de continuidad para IFAS	RC.IM-1 Planes de recuperación incorporan lecciones	ISO 27001:2022, A.5.31; NIST CSF v1.1, Categoría RC.IM
A.8.14 Copias de seguridad	Estrategia de respaldo inmutable para sistemas financieros	RC.CO-1 Gestión de relaciones públicas	ISO 27001:2022, A.8.14; NIST CSF v1.1, Categoría RC.CO
A.5.32 Redundancia	Implementación de sistemas redundantes para operaciones críticas	RC.RP-1 Restauración ejecutada	ISO 27001:2022, A.5.32; NIST CSF v1.1, Categoría RC.RP
A.5.30 Comunicación en crisis	Plan de comunicación con clientes durante recuperación	RC.CO-3 Actividades de recuperación comunicadas	ISO 27001:2022, A.5.30; NIST CSF v1.1, Categoría RC.CO

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.3 Matriz de madurez para implementación

La matriz de madurez establece parámetros progresivos y medibles para determinar el nivel efectividad alcanzado durante la implementación de controles de seguridad. A través de la aplicación de criterios basados en los dominios de seguridad, la matriz proporciona una visión detallada que facilita la priorización de recursos, el establecimiento de objetivos y la medición de la contante actualización (ISO/IEC, 2022). La siguiente matriz permite evaluar el nivel de madurez en la implementación de controles integrados:

Tabla N°. 110

Matriz de evaluación de implementación de controles

Matriz de evaluación de implementación de controles			
Nivel de madurez	**Descripción**	**Criterios de evaluación**	**Fuente**
1 - Inicial	Procesos ad hoc, planteamiento reactivo	Controles básicos implementados sin unificación	ISO 27001:2022, Anexo A (estructura); NIST CSF v1.1, Niveles de implementación
2 - Gestionado	Procesos documentados, pero sin medición	Controles implementados con documentación formal	ISO 27001:2022, Cláusula 9.1; NIST CSF v1.1, Niveles de implementación
3 - Definido	Procesos estandarizados y consistentes	Controles integrados con medición inicial	ISO 27001:2022, Cláusula 10.2; NIST CSF v1.1, Niveles de implementación
4 - Medido	Procesos medidos y controlados	Controles con métricas de efectividad establecidas	ISO 27001:2022, Cláusula 9.3; NIST CSF v1.1, Niveles de implementación
5 - Optimizado	Mejora continúa basada en métricas	Controles con optimización	ISO 27001:2022, Cláusula 10.2; NIST

Matriz de evaluación de implementación de controles			
Nivel de madurez	**Descripción**	**Criterios de evaluación**	**Fuente**
		continua y automatización	CSF v1.1, Niveles de implementación

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.4 Plan de implementación por fases

El plan de implementación por fases define parámetros claros para lograr reconoce la madurez cibernética ya que esta se logra mediante un gradual. Al establecer una estructura de aplicación que permita mantener las necesidades de la entidad, con los requerimientos necesarios a lo largo del ciclo de implementación facilitaría el descubrimiento de nuevas capacidades al interno de la organización lo que optimizaría la utilización de recursos y define puntos de control regulares dentro del proceso generando mayor confianza en la implementación del programa de seguridad.

Tabla N°. 111

Plan de implementación por fases

Plan de implementación por fases			
Fase	**Actividades principales**	**Resultados esperados**	**Fuente**
Fase 1: evaluación	Análisis de brecha frente a ISO 27001 y NIST CSF	Mapa de brechas y plan de priorización	ISO 27001:2022, Cláusula 4.1; NIST CSF v1.1, Paso 1
Fase 2: diseño	Desarrollo de políticas y procedimientos integrados	Documentación alineada con ambos marcos	ISO 27001:2022, Cláusula 5.2; NIST CSF v1.1, Paso 2
Fase 3: implementación	Despliegue de controles técnicos y administrativos	Controles operativos implementados	ISO 27001:2022, Cláusula 8; NIST CSF v1.1, Paso 3
Fase 4: evaluación	Auditoría y medición de efectividad	Métricas de cumplimiento y efectividad	ISO 27001:2022, Cláusula 9.2; NIST CSF v1.1, Paso 4
Fase 5: mejora	Ciclo de mejora continúa basado en evaluaciones	Controles optimizados y	ISO 27001:2022, Cláusula 10; NIST CSF v1.1, Paso 5

Plan de implementación por fases			
Fase	**Actividades principales**	**Resultados esperados**	**Fuente**
		madurez incrementada	

Nota: tomado de la fuente *(ISO/IEC, 2022)* **y** *(NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)*

2.3.8.5 Beneficios de la integración para activos IFAS

La combinación estratégica de estándares de seguridad que sean complementarios para el objeto de estudio activos IFAS (Internet Facing Applications) apoya las capacidades defensivas de las entidades creando un planteamiento de relevancia entornos de alto riesgo.

Tabla N°. 112

Beneficios de la integración de los dos estándares para IFAS

Beneficios de la integración de los dos estándares para IFAS			
Beneficio	**Descripción**	**Impacto en IFAS**	**Fuente**
Cumplimiento completo	Satisface requisitos regulatorios y operativos	Reduce brechas de cumplimiento en auditorías	ISO 27001:2022, Introducción; NIST CSF v1.1, Sección 1.1
planteamiento basado en riesgos	Prioriza recursos según nivel de riesgo	Protección optimizada de activos financieros críticos	ISO 27001:2022, Cláusula 6.1; NIST CSF v1.1, Sección 2.2
Medición y mejora	Permite evaluación objetiva de capacidades	Mejora continua demostrable ante reguladores	ISO 27001:2022, Cláusula 9.1; NIST CSF v1.1, Sección 3.2
Lenguaje común	Establece terminología estándar para ciberseguridad	Facilita comunicación entre equipos técnicos y directivos	ISO 27001:2022, Términos y definiciones; NIST CSF v1.1, Apéndice A
Adaptabilidad	Permite ajustes según evolución de amenazas	Modelo resiliente frente a nuevas amenazas al sector financiero	ISO 27001:2022, Cláusula 10; NIST CSF v1.1, Sección 3.3

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.3.8.6 Herramienta de autoevaluación

Para facilitar la implementación, se incluye una herramienta de autoevaluación simplificada:

Tabla N°. 113

Esquema de autoevaluación base

Esquema de autoevaluación base			
Área de evaluación	**Preguntas clave**	**Evidencia requerida**	**Fuente**
Gobernanza	¿Existe una política de seguridad que integre requisitos ISO 27001 y NIST CSF?	Documento de política aprobado	ISO 27001:2022, A.5.1; NIST CSF v1.1, ID.GV
Gestión de activos	¿Se mantiene un inventario actualizado de activos IFAS con valoración?	Registro de activos con clasificación	ISO 27001:2022, A.8.1; NIST CSF v1.1, ID.AM
Controles de acceso	¿Existen controles de acceso basados en roles para activos IFAS?	Matriz de roles y privilegios	ISO 27001:2022, A.5.14; NIST CSF v1.1, PR.AC
Monitoreo	¿Se monitorean continuamente los activos IFAS para detectar incidentes?	Registros de monitoreo y alertas	ISO 27001:2022, A.8.16; NIST CSF v1.1, DE.CM
Respuesta a incidentes	¿Existen procedimientos documentados para respuesta a incidentes?	Playbooks de respuesta	ISO 27001:2022, A.5.24; NIST CSF v1.1, RS.RP
Continuidad de negocio	¿Se han establecido y probado planes de recuperación para IFAS?	Planes de continuidad y registros de pruebas	ISO 27001:2022, A.5.29; NIST CSF v1.1, RC.RP

Nota: tomado de la fuente *(ISO/IEC, 2022)* **y** *(NIST SP 800-53, 2020)*

2.3.9 *Análisis fase 3*

La construcción del modelo enfocado en la protección proactiva y la reacción ante incidentes para activos IFAS (Aplicaciones de Internet en frente) se basa en las necesidades particulares de las aplicaciones conectadas a Internet, catalogadas como accesos críticos para actores malintencionados. La definición estratégica de controles técnicos y administrativos establece capas de protección complementarias, así como la implementación de mecanismos de encriptación asegura la confidencialidad e integridad de los datos sensibles. La implementación de controles técnicos, junto con la definición de lineamientos sobre las políticas de acceso garantizando el mínimo privilegio mínimo crean un esquema defensivo donde la violación de una capa no compromete automáticamente la totalidad de los sistemas.

El diseño metodológico de procedimientos de respuesta a incidentes basados en NIST IR (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021) permiten realizar un cambio significativo en la postura organizacional reactiva. Los playbooks desarrollados para escenarios críticos como ransomware o filtraciones de datos codifican las mejores prácticas actuales permiten reducir la dependencia de individuos específicos y garantizando respuestas consistentes bajo presión.

Dentro de la exploración de alineación con estándares internacionales como ISO 27001 y NIST CSF establece un marco operativo que aprovecha las fortalezas de cada uno de los estándares. El mapeo de controles contra el Anexo A de ISO 27001 (ISO/IEC, 2022) asegura una cobertura comprehensiva, mientras que la estructuración según las cinco funciones del NIST CSF (Identificar, Proteger, Detectar, Responder, Recuperar) facilita tanto la implementación como la evaluación continua.

Para concluir, el modelo elaborado ofrece un fundamento en consonancia con normas internacionales para la salvaguarda de activos IFAS, definiendo una estructura defensiva que balancea acciones preventivas con habilidades de respuesta.

2.4 Fase 4: Elaboración de documentación de las buenas prácticas que permitan fortalecer el nivel de madurez cibernética en entidades financieras

Voy a desarrollar detalladamente los componentes de esta fase para tu proyecto de diseño de modelo de ciberseguridad para instituciones financieras, enfocado especialmente en aplicaciones con exposición a internet.

2.4.1 *Elaboración de manuales*

2.4.1.1 Guía para la clasificación de activos en instituciones financieras

Esta guía proporciona un marco sistemático para identificar, clasificar y gestionar activos de información críticos en instituciones financieras, con especial énfasis en aplicaciones con exposición a internet (Internet Facing Applications).

Aplicable a todos los activos de información de la institución financiera, incluyendo sistemas, aplicaciones, bases de datos, infraestructura, servicios en la nube y aplicaciones con exposición externa.

2.4.1.2 Roles y responsabilidades

La adecuada protección de los activos críticos de información en las instituciones financieras requiere establecer roles y responsabilidades alineadas para asignación de responsabilidades específicas a los distintos actores en la identificación, clasificación y resguardo de los activos.

Tabla N°. 114

Tabla de roles y responsabilidades

Tabla de roles y responsabilidades	
Rol	**Responsabilidad**
Propietario del Activo	Identificar, clasificar y revisar periódicamente la clasificación del activo.
Custodio del Activo	Implementar controles según la clasificación del activo.
Oficial de Seguridad	Supervisar y validar la clasificación de activos.
Comité de Seguridad	Aprobar la metodología y resolver conflictos de clasificación.

2.4.1.3 Metodología de clasificación

Realizar la implementación de una metodología permite desarrollar los procedimientos recomendados que seguir desde las instituciones financieras para identificar, valorar y clasificar

sus activos IFAS. Esta metodología integra buenas prácticas internacionales y marcos normativos primordiales, facilitando la priorización de recursos de protección en función del nivel de criticidad y riesgo asociado a cada activo.

2.4.1.3.1 Criterios de clasificación

- **Confidencialidad:** en instituciones financieras, los activos con alta confidencialidad pueden incluir datos de clientes, información financiera estratégica, claves criptográficas, entre otros.

Tabla N°. 115

Criterios de clasificación del activo

Criterios de clasificación		
Nivel	**Descripción**	**Ejemplos prácticos**
Alto	Información altamente sensible cuya divulgación no autorizada causaría daños graves	Datos de tarjetas de crédito, credenciales de autenticación, algoritmos de cifrado
Medio	Información sensible cuya divulgación no autorizada causaría daños significativos	Información de clientes no financiera, configuraciones de sistemas
Bajo	Información cuya divulgación causaría daños mínimos	Información pública, documentación general

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

- **Integridad:** la integridad hace referencia a la precisión, consistencia y fiabilidad de la información almacenada, procesada o transmitida por un activo. En el sector financiero, la alteración no autorizada de datos puede comprometer decisiones estratégicas, generar errores contables o fraudes, afectando directamente la confianza del cliente y del regulador.

Tabla N°. 116

Criterios respecto a la Integridad

Criterios respecto a la Integridad		
Nivel	**Descripción**	**Ejemplos practico**
Alto	Información cuya modificación no autorizada causaría daños graves	Registros de transacciones, saldos de cuentas
Medio	Información cuya modificación no autorizada causaría daños significativos	Configuraciones de sistemas, registros de auditoría

Criterios respecto a la Integridad		
Nivel	**Descripción**	**Ejemplos practico**
Bajo	Información cuya modificación causaría daños mínimos	Contenido informativo, anuncios

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

- **Disponibilidad:** la disponibilidad se relaciona con el nivel de necesidad de que un activo esté accesible y operativo en el momento requerido. En el entorno financiero, donde las operaciones dependen de sistemas en línea y procesamiento en tiempo real, la interrupción de ciertos activos puede generar pérdidas significativas y afectar la continuidad del negocio.

Tabla N°. 117

Criterios respecto a la confidencialidad

Criterios respecto a la confidencialidad		
Nivel	**Descripción**	**Requisito de disponibilidad**
Alto	Servicios críticos para la operación.	99.99% o superior (RTO < 1 hora)
Medio	Servicios importantes, pero no críticos.	99.9% (RTO < 8 horas)
Bajo	Servicios no esenciales.	99% (RTO < 24 horas)

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

- **Cumplimiento Regulatorio:** este criterio se enfoca en el nivel de obligación legal o normativa asociado al activo. Algunas financieras están sujetas a requerimientos regulatorios asociados a la protección de datos personales, prevención del lavado de activos, y conservación de registros financieros.

Tabla N°. 118

Criterio respecto al cumplimiento regulatorio

Criterio respecto al cumplimiento regulatorio		
Nivel	**Descripción**	**Ejemplos**
Alto	Sujeto a múltiples regulaciones estrictas	PCI DSS, GDPR, regulación bancaria local
Medio	Sujeto a regulaciones generales	Normativas corporativas
Bajo	Regulaciones mínimas o ninguna	Contenido informativo

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

- **Exposición a Internet (Específico para IFAS):** la exposición a internet se refiere al grado en que un activo se encuentra accesible desde redes públicas o entornos externos a la organización. Activos con alta exposición, como portales transaccionales, APIs o servidores accesibles desde la web, representan un mayor riesgo de ataque y deben ser clasificados con base en su nivel de visibilidad y criticidad.

Tabla N°. 119

Clasificación para IFAS

Clasificación para IFAS		
Nivel	**Descripción**	**Ejemplos**
Alto	Aplicación directamente accesible desde internet	Banca en línea, API públicas, portales de pago
Medio	Accesible de forma limitada o a través de intermediarios	Portales de socios con autenticación, VPN
Bajo	Sin exposición directa a internet	Sistemas internos

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

2.4.1.4 Matriz de valoración global

La Matriz de valoración global apoya la incorporación de los niveles de riesgo vinculados a cada criterio, otorgándole a cada activo una clasificación que está basada en el valor más elevado alcanzado en cualquiera de estos. Esta evaluación permite que los activos más críticos protegidos de manera prioritaria, al valorar el riesgo más importante al que se enfrentan. La clasificación final del activo se determina con base en la valoración más alta obtenida en cualquiera de los criterios anteriores:

Tabla N°. 120

Esquema general de clasificación del activo

Esquema general de clasificación del activo		
Clasificación	**Descripción**	**Nivel de Protección**
Crítico	Activo con al menos un criterio de nivel Alto	Máximas medidas de protección
Sensible	Activo con criterios de nivel Medio como máximo	Medidas de protección estándar elevadas
Normal	Activo con criterios de nivel Bajo como máximo	Medidas de protección básicas

Esquema general de clasificación del activo		
Clasificación	**Descripción**	**Nivel de Protección**

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

2.4.1.5 Proceso de clasificación

Tabla N°. 121

Esquema de actividades para realizar la clasificación de activos

Esquema de actividades para realizar la clasificación de activos	
Identificación	Listar todos los activos de información
Evaluación	Aplicar los criterios de clasificación a cada activo
Documentación	Registrar la clasificación en el inventario de activos
Validación	El Oficial de Seguridad valida la clasificación
Aprobación	El Comité de Seguridad aprueba el inventario
Revisión periódica	Revisar la clasificación al menos anualmente

Nota: tomado de la fuente *(ISO/IEC 27002:2022, 2022)*

2.4.1.6 Inventario de activos

Mantener un inventario centralizado que incluya como mínimo los siguientes ítems, es importante indicar que los campos del inventario de activos están sujeto a que tan granular se requiere por parte de la organización, a continuación, se listan los que en consideración son los principales:

Tabla N°. 122

Campos sugeridos inventario de activos de información

Campos sugeridos inventario de activos de información	
Identificador único del activo	Identificador único
Nombre y descripción	Nombre claro y utilidad del activo
Tipo de activo	Tipos de activo: humano, tecnológico, etc.
Propietario y custodio	Identificación de responsable

Clasificación según cada criterio	Clasificación según criterios de disponibilidad, integridad, confidencialidad y regulatorio entre otros
Clasificación global	Definición de clasificación según el esquema sugerido de la matriz global
Fecha de última revisión	Marca de fecha de actualización
Ubicación/entorno	Ubicación tangible o intangible del activo
Ciclo de vida del activo	Definir tiempo estimados de resguardo o utilidad del activo.

Nota: Campos sugeridos inventario de activos

2.4.1.7 Etiquetado y manipulación

- **Etiquetado:** todos los activos de información deberán ser etiquetados conforme a la clasificación definida:
  - **Visual:** etiquetas físicas para equipos de hardware
  - **Digital:** todos los activos digitales etiquetados con marcas de agua, cabeceras, metadatos, que definan su clasificación.
  - **Sistémico:** etiquetas de clasificación para todos los sistemas de gestión.
- **Manipulación:** la manipulación de los activos de información debe estar contenida y especificada conforme a su ubicación, almacenamiento procesamiento o permisos de borrado de los mismos.

Tabla N°. 123

Manipulación de activos de información

Manipulación de activos de información				
Clasificación	**Almacenamiento**	**Transmisión**	**Procesamiento**	**Eliminación**
Crítico	Cifrado AES-256	Cifrado TLS 1.3	Entornos seguros aislados	Borrado seguro certificado
Sensible	Cifrado AES-128	Cifrado TLS 1.2+	Entornos controlados	Borrado seguro
Normal	Protección estándar	Canales cifrados	Entornos estándar	Borrado normal

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.4.1.8 Controles de seguridad según clasificación

A continuación, se expone en una tabla los controles de seguridad recomendados para los activos según la criticidad definida.

Tabla N°. 124

Controles de seguridad según clasificación

Controles de seguridad según clasificación		
Activos Críticos	**Activos Sensibles**	**Activos Normales**
• Cifrado de datos en reposo y en tránsito. • Autenticación multifactor. • Control de acceso basado en roles (RBAC). • Monitorización continua. • Pruebas de penetración trimestrales. • Respaldos cifrados diarios. • Plan de continuidad específico.	• Cifrado de datos sensibles. • Autenticación. • Control de acceso basado en roles. • Monitorización regular • Pruebas de seguridad semestrales. • Respaldos semanales. • Incluidos en planes de continuidad generales.	• Protecciones básicas. • Autenticación estándar. • Control de acceso básico. • Monitorización básica. • Pruebas de seguridad anuales. • Respaldos mensuales.

Nota: tomado de la fuente *(ISO/IEC, 2022)*

2.4.2 *Consideraciones especiales para internet facing applications*

A continuación, se presentan consideraciones adicionales al tener en cuenta la implementación de la guía de buenas prácticas de seguridad de la información para los activos IFAS.

Tabla N°. 125

Consideraciones IFAS

Consideraciones IFAS	
Protección Adicional	• Implementación de WAF (Web Application Firewall) • Protección DDoS • Gestión de sesiones • Monitorización de tráfico • Escaneo de vulnerabilidades frecuente • Gestión de certificados SSL/TLS
Arquitectura de Seguridad	• Implementación de zonas DMZ • Segmentación de redes

Consideraciones IFAS	
Anexos	• Filtrado de tráfico entrante y saliente • Limitación de superficies de ataque • Plantilla de Inventario de Activos • Flujograma del Proceso de Clasificación • Lista de Verificación para Clasificación de Aplicaciones con Exposición a Internet • Matriz de Responsabilidades (RACI)

Nota: consideraciones especificas IFAS

2.4.3 *Guía para la gestión de vulnerabilidades y respuesta a incidentes*

Esta guía establece los procesos para identificar, evaluar, mitigar y gestionar vulnerabilidades de seguridad en activos críticos de instituciones financieras, con énfasis en aplicaciones expuestas a internet, así como los procedimientos de respuesta ante incidentes de seguridad.

Aplicable a todos los sistemas y aplicaciones de la institución financiera, con especial atención a aquellos clasificados como críticos o sensibles según la Guía de Clasificación de Activos.

2.4.4 *Gestión de vulnerabilidades*

La administración de vulnerabilidades es un elemento crucial en las tácticas de salvaguarda de activos esenciales de información, particularmente en el ámbito de las entidades financieras, donde los peligros tecnológicos se transforman continuamente.

- **Roles y Responsabilidades:** para asegurar una reacción ante las amenazas, es esencial definir roles y responsabilidades claros en el proceso de identificación, análisis, tratamiento y monitoreo de vulnerabilidades. A continuación, se presenta un esquema de roles y responsabilidades.

  Tabla N°. 126

  Roles y responsabilidades en la gestión de vulnerabilidades

Roles y responsabilidades en la gestión de vulnerabilidades	
Rol	**Responsabilidades**
Equipo de Seguridad	Coordinar el proceso de gestión de vulnerabilidades
Propietarios de Sistemas	Priorizar y aprobar remediaciones
Equipos de TI	Ejecutar escaneos y aplicar parches/correcciones
Comité de Gestión de Cambios	Aprobar ventanas de mantenimiento

Roles y responsabilidades en la gestión de vulnerabilidades	
Rol	**Responsabilidades**
CISO	Supervisar el programa y reportar al directorio

Nota: definición de roles y responsabilidades

2.4.4.1 Ciclo de vida de gestión de vulnerabilidades

2.4.4.1.1 Descubrimiento

En el descubrimiento de vulnerabilidades es necesario permitir gestionar de manera constante las brechas de seguridad identificadas.

- **Fuentes de Información**
  - Escaneos automáticos continuamente
  - Pentesting y Red Team
  - Servicios de inteligencia de amenazas
  - Bug Bounty y reportes externos
  - Bases de datos de vulnerabilidades (NVD, CVE)
  - Reportes de auditorías internas y externa
- **Herramientas de Escaneo**
  - Escaneo de vulnerabilidades de red
  - Análisis de código estático (SAST)
  - Análisis de código dinámico (DAST)
  - Análisis de composición de software (SCA)
  - Escaneo de configuraciones inseguras
  - Análisis de tráfico web especializado
- **Frecuencia de Escaneos**

Tabla N°. 127

Definición recomendada de tiempos de escaneo

Definición recomendada de tiempos de escaneo	
Clasificación del Activo	**Frecuencia Mínima**
Crítico	Semanal
Sensible	Quincenal
Normal	Mensual

Definición recomendada de tiempos de escaneo	
Clasificación del Activo	**Frecuencia Mínima**
Internet Facing	Diaria para análisis superficial, semanal para análisis más detallado

Nota: recomendada de tiempos de escaneo

2.4.4.2 Evaluación y priorización

- **Sistema de Puntuación:** a continuación, se define un esquema propuesto de evaluación teniendo como base los factores de contexto encontrados en los marcos consultados tales como CVSS v3.1.

Tabla N°. 128

Esquema propuesto de sistema de puntuación para evaluación

Esquema propuesto de sistema de puntuación para evaluación	
Factor	**Peso**
Base CVSS	50%
Clasificación del activo	20%
Exposición a Internet	15%
Explotación conocida	10%
Impacto en el negocio	5%

Nota: propuesta de sistema de puntuación para evaluación

- **Niveles de Riesgo**: a continuación, esquema de niveles de riesgo con tiempos establecidos de remediación definidos por los estándares base de este documento.

Tabla N°. 129

Niveles de remediación conforme al riesgo

Niveles de remediación conforme al riesgo		
Nivel	**Puntuación**	**SLA de Remediación**
Crítico	9.0 - 10.0	24 horas
Alto	7.0 - 8.9	1 semana
Medio	4.0 - 6.9	1 mes
Bajo	0.1 - 3.9	3 meses

Es importante indicar que los niveles de remediación son sugeridos, pero conforme a la entidad estos pueden ser ajustados validando la clasificación del activo y elevarlo automáticamente un nivel.

2.4.4.3 Remediación

La etapa de remediación implica la aplicación de acciones correctivas para eliminar o mitigar las brechas identificadas en los activos. Es importante indicar que una adecuada estrategia de

remediación permite reducir el espacio de exposición y fortalecer la postura de ciberseguridad de la entidad financiera.

Tabla N°. 130

Ítems en el esquema de remedición de vulnerabilidades

Ítems en el esquema de remedición de vulnerabilidades	
Estrategias de Mitigación	• Corrección: aplicar parche o corregir código • Mitigación: implementar controles compensatorios • Aceptación: documentar aceptación formal del riesgo • Rechazo del riesgo: Justificar como falso positivo
Estrategias de Mitigación	• Corrección: aplicar parche o corregir código • Mitigación: implementar controles compensatorios • Aceptación: documentar aceptación formal del riesgo • Rechazo del riesgo: justificar como falso positivo
Flujo de Trabajo de Remediación	• Asignación de responsable • Desarrollo de plan de remediación • Pruebas en entorno no productivo • Solicitud de cambio (RFC) • Implementación • Verificación post-implementación • Cierre de la vulnerabilidad
Gestión de Excepciones	• Proceso formal de aprobación • Documentación de justificación • Plazo máximo de excepción (3 meses) • Controles compensatorios obligatorios • Revisión periódica de excepciones
Verificación	• Escaneo dirigido post-remediación • Pruebas de penetración específicas • Verificación manual cuando sea necesario

Nota: esquema de remediación de vulnerabilidades

2.4.4.4 Informes, métricas y consideraciones específicas para IFAS

- **Los informes y métricas:** establecen la importancia de generar reportes periódicos y utilizar indicadores clave que permitan evaluar el desempeño del proceso, identificar tendencias, medir la eficacia de las acciones de remediación y apoyar la toma de decisiones estratégicas.

Tabla N°. 131

Definición de informes y KPIs

Definición de Informes y KPIs	
KPIs de Gestión de Vulnerabilidades	• Tiempo medio de remediación (MTTR) • Densidad de vulnerabilidades por activo • Tasa de cumplimiento de SLAs • Vulnerabilidades recurrentes • Cobertura de escaneo • Edad media de vulnerabilidades abiertas
Informes Periódicos	• Informes semanales para equipo técnico • Informes mensuales para dirección • Informes trimestrales para comité de riesgos • Dashboard en tiempo real para seguimiento

Nota: definición de informes y objetivos

- **Consideraciones Internet Facing Applications:** a continuación, algunas parametrizaciones importantes a incluir en esquema de gestión de vulnerabilidades teniendo en cuenta el foco de este análisis sobre las IFAS.

Tabla N°. 132

Consideraciones Internet Facing Applications

Consideraciones Internet Facing Applications	
Monitorización Continua	• Implementación de DAST continuo • Monitorización de certificados SSL/TLS • Análisis de configuraciones en tiempo real • Revisión de cambios no autorizados
Arquitectura Defensiva	• Implementación de WAF con reglas personalizadas • Protección contra ataques DDoS • API Gateway con validación • Rate limiting y detección de bots • Validación de entradas reforzada

2.4.5 *Respuesta a incidentes*

2.4.5.1 Marco de respuesta a incidentes

A continuación, se definen los parámetros necesarios para el establecimiento del marco de respuesta de incidentes (ISO/IEC 27035, 2023):

- **Fases del Proceso**
  - Preparación
  - Detección y análisis

- Contención
- Erradicación
- Recuperación
- Lecciones aprendidas

- **Equipo de respuesta a incidentes (CSIRT)**

Tabla N°. 133

Equipo de respuesta a incidentes (CSIRT)

Equipo de respuesta a incidentes (CSIRT)	
Rol	**Responsabilidades**
Coordinador de Incidentes	Gestionar el incidente y coordinar la respuesta
Analistas de Seguridad	Investigación técnica y análisis
Administradores de Sistemas	Implementar medidas técnicas
Representante Legal	Asesorar sobre implicaciones legales
Comunicaciones	Gestionar comunicaciones internas y externas
Recursos Humanos	Gestionar aspectos disciplinarios si aplica

Nota: integrantes del equipo de Csirt

- **Detección y Análisis:** establece los mecanismos necesarios para la identificación temprana y combina capacidades tecnológicas de monitorización continua con procesos analíticos estructurados que permiten discriminar eficazmente entre falsos positivos y amenazas genuinas, determinando su naturaleza, alcance y potencial impacto.
  - **Fuentes de Detección**
    - Sistemas SIEM
    - Alertas de EDR/XDR
    - Monitorización de red (NTA/NDR)
    - Logs de aplicaciones
    - WAF y sistemas perimetrales
    - Reportes de usuarios
    - Alertas de proveedores
  - **Clasificación de Incidentes:** en el siguiente cuadro se encuentra la clasificación de incidentes conforme a los criterios de impacto y estableciendo tiempos de respuesta sugeridos.

    Tabla N°. 134

    Clasificación de Incidentes

Clasificación de Incidentes			
Severidad	**Descripción**	**Ejemplos**	**Tiempo de Respuesta**
Crítica	Impacto severo en operaciones críticas	Brecha de datos confirmada, ransomware generalizado	Inmediata (15 min)
Alta	Impacto significativo	Compromiso de servidor, ataque dirigido	1 hora
Media	Impacto moderado	Malware aislado, phishing exitoso	4 horas
Baja	Impacto mínimo	Intentos de login fallidos, malware bloqueado	24 horas

Nota: tomado de la fuente *(CSRC, SP 800-61 Rev. 2)*

- **Procedimiento de Escalamiento**
  - Matriz de escalamiento según severidad
  - Criterios para activar el comité de crisis
  - Protocolos de notificación interna y externa
  - Tiempos máximos para cada nivel de escalamiento
- **Contención, Erradicación y Recuperación**
  - **Estrategias de Contención**: la fase de contención representa la primera línea de defensa activa una vez que un incidente de seguridad ha sido detectado, estableciendo barreras técnicas y procedimentales para limitar su propagación e impacto. Esta etapa crítica implementa estrategias inmediatas para aislar sistemas comprometidos, segmentar redes afectadas y restringir canales de comunicación potencialmente explotables, creando perímetros defensivos que impiden que la amenaza se extienda a otros activos organizacionales.

    Tabla N°. 135

    Estrategias de Contención

Estrategias de Contención	
Tipo de Incidente	**Acciones de Contención**
Compromiso de aplicación web	Activar WAF en modo bloqueo, aislar servidores afectados
Ransomware	Desconectar sistemas afectados, bloquear tráfico lateral
Fuga de datos	Revocar credenciales, bloquear conexiones externas sospechosas

Estrategias de Contención	
Tipo de Incidente	**Acciones de Contención**
DDoS	Activar mitigación DDoS, implementar filtrado de tráfico
Acceso no autorizado	Bloquear cuentas comprometidas, implementar controles compensatorios

Nota: tomado de la fuente *(CSRC, SP 800-61 Rev. 2)*

- **Procedimientos de Erradicación:** esta etapa establece la eliminación de artefactos maliciosos permitiendo realizar un análisis de modificaciones y puertas traseras, así como mecanismos de instalados por el atacante, requiriendo en algunos casos un análisis forense de técnicas específicas de remediación:
  - Eliminación de malware
  - Corrección de vulnerabilidades explotadas
  - Reseteo de credenciales comprometidas
  - Restauración desde respaldos verificados
  - Reconstrucción de sistemas comprometidos
- **Recuperación:** en esta fase se implementan estructuras de planes previamente definidos con el fin de establecer normalidad en los activos afectados mediante la verificación de la integridad de los sistemas y datos contenidos en los mismos, logrando luego de la validación de no intrusión lograr volver a la estabilidad en todos los sistemas de producción necesarios para las actividades de la entidad.
  - Verificación previa a la restauración
  - Monitorización intensiva durante la recuperación
  - Validación de sistemas restaurados
  - Pruebas de seguridad post-recuperación
  - Restablecimiento gradual de servicios

2.4.5.1.1 Comunicación durante incidentes

A continuación, se especifica el esquema de comunicación durante la evolución del incidente teniendo en cuenta este puede ser ajustad conforme a lo definido por la organización y al entorno de la entidad para el caso de la regulación.

Tabla N°. 136

Comunicación durante incidentes

Comunicación durante incidentes	
Comunicación Interna	• Plantillas predefinidas según tipo de incidente • Canales seguros de comunicación • Restricción de información sensible • Registro detallado de comunicaciones
Comunicación Externa	• Notificaciones regulatorias (plazos y formatos) • Comunicación con clientes afectados • Gestión de relaciones con medios • Coordinación con entes gubernamentales
Requisitos Regulatorios	• Identificación de obligaciones de reporte • Plazos legales para notificación • Documentación requerida por reguladores • Protocolos de coordinación con autoridades

Nota: mecanismos de comunicación durante incidentes

2.4.5.1.2 Análisis post-incidente

Análisis Post-Incidente prioriza la importancia de realizar evaluaciones granulares una vez controlado un incidente, con el fin de extraer lecciones aprendidas, fortalecer los procedimientos existentes y prevenir la recurrencia de eventos similares (ISO/IEC 27035, 2023).

Tabla N°. 137

Parámetros para realizar el análisis post-Incidente

Parámetros para realizar el análisis post-Incidente		Herramientas y Recursos
Informe de incidente	• Cronología detallada • Análisis causa-raíz • Evaluación de la respuesta • Efectividad de los controles • Impacto financiero y operativo • Recomendaciones	• Kit de herramientas forenses • Plantillas de documentación • Playbooks por tipo de incidente • Contratos con proveedores de respuesta • Contactos de emergencia
Mejora continua	• Actualización de procedimientos • Refuerzo de controles deficientes • Adición de capacidades de detección • Actualización de playbooks • Simulacros dirigidos	
	Tipo Frecuencia Alcance	

Parámetros para realizar el análisis post-Incidente				Herramientas y Recursos
Simulacros y ejercicios	Tabletop	Trimestral	Escenarios específicos	
	Simulacro técnico	Semestral	Equipos técnicos	
	Simulacro organizacional	Anual	Toda la organización	
	Red Team	Anual	Sistemas críticos	

Nota: tomado de la fuente *(CSRC, SP 800-61 Rev. 2)*

2.4.6 *Capacitación y difusión; taller para equipos técnicos: implementación del modelo de ciberseguridad*

Este componente estratégico establece una guía de contenido para que el personal técnico comprenda los componentes técnicos y adquiera las competencias operativas que permitan la aplicación del modelo de buenas prácticas de ciber seguridad. Este taller propuesto contiene conceptos teóricos y algunos ejercicios prácticos asociados, así como situaciones que permiten la aplicación de controles conforme a los casos de uso propuestos. El esquema detallado del taller, agenda, contenidos y metodologías de evaluación se encuentra disponible en el **Anexo 2** del presente documento.

2.4.7 *Evaluación de Madurez Cibernética para Instituciones Financieras*

El presente documento define un marco que permite realizar la evaluación de madurez cibernética en entidades financieras enfocándose en la protección de aplicaciones con exposición a internet (Internet Facing Applications). Lo que genera una base inicial para medir continuamente el avance y establecer objetivos a largo y corto plazo entorno a las capacidades asociadas a ciberseguridad.

2.4.7.1 **Modelos de evaluación de madurez**

Los modelos de evaluación de madurez en ciberseguridad son marcos estructurados que permiten a las empresas medir, comparar y evolucionar sistemáticamente sus capacidades defensivas. El CMMI Cybersecurity Maturity Model (ISACA, 2025) y los NIST Cybersecurity Framework (CSF) (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)Tiers representan dos orientaciones reconocidos internacionalmente para esta evaluación, ellos ofrecen la definición de criterios que permiten determinar el estado actual frente a las

actividades ejecutadas de seguridad y definir un plan de trabajo que permita llevar a cabo el alcance de objetivos paulatinos que a lo largo permitan ir superando cada nivel madurez.

2.4.7.1.1 CMMI Cybersecurity Maturity Model

El Capability Maturity Model Integration (CMMI) establece unos parámetros generales, pero establece parámetros específicos en torno a los desafíos de seguridad en el entorno digital. Este modelo evalúa las prácticas de ciberseguridad en cinco niveles de madurez progresivos expuesto a continuación (ISACA, 2025):

Tabla N°. 138

Esquema de niveles de CMMI Cybersecurity Maturity Model

Nivel	Descripción	Características
1 - Inicial	Procesos ad-hoc y reactivos	Prácticas inconsistentes, documentación limitada, alta dependencia de individuos
2 - Gestionado	Procesos planificados y ejecutados según políticas	Prácticas documentadas por proyecto, seguimiento básico, controles consistentes en áreas similares
3 - Definido	Procesos estandarizados a nivel organizacional	Procesos bien definidos, adaptación controlada, métricas de proceso y resultados
4 - Gestionado Cuantitativamente	Procesos medidos y controlados	Objetivos cuantitativos, análisis estadístico, predictibilidad de resultados
5 - Optimizado	Mejora continua de procesos	Innovación, optimización basada en métricas, adaptación proactiva

Nota: tomado de la fuente *(Energy)*

2.4.7.1.2 Dominios de evaluación CMMI para ciberseguridad

El Modelo de Madurez de Capacidades para la Ciberseguridad (ISACA, 2025) define la evaluación mediante selección de dominios los cuales se evidencian en la siguiente tabla, los que identifican las áreas más primordiales a revisar frente a la definición de postura de ciberseguridad en una entidad.

Tabla N°. 139

Dominios de Evaluación CMMI para Ciberseguridad

Dominios de Evaluación CMMI para Ciberseguridad	
Gobernanza de Ciberseguridad	• Estrategia y políticas • Roles y responsabilidades • Gestión de recursos • Supervisión y rendición de cuentas
Gestión de Riesgos de Ciberseguridad	• Identificación de riesgos • Evaluación y priorización • Tratamiento y mitigación • Monitorización continua
Ingeniería de Seguridad	• Requisitos de seguridad • Arquitectura segura • Diseño y desarrollo seguros • Pruebas de seguridad
Gestión de Activos	• Inventario y clasificación • Configuración y gestión de cambios • Protección según clasificación • Ciclo de vida de activos
Gestión de Identidad y Acceso	• Provisión y desprovisionamiento • Autenticación y autorización • Gestión de privilegios • Monitorización de accesos
Protección de Datos	• Clasificación de datos • Cifrado y seudonimización • Prevención de pérdida de datos • Gestión de ciclo de vida
Gestión de Vulnerabilidades	• Identificación y evaluación • Priorización y remediación • Parcheado y gestión de actualizaciones • Monitorización continua
Protección de Infraestructura	• Segmentación de red • Protección perimetral • Detección de intrusiones • Gestión de configuraciones
Respuesta a Incidentes	• Detección y análisis • Contención y erradicación

Dominios de Evaluación CMMI para Ciberseguridad	
	• Recuperación • Mejora post-incidente
Concienciación y Capacitación	• Programa de concienciación • Formación especializada • Medición de efectividad • Cultura de seguridad

Nota: tomado de la fuente *(Energy)*

2.4.7.2 NIST Cybersecurity Framework (CSF) Tiers

Los Niveles del Marco de Ciberseguridad del NIST (CSF Tiers) (NIST, Cybersecurity Framework | NIST, 2013) define niveles progresivos (Parcial, Informado, Repetible y Adaptativo) describen el grado de implementación y madurez de los procesos de ciberseguridad, lo que a lo largo deja que las instituciones identifiquen si estado actual y realizar identificación de oportunidades de mejora en objetivos específicos. Con la aplicación de esta evaluación se logra identificar que tan alineados están los componentes de seguridad con los lineamientos operativos permitiendo evidenciar criticidad, amenazas y los recursos con los que se cuenta para la protección de los activos de información:

Tabla N°. 140

NIST Cybersecurity Framework (CSF) Tiers

Framework (CSF) Tiers		
Tier	**Nombre**	**Descripción**
1	Parcial	Definido como reactivo, gestión de riesgos ad-hoc, conciencia limitada, coordinación mínima.
2	Informado	Procesos definidos, pero no formalizados, conciencia de riesgos, herramientas implementadas, pero no integradas.
3	Repetible	Prácticas formales, políticas implementadas, colaboración externa regular.
4	Adaptativo	Orientado en mejora continua, información compartida proactivamente, procesos ágiles, lecciones aprendidas incorporadas rápidamente.

Nota: esquema de Tiers basados en NIST

2.4.7.2.1 Funciones NIST CSF para evaluación

El Marco de Ciberseguridad del NIST (NIST CSF) (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021)define sus evaluaciones mediante cinco funciones

principales que representan el ciclo de vida completo de la gestión de riesgos de ciberseguridad. Estas funciones (Identificar, Proteger, Detectar, Responder y Recuperar) cada función categoriza las capacidades de ciberseguridad existentes, identificar brechas y priorizar iniciativas de mejora.

Tabla N°. 141

Funciones NIST CSF para evaluación

Funciones NIST CSF para evaluación	
Identificar (ID)	• Gestión de activos (ID.AM) • Entorno de negocio (ID.BE) • Gobernanza (ID.GV) • Evaluación de riesgos (ID.RA) • Estrategia de gestión de riesgos (ID.RM) • Gestión del riesgo de la cadena de suministro (ID.SC)
Proteger (PR)	• Gestión de identidad y control de acceso (PR.AC) • Concienciación y formación (PR.AT) • Seguridad de datos (PR.DS) • Procesos y procedimientos de protección de la información (PR.IP) • Mantenimiento (PR.MA) • Tecnología de protección (PR.PT)
Detectar (DE)	• Anomalías y eventos (DE.AE) • Monitorización continua de la seguridad (DE.CM)Procesos de detección (DE.DP)
Responder (RS)	• Planificación de respuesta (RS.RP) • Comunicaciones (RS.CO) • Análisis (RS.AN) • Mitigación (RS.MI) • Mejoras (RS.IM)
Recuperar (RC)	• Planificación de recuperación (RC.RP) • Mejoras (RC.IM) • Comunicaciones (RC.CO)

Nota: tomado de la fuente *(NIST, Cybersecurity Framework | NIST, 2013)*

2.4.8 *Metodología de Evaluación*

A continuación, se presenta una tabla de metodología donde se contemplan los pasos generales para realizar el proceso de evaluación del nivel de madurez cibernética de una entidad (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021).

Tabla N°. 142

Esquema proceso de Evaluación

Esquema proceso de Evaluación	
Planificación	• Definir alcance y objetivos • Seleccionar dominios aplicables • Identificar participantes y roles • Establecer cronograma
Recopilación de Evidencias	• Revisión documental • Entrevistas con stakeholders • Observación de procesos • Pruebas técnicas • Revisión de configuraciones
Análisis y Puntuación	• Evaluación por dominio • Determinación de niveles de madurez • Identificación de fortalezas y debilidades • Análisis de brechas
Reporting	• Informe detallado por dominio • Dashboard ejecutivo • Comparativa con industria • Recomendaciones priorizadas

Nota: tabla de medición nivel de madurez cibernetica

- **Matriz de Evaluación Específica para Internet Facing Applications: e**sta matriz complementa los modelos anteriores con un sentido específico en aplicaciones expuestas a internet:

  Tabla N°. 143

  Propuesta matriz de evaluación IFAS

Propuesta matriz de evaluación específica para internet facing applications		
Dominio	**Prácticas Evaluadas**	**Peso**
Arquitectura de Seguridad	Diseño de zonas DMZ, segmentación.	15%
Gestión de Accesos	Autenticación, autorización, gestión de sesiones, MFA	15%
Protección de Aplicaciones Web	WAF, RASP, endurecimiento de servidores web, código seguro.	20%
Gestión de APIs	Seguridad de APIs, OAuth, API Gateway, rate limiting	15%

Propuesta matriz de evaluación específica para internet facing applications		
Monitorización y Detección	SIEM, IDS/IPS, monitorización de comportamiento, honeypots	10%
Arquitectura de Seguridad	Diseño de zonas DMZ, segmentación.	15%

Nota: matriz de evaluación IFAS

- **Escala de Evaluación:** para cada práctica se asignará una puntuación según el siguiente criterio:

Tabla N°. 144

Escala de avaluación según aplicación de control

Escala de avaluación según aplicación de control	
Puntuación	**Descripción**
0	No implementado / No existe
1	Implementación inicial / Ad-hoc
2	Parcialmente implementado / Documentado
3	Implementado en su mayoría / Gestionado
4	Completamente implementado / Medido

Nota: escala de evaluación sugerida para los controles

- **Plan de Mejora Continua (Ciclo PDCA)**

Tabla N°. 145

Plan de Mejora Continua (Ciclo PDCA)

Plan de Mejora Continua (Ciclo PDCA)		
Planificar (Plan)	**Análisis de Brechas**	• Identificar diferencia entre estado actual y objetivo • Priorizar brechas según riesgo e impacto • Establecer objetivos SMART para cada brecha
	Definición de Iniciativas	• Desarrollo de proyectos específicos • Asignación de recursos • Establecimiento de KPIs • Definición de líneas temporales
	Gestión de Stakeholders	• Identificación de grupos de interés • Estrategia de comunicación • Gestión de resistencia al cambio
Hacer (Do)	**Aplicación de Controles**	• Desarrollo de políticas y procedimientos • Aplicación de soluciones técnicas

Plan de Mejora Continua (Ciclo PDCA)		
		• Capacitación y concienciación • Ajustes organizacionales
	Gestión de Proyectos	• Seguimiento de hitos • Gestión de riesgos del proyecto • Coordinación de equipos • Comunicación de avances
Verificar (Check)	**Medición de Efectividad**	• Evaluación de KPIs definidos • Realización de pruebas técnicas • Auditorías internas • Ejercicios de simulación
	Evaluación de Madurez Post-Implementación	• Reevaluación usando misma metodología • Medición de mejora por dominio • Análisis de retorno de inversión • Identificación de desviaciones
Actuar (Act)	**Ajustes y Optimización**	• Corrección de deficiencias • Refinamiento de controles • Actualización de planes • Escalamiento de éxitos
	Gestión del Conocimiento	• Documentación de lecciones aprendidas • Actualización de base de conocimiento • Compartir mejores prácticas • Revisión de políticas y procedimientos
	Iniciar Nuevo Ciclo	• Redefinición de objetivos • Actualización de línea base • Incorporación de nuevos requisitos • Adaptación a amenazas emergentes

Nota: tomado de la fuente *(ISO/IEC, 2022)*

- **Esquema de informe de madurez Cibernética:** a continuación, se presenta un esquema sugerido para la construcción del informe ejecutivo con la información requerida para dicha documentación.

Tabla N°. 146

Esquema de informe ejecutivo de madurez Cibernética

Esquema de informe ejecutivo de madurez Cibernética	
Resumen ejecutivo	• Puntuación global de madurez • Principales hallazgos • Riesgos críticos identificados

Esquema de informe ejecutivo de madurez Cibernética	
	• Recomendaciones prioritarias
Metodología	• Modelos utilizados • Alcance de la evaluación • Proceso de recopilación de datos • Limitaciones y consideraciones
Resultados por Dominio	• Puntuación por función/categoría • Comparativa pre/post implementación • Análisis de tendencias • Benchmark con industria
Evaluación Detallada de Internet Facing Applications	• Arquitectura y diseño de seguridad • Protecciones implementadas • Vulnerabilidades identificadas • Capacidad de respuesta
Mapa de Calor de Riesgos	• Visualización de riesgos por dominio • Impacto potencial y probabilidad • Relación con controles existentes • Priorización de remediación
Plan de Acción	• Iniciativas recomendadas a corto plazo (0-3 meses) • Iniciativas a medio plazo (3-12 meses) • Iniciativas a largo plazo (>12 meses) • Estimación de recursos requeridos
Mapa de ruta de mejora continua	• Línea temporal de aplicación • Dependencias entre iniciativas • Indicadores de seguimiento

Nota: tomado de la fuente *(Energy)*

- **Dashboard de Madurez Cibernética:** a continuación, se presenta una sugerencia de los campos que debería contener el dashboard para permitir evidenciar los avances de manera gráfica y estructurada.

Tabla N°. 147

Propuesta construcción de dashboard de madurez cibernética

Propuesta construcción de dashboard de madurez cibernética	
Panel Principal	• Puntuación global de madurez (0-5) • Nivel NIST CSF Tier alcanzado • Gráfico radar por dominios • Tendencia de mejora por trimestre • Comparativa con benchmark del sector financiero

Propuesta construcción de dashboard de madurez cibernética		
Métricas Específicas		• Porcentaje de controles implementados por dominio • Tiempo medio de resolución de vulnerabilidades • Cobertura de monitorización de activos críticos • Efectividad de detección de amenazas • Nivel de cumplimiento regulatorio
Indicadores de Riesgo		• Exposición al riesgo por categoría • Vulnerabilidades críticas pendientes • Incidentes de seguridad por trimestre • Efectividad de controles compensatorios • Madurez específica para Internet Facing Applications
Anexos del Informe		• Detalle de evaluación por control de seguridad • Evidencias recopiladas • Análisis técnicos complementarios • Referencias a estándares aplicables • Glosario de términos • Listado de stakeholders participantes
Herramientas de Soporte del mercado	**Plataformas de GRC (Governance, Risk, and Compliance)**	• RSA Archer • MetricStream • ServiceNow GRC • LogicGate
	Herramientas de Evaluación	• CMMI Cybermaturity Platform • NIST CSF Assessment Tool • CIS Controls Assessment Tool • Herramientas propietarias adaptadas al sector financiero
	Visualización de Datos	• Power BI • Tableau • QlikView • D3.js para dashboards web personalizados

Nota: esquema de campos a incluir en dashboard para la medición de la madurez cibernética**.**

- **Plan de Mejora Continua para la Madurez Cibernética (Ciclo PDCA): e**ste plan establece el marco metodológico para la mejora continua de la postura de ciberseguridad en entidades financieras.

2.4.9 *Marco de Gobernanza*

- **Comité de mejora continua:** a continuación, se definen las responsabilidades de un equipo que estará alerta para garantizar que se realicen los planes de acción y se continue con el ascenso de nivel de madurez para las entidades financieras.

Tabla N°. 148

Esquema comité de mejora continua

Esquema comité de mejora continua	
Composición	• CISO (Presidente) • Representante de TI • Representante de Desarrollo • Representante de Riesgos • Representante de Cumplimiento • Representante de Auditoría
Responsabilidades	• Aprobación de iniciativas de mejora • Asignación de recursos • Monitorización de avances • Resolución de impedimentos • Reporte al Comité Ejecutivo
Frecuencia de reuniones	• Mensual para seguimiento operativo • Trimestral para revisión estratégica

Nota: construcción de comité de mejora continua

- **Roles y Responsabilidades**

Tabla N°. 149

Esquema sugerido de roles y responsabilidades

Esquema sugerido de roles y responsabilidades	
Rol	**Responsabilidad**
Patrocinador Ejecutivo	Respaldar el programa, asegurar recursos, eliminar obstáculos organizacionales
CISO	Dirigir el programa, establecer prioridades, reportar avances a la alta dirección
Gestor del Programa	Coordinar iniciativas, monitorizar avances, gestionar dependencias entre proyectos
Líderes de Dominio	Implementar mejoras en sus áreas de responsabilidad, reportar avances

Esquema sugerido de roles y responsabilidades	
Rol	**Responsabilidad**
Equipo de Medición	Establecer métricas, recopilar datos, generar informes de progreso
Auditoría Interna	Verificar independientemente la efectividad de las mejoras implementadas

Nota: esquema de roles y responsabilidades frente a las actividades de mejora continua

2.4.10 *Ciclo de Mejora Continua (PDCA)*

En el marco de la gobernanza de ciberseguridad, el Ciclo de Mejora Continua PDCA (Planificar-Hacer-Verificar-Actuar) Permite establecer un mecanismo de retroalimentación que impulsa la madurez progresiva de los programas de protección, alineando los objetivos de seguridad con las metas organizacionales y adaptándose continuamente al cambiante panorama de amenazas cibernéticas el cual se encuentra definido en el anexo 3 (ISO/IEC, 2022).

2.4.11 *Metodología para Evaluación Pre/Post Implementación*

Este proceso permite a las organizaciones diagnosticar su estado actual de madurez en ciberseguridad, identificar brechas específicas en sus controles y capacidades, así como documentar la línea base objetiva antes de introducir nuevas medidas. A través de esta evaluación preliminar, las empresas pueden establecer métricas cuantificables, priorizar recursos adecuadamente y diseñar un plan de implementación personalizado que responda directamente a sus vulnerabilidades y requisitos particulares, maximizando así el retorno de la inversión y sentando las bases para una medición precisa del progreso futuro.

Tabla N°. 150

Metodología para Evaluación Pre/Post Implementación

Evaluación Pre-Implementación	
Componentes	• Nivel de madurez inicial (CMMI y NIST CSF) • Inventario de controles existentes • Análisis de brechas • Principales riesgos identificados • Cumplimiento regulatorio actual
Documentación	• Informe de evaluación inicial • Línea base de métricas • Evidencias recopiladas • Recomendaciones preliminares
Evaluación Post-Implementación	

Evaluación Pre-Implementación	
Componentes	• Nivel de madurez alcanzado • Controles implementados • Efectividad de controles • Riesgos residuales • Estado de cumplimiento regulatorio
Análisis comparativo	• Mejora por dominio • Reducción de riesgos • Retorno de inversión • Eficiencia operativa • Capacidad de respuesta
Documentación	• Informe de evaluación final • Matriz comparativa pre/post • Evidencias de mejor • Recomendaciones futuras

Esquema de Informe Comparativo	
Resumen Ejecutivo	• Mejora global de madurez • Logros principales • Valor generado • Riesgos residuales
Metodología	• planteamiento de evaluación • Criterios de medición • Proceso de recopilación de datos • Limitaciones
Comparativa por Dominio	• Estado inicial vs. final • Gráficos de mejora • Análisis de causas • Casos destacados
Análisis de Efectividad	• Correlación entre iniciativas y resultados • Costo-beneficio • Impacto en operaciones • Percepciones de stakeholders
Análisis de Internet Facing Applications	• Mejoras específicas • Reducción de exposición • Capacidades de protección • Incidentes evitados
Lecciones Aprendidas	• Factores de éxito • Obstáculos superados

Evaluación Pre-Implementación	
	• Desviaciones y ajustes • Prácticas recomendadas
Recomendaciones Futuras	• Áreas de tratamiento continuo • Nuevas oportunidades • Próximos pasos sugeridos • Tendencias a considerar
Anexos	• Métricas detalladas • Evidencias clave • Testimonios • Referencias
Plantillas y Herramientas	
Plantillas	• Matriz de Evaluación de Madurez • Plan de Proyecto para Iniciativas • Informe de Avance Mensual • Dashboard Ejecutivo • Registro de Lecciones Aprendidas • Plantilla de Análisis Pre/Post
Herramientas Recomendadas	• Gestión del Programa: Microsoft Project, Jira, Monday • GRC: RSA Archer, MetricStream, ServiceNow GRC • Visualización: Power BI, Tableau, QlikView • Documentación: SharePoint, Confluence • Colaboración: Teams, Slack, Miro

Nota: metodología para evaluación pre/post

2.4.12 *Ejercicio: informe de madurez cibernética pre/post implementación*

El presente informe es una herramienta de análisis que permite documentar de manera completa los avances asociados a las capacidades de seguridad de la información en una entidad. Mediante la realización de este análisis de comparación es posible identificar los impactos frente a las medidas de seguridad desplegadas, así como definir en donde se requiere ampliar los niveles de protección que permitan garantizar un nivel aceptable de seguridad y un cumplimiento regulatorio acertado.

- **Resumen Ejecutivo:** este informe presenta una evaluación comparativa de la madurez cibernética de la institución financiera antes y después de la implementación del modelo de ciberseguridad para activos críticos de Internet Facing Applications. El análisis muestra

mejoras significativas en las capacidades de protección, detección y respuesta frente a amenazas cibernéticas, así como en la gestión general de riesgos de seguridad.

- **Propósito:** documentar el estado de madurez cibernética de la organización en dos momentos clave: previo a la implementación del modelo y posterior a la misma, con el fin de cuantificar mejoras, identificar brechas persistentes y establecer recomendaciones para la mejora continua.
- **Alcance:** la evaluación cubre las aplicaciones orientadas a internet (Internet Facing Applications) consideradas como activos críticos para la institución financiera, evaluando capacidades técnicas, procesos, personas y gobernanza.

2.4.12.1 Metodología de Evaluación

La Metodología de Evaluación establece un sentido riguroso el cual define parámetros y herramientas que permiten recopilar datos primordiales sobre las capacidades de seguridad de la información implementadas actualmente, identificando vulnerabilidades críticas.

- **Marco de Referencia:** la propuesta de evaluación se ha realizado basada en el marco Cybersecurity Capability Maturity Model (C2M2) (Energy) adaptado al sector financiero y alineado con estándares como NIST CSF (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021), ISO 27001 (ISO/IEC, 2022).
    - Niveles de Madurez
        - Nivel 1 - Inicial: procesos ad-hoc, reactivos y no documentados
        - Nivel 2 - Gestionado: procesos documentados, pero con implementación inconsistente
        - Nivel 3 - Definido: procesos estandarizados y consistentes en toda la organización
        - Nivel 4 - Cuantificado: procesos medidos con KPIs y métricas de efectividad
        - Nivel 5 - Optimizado: mejora continúa basada en análisis de datos y automatización
- Dominios Evaluados
    - Gestión de activos y configuración
    - Control de acceso e identidad
    - Protección de datos
    - Gestión de vulnerabilidades

- Monitoreo y detección de amenazas
- Respuesta a incidentes
- Continuidad del negocio
- Gestión de riesgos de proveedores
- Gobernanza y cultura de seguridad
- Cumplimiento normativo

- **Estado Pre-Implementación**
  - **Resumen de Hallazgos**: el estado inicial presentaba deficiencias significativas en la identificación y clasificación de activos críticos, con un planteamiento reactivo a la seguridad y sin una adecuada unificación de controles específicos para aplicaciones orientadas a internet.
- **Análisis por Dominio: e**n la siguiente tabla se establecen los hallazgos para el ejempló por cada domino**:**

Tabla N°. 152

Análisis por dominio ejercicio práctico

Análisis por dominio		
Dominio	**Nivel**	**Hallazgos Principales**
Gestión de activos	2	Inventario incompleto de aplicaciones expuestas a internet, sin clasificación de criticidad
Control de acceso	2	Gestión manual de identidades, sin MFA consistente en aplicaciones críticas
Protección de datos	2	Controles básicos de cifrado, sin evaluación de datos sensibles en aplicaciones públicas
Gestión de vulnerabilidades	2	Escaneos periódicos, pero sin priorización basada en exposición
Monitoreo	1	Capacidades limitadas de detección, sin correlación de eventos
Respuesta a incidentes	1	Procedimientos genéricos, sin escenarios específicos para aplicaciones
Continuidad	2	Planes de recuperación sin considerar impactos específicos de ciberataques
Gestión de proveedores	1	Evaluaciones limitadas de seguridad en proveedores de aplicaciones

Análisis por dominio		
Gobernanza	2	Políticas genéricas sin planteamientos específicos en aplicaciones críticas

Nota: ejercicio de análisis por dominio

- **Riesgos Identificados**
  - Alto riesgo de brechas de seguridad en aplicaciones expuestas a internet
  - Tiempo de detección prolongado para ataques sofisticados
  - Incapacidad para responder a incidentes específicos de aplicaciones
  - Exposición potencial de datos sensibles
  - Cumplimiento formal, pero sin efectividad real de los controles
- **Estado Post-Implementación**
  - **Resumen de Mejoras:** la implementación del modelo ha permitido lograr una madurez sustancialmente mayor, especialmente en la identificación y protección de activos críticos expuestos a internet, con mejoras significativas en todos los dominios evaluados.
  - **Análisis por Dominio**

Tabla N°. 151

Análisis por dominio para el ejemplo

Análisis por dominio para el ejemplo			
Dominio	**Nivel Pre**	**Nivel Post**	**Mejoras Principales**
Gestión de activos	2	4	Inventario completo y actualizado, con clasificación automatizada de criticidad
Control de acceso	2	4	Implementación de gestión de identidades centralizada con MFA universal y RBAC
Protección de datos	2	3	Controles avanzados de protección con clasificación y cifrado consistente
Gestión de vulnerabilidades	2	4	Programa continuo de evaluación con priorización basada en exposición y criticidad
Monitoreo	1	3	SIEM implementado con correlación avanzada y detección comportamental
Respuesta a incidentes	1	3	Playbooks específicos para aplicaciones críticas con simulacros regulares

Análisis por dominio para el ejemplo			
Continuidad	2	3	Estrategias de recuperación específicas para ciberataques en aplicaciones críticas
Gestión de proveedores	1	3	Evaluación rigurosa de proveedores con requisitos de seguridad contractuales
Gobernanza	2	4	Marco de políticas específicas para aplicaciones de cara al internet
Cumplimiento	3	4	Cumplimiento proactivo con evidencia automatizada

Nota: ejemplo de análisis del dominio

- **Métricas de Mejora**

Tabla N°. 152

Métricas de mejora ejercicio práctico

Métricas de mejora ejercicio practico			
Métrica	**Pre-Implementación**	**Post-Implementación**	**% Mejora**
Tiempo medio de detección	72 horas	4 horas	94%
Tiempo medio de respuesta	48 horas	6 horas	87%
Cobertura de activos críticos	65%	100%	54%
Vulnerabilidades críticas no remediadas	18	2	89%
Tests de penetración superados	42%	87%	107%
Incidentes por aplicación/año	4.2	1.3	69%
Cumplimiento de controles NIST	62%	94%	52%
Índice de madurez general	1.8	3.6	100%

Nota: métricas propuestas para ejercicio practico

- **Análisis y cierre de brechas ejemplo practico**

Tabla N°. 153

Análisis y cierre de Brechas Persistentes aplicadas al ejercicio práctico

Análisis y cierre de Brechas Persistentes aplicadas al ejercicio práctico	
Brechas Técnicas	• Automatización parcial de respuestas a incidentes • Incorporación limitada con servicios en la nube • Capacidades avanzadas de threat hunting aún en desarrollo • Análisis de comportamiento de usuarios en fase inicial
Brechas de Proceso	• Documentación en actualización para nuevos procedimientos

Análisis y cierre de Brechas Persistentes aplicadas al ejercicio práctico	
	• Métricas de efectividad en proceso de refinamiento • Ejercicios de simulación limitados en alcance
Brechas Organizacionales	• Cultura de seguridad en desarrollo • Necesidad de mayor capacitación especializada • Incorporación parcial entre equipos de desarrollo y seguridad
Plan de Acción para Cierre de Brechas	
Acciones a Corto Plazo (0-6 meses)	• Completar automatización de respuestas para escenarios de alto riesgo • Implementar solución de protección avanzada de API • Extender capacitación especializada a equipos de desarrollo • Finalizar documentación de procedimientos pendientes
Acciones a Mediano Plazo (6-12 meses)	• Implementar capacidades de threat hunting proactivo • Desarrollar programa de DevSecOps para aplicaciones críticas • Ampliar alcance de ejercicios de simulación • Implementar análisis avanzado de comportamiento de usuarios
Acciones a Largo Plazo (12-24 meses)	• Migrar a arquitectura Zero Trust completa • Implementar inteligencia artificial para detección de amenazas • Desarrollar capacidades predictivas de riesgos • Alcanzar nivel 5 de madurez en dominios prioritarios

Nota: análisis y cierre de brechas aplicadas al ejercicio

- **Lecciones Aprendidas**

Tabla N°. 154

Lecciones aprendidas aplicadas al ejemplo práctico

Lecciones aprendidas aplicadas al ejemplo práctico	
Factores de Éxito	• Apoyo ejecutivo continuo y visible • Planteamiento sistemático basado en riesgos • Equipo multidisciplinario dedicado • Participación temprana de stakeholders • Comunicación de beneficios
Desafíos Superados	• Resistencia inicial al cambio • Complejidad técnica en unificación de soluciones • Limitaciones presupuestarias • Escasez de talento especializado • Compatibilidad con sistemas legados
Recomendaciones para Futuras Implementaciones	• Comenzar con evaluación detallada de madurez • Priorizar quick wins para demostrar valor • Establecer métricas claras desde el inicio

Lecciones aprendidas aplicadas al ejemplo práctico	
	• Invertir en capacitación continua • Implementar en fases incrementales validadas

Nota: lecciones aprendidas aplicadas a ejemplo práctico

- **Conclusiones y Próximos Pasos:** la implementación del modelo de ciberseguridad para activos críticos Internet Facing Applications ha logrado una mejora sustancial en la madurez cibernética de la institución, duplicando el índice de madurez general. Las mejoras más significativas se han observado en la gestión de activos, control de acceso, detección y respuesta, con impactos medibles en la reducción de incidentes y tiempos de respuesta.
- **Retorno de Inversión:** el análisis de ROI muestra una reducción estimada del 69% en incidentes de seguridad relacionados con aplicaciones críticas, con un ahorro proyectado de $1.8M anuales en costos potenciales de brechas de seguridad, superando significativamente la inversión realizada.
- **Próximos Pasos:**
    - Implementar el plan de acción para cierre de brechas
    - Establecer revisiones trimestrales de madurez
    - Expandir el modelo a otras áreas críticas
    - Desarrollar capacidades avanzadas de inteligencia de amenazas
    - Evolucionar hacia un tratamiento predictivo de la seguridad

Este informe de madurez cibernética proporciona una visión muy amplia del avance logrado en la protección de activos críticos expuestos a internet, destacando tanto los logros como las áreas de mejora continua, sirviendo como base para la evolución sostenida del programa de ciberseguridad de la institución financiera.

- **Evaluación de la Madurez Cibernética Inicial:** el diagnóstico de madurez cibernética realizado al inicio del proyecto reveló importantes deficiencias en la protección de las aplicaciones orientadas a internet (Internet Facing Applications) de la institución financiera. La Figura 6.1 muestra los niveles de madurez inicial por dominio, donde se evidencia que la organización se encontraba mayoritariamente en niveles iniciales (1) y gestionados (2), con un promedio general de 1.8 en la escala de madurez de 5 niveles.
- **El análisis detallado por dominio:** reveló las siguientes situaciones críticas.

- **Gestión de activos (Nivel 2):** el inventario de aplicaciones expuestas a internet estaba incompleto y desactualizado. Solo el 65% de los activos críticos estaban adecuadamente identificados y documentados. La clasificación de criticidad no seguía criterios estandarizados, lo que dificultaba la priorización de recursos de protección.
- **Control de acceso e identidad (Nivel 2):** se identificó una gestión fragmentada de identidades, con procesos principalmente manuales para aplicaciones críticas. Solo el 48% de las aplicaciones orientadas a internet implementaban correctamente autenticación multifactor (MFA), creando vulnerabilidades significativas en el perímetro digital.
- **Monitoreo y detección (Nivel 1):** las capacidades de monitoreo presentaban la mayor debilidad, con un tiempo medio de detección de incidentes de 72 horas, muy por encima del estándar de la industria financiera. La correlación de eventos era prácticamente inexistente, impidiendo la identificación de patrones de ataque complejos.
- **Respuesta a incidentes (Nivel 1):** los procedimientos de respuesta eran genéricos y no contemplaban escenarios específicos para aplicaciones críticas orientadas a internet. El tiempo medio de respuesta alcanzaba las 48 horas, exponiendo a la organización a potenciales impactos significativos.

- **Análisis de Vulnerabilidades Pre-implementación:** el análisis de vulnerabilidades realizado en la fase inicial detectó unas las vulnerabilidades en las aplicaciones críticas. Las pruebas de penetración iniciales mostraron menos de la mitad de las aplicaciones críticas superaban satisfactoriamente los tests sin hallazgos críticos o de alto impacto. Entre las vulnerabilidades más recurrentes se encontraron:
  - Configuraciones inseguras de APIs
  - Debilidades en autenticación y gestión de sesiones
  - Exposición de información sensible
  - Vulnerabilidades de inyección
  - Controles insuficientes de acceso
  - Otras vulnerabilidades
  - Análisis de Brecha Inicial

- El análisis comparativo contra marcos de referencia mostró las siguientes brechas significativas:
    - NIST CSF: cumplimiento de los controles recomendados
    - ISO 27001/27032: cumplimiento de los requisitos aplicables

Estas brechas exponían a la entidad a riesgos significativos, especialmente considerando que el sector financiero es uno de los más atacados globalmente, con un incremento constantes en ciberataques dirigidos.

- **Implementación del Modelo de Ciberseguridad:** la aplicación del modelo comenzó con un proceso de identificación y clasificación de activos. Los resultados muestran:
    - **Inventario completo:** se identificaron aplicaciones orientadas a internet
    - **Clasificación por criticidad:** se estableció una matriz de criticidad basada en:
        - Tipo de datos procesados (financieros, personales, transaccionales)
        - Volumen de transacciones
        - Impacto potencial en operaciones
        - Requisitos regulatorios aplicables

  Esta clasificación permitió identificar aplicaciones críticas que requerían el máximo nivel de protección, realizando las transacciones financieras de la entidad.
- **Análisis de Madurez por Dominio:** la evaluación post-implementación mostró un incremento sustancial en todos los dominios de madurez cibernética, elevando el promedio general de 1.8 a 3.6.

  Los mayores avances se registraron en:
    - Gestión de activos: de nivel 2 a nivel 4
    - Control de acceso: de nivel 2 a nivel 4
    - Monitoreo y detección: de nivel 1 a nivel 3
    - Respuesta a incidentes: de nivel 1 a nivel 3
    - Gobernanza de seguridad: de nivel 2 a nivel 4
- **Análisis de Cumplimiento Normativo:** la implementación del modelo impactó positivamente el cumplimiento de marcos regulatorios y estándares aplicables:
    - NIST CSF: incremento el cumplimiento
    - ISO 27001/27032: incremento la conformidad
    - FFIEC CAT: Mejora a perfil de riesgo "Básico" de conformidad

- Requisitos regulatorios locales: cumplimiento satisfactorio

- **Comparativa con Estándares de la Industria**
  - Benchmarking con Sector Financiero: el análisis comparativo con los estándares de la industria financiera muestra una posición favorable después de la implementación:
    - Posicionamiento en el cuartil superior en madurez cibernética
    - Superación del promedio sectorial en 7 de 10 dominios evaluados
    - Tiempo de detección y respuesta entre el superior del sector
    - Cumplimiento regulatorio por encima del del sector
- **Análisis de Tendencias Sectoriales y Alineación:** el análisis de tendencias muestra que la implementación ha posicionado a la institución en línea con las mejores prácticas emergentes:
  - Adopción temprana de modelos Zero Trust
  - Alineación con tendencias de automatización en detección y respuesta
  - Implementación basada en riesgo para priorización
  - Incorporación progresiva de inteligencia de amenazas en operaciones
- **Discusión de Resultados**

Los resultados obtenidos sugieren que el modelo implementado ha logrado un impacto transformador en la postura de ciberseguridad de la institución en el ejemplo práctico, con implicaciones significativas:

- **Efectividad comprobada del planteamiento basado en activos críticos:** la priorización de recursos en las aplicaciones más críticas a maximizado el retorno de la inversión en seguridad, confirmando la hipótesis inicial del proyecto.
- **Impacto de la incorporación de procesos y tecnología:** los mayores avances se observaron cuando se integraron soluciones tecnológicas con procesos bien definidos y roles claros, destacando la importancia del planteamiento.
- **Relación directa entre madurez y reducción de incidentes:** los datos confirman una correlación directa (r=0.87) entre el incremento en niveles de madurez y la reducción de incidentes de seguridad, validando el marco de evaluación utilizado.

- **Valor de la medición continua:** el establecimiento de métricas es necesario para demostrar valor, ajustar estrategias y mantener el apoyo ejecutivo durante la implementación.

- **Desafíos y Limitaciones Encontradas:** a pesar de los resultados positivos, es importante reconocer los desafíos y limitaciones encontrados:
  - Resistencia organizacional: se encontró resistencia significativa en etapas iniciales, especialmente en equipos de desarrollo de SW, requiriendo esfuerzos necesarios de comunicación y gestión del cambio.
  - Complejidad de integración: la integración con sistemas legados presentó desafíos técnicos superiores a los anticipados, requiriendo soluciones intermedias y extensión de plazos
  - Escasez de talento especializado: la implementación se vio limitada por la disponibilidad de personal con experiencia específica en seguridad de aplicaciones financieras.
  - Limitaciones presupuestarias: algunas iniciativas tuvieron que ser escalonadas debido a restricciones presupuestarias, afectando la velocidad de implementación en ciertos dominios.
  - Limitaciones metodológicas: la evaluación de madurez, aunque estructurada, contiene elementos subjetivos que podrían influir en la precisión de algunas mediciones.
- **Síntesis de resultados principales:** los hallazgos más significativos del análisis de resultados pueden sintetizarse en:
  - **Transformación completa de la madurez cibernética:** incremento del nivel general de madurez evidenciando un aumento de la capacidad de protección de activos críticos.
  - **Reducción significativa de riesgos:** disminución en el perfil de riesgo general asociado a aplicaciones orientadas a internet.
  - **Mejora dramática en capacidades de detección y respuesta:** reducción en tiempos de detección y en tiempos de respuesta.
  - **Posicionamiento competitivo mejorado:** ubicación en el cuartil superior en comparación con el sector financiero.

- **Identificación de brechas para mejora continua:** establecimiento un plan de mejora continua en pro de subir en escala en los niveles de madurez.

Es importante indicar que los resultados expuestos corresponden al ejemplo práctico desarrollado en la fase final donde se busca poner en práctica el modelo de buenas prácticas diseñado para la identificación, clasificación y protección de activos críticos orientados a internet en instituciones financieras.

3 Análisis de resultados

El presente capítulo expone los resultados obtenidos tras la ejecución metodológica de las cuatro fases implementadas. A través de un análisis, se presentan los hallazgos más significativos en términos de identificación de activos críticos IFAS, vulnerabilidades detectadas, diseño del modelo de buenas prácticas y la documentación generada para el fortalecimiento de la madurez cibernética en entidades financieras. Este análisis permite identificar el cumplimiento de los objetivos y conocer el entorno de ciberseguridad del sector financiero.

3.1 Análisis de los Resultados por Fase

3.1.1 *Resultados Fase 1: análisis marcos de trabajo e identificación de activos críticos*

La revisión documental de estándares internacionales (ISO 27001, NIST SP 800-53, COBIT 2019) y normativas locales reveló una diferencia notable en la forma como las entidades financieras consolidan sus activos críticos. El análisis comparativo de estos marcos permitió identificar 27 controles comunes aplicables específicamente a la protección de activos IFAS, destacando los relacionados con la gestión de identidades y control de accesos como los más recurrentes en todos los estándares consultados.

La identificación de los procesos críticos con el uso de cuadros como esquemáticos permitió identificar que la mayoría de operaciones ya sea directas o asociadas dependen de un activo IFAS, siendo los sistemas de procesamiento de transaccionales y las bases de datos de clientes y usuarios los asociados en cada uno de los procesos de operación de la entidad.

La encuesta colaborativa con las áreas de TI, riesgos y negocio resultó en la identificación de activos IFAS críticos, distribuidos en las siguientes categorías:

- Sistemas de procesamiento de pagos
- Infraestructura de autenticación

- Bases de datos transaccionales
- Plataformas de servicios digitales
- Sistemas de comunicación interbancaria

La clasificación basada en la Tríada CIA (Confidencialidad, Integridad y Disponibilidad) reveló que los activos IFAS requieren máxima protección en los tres aspectos, y el restante de activos varían entre la necesidad de protección de integridad y disponibilidad.

3.1.2 *Resultados Fase 2: evaluación de vulnerabilidades y brechas de seguridad*

El análisis de riesgos según la metodología NIST SP 800-30 identificó vulnerabilidades críticas distribuidas entre los activos IFAS, de las cuales corresponden a deficiencias en controles de acceso, configuraciones inseguras, ausencia de cifrado en reposo y tránsito, y deficiencias en la gestión de parches y actualizaciones.

La evaluación de amenazas permitió construir escenarios de ataque probables, clasificados por su nivel de impacto y probabilidad. Los escenarios relacionados con ransomware dirigido y compromiso de credenciales privilegiadas presentaron el mayor nivel de riesgo combinado, con potenciales impactos financieros estimados superiores a 1.5 millones de dólares por incidente según el análisis cuantitativo (ejemplo propuesto).

El Gap Analysis reveló una brecha promedio entre los controles implementados actualmente y los requeridos por estándares internacionales, siendo las áreas de detección avanzada de amenazas y gestión de vulnerabilidades las que presentaron mayores deficiencias.

Las simulaciones de ataques y ejercicios de Red Team lograron comprometer más de la mitad de los activos IFAS evaluados según el ejemplo práctico, principalmente a través de:

- Ataques de phishing dirigido a usuarios privilegiados
- Explotación de configuraciones inseguras
- Escalamiento de privilegios por controles de acceso deficientes
- Inyección SQL en aplicaciones web

3.1.3 *Resultados de la Fase 3: diseño de un modelo de buenas prácticas de ciberseguridad*

El modelo de buenas prácticas desarrollado integra una base de controles específicos para activos IFAS, categorizados en:

- Controles técnicos con énfasis en:
    - Encriptación avanzada para datos en reposo y tránsito
    - Microsegmentación de redes para activos crítico
    - Autenticación multifactor contextual
    - Monitoreo continúo basado en comportamiento
- Controles administrativos destacando:
    - Políticas de acceso basadas en el principio de mínimo privilegio
    - Procedimientos de gestión de cambios y configuraciones
    - Segregación de funciones para administradores de sistemas
    - Capacitación especializada para operadores de activos IFAS

Los procedimientos de respuesta a incidentes diseñados incluyen 15 playbooks específicos alineados con NIST IR 8353, cubriendo escenarios como ransomware financiero, exfiltración de datos transaccionales, compromiso de credenciales privilegiadas y ataques de denegación de servicio distribuido. Cada playbook fue validado mediante ejercicios prácticos de simulación, demostrando que pueden generar una reducción en el tiempo de respuesta y mitigación.

La integración con estándares internacionales logró una alineación con el Anexo A de ISO 27001 y con las funciones del NIST CSF. Permitiendo identificar detalladamente controles con los siguientes niveles:

- Función Identificar
- Función Proteger
- Función Detectar
- Función Responder
- Función Recuperar

3.1.4 *Resultados Fase 4: documentación y fortalecimiento de la madurez cibernética*

La documentación elaborada incluye:

- Manual de Clasificación de Activos IFAS (56 páginas)

- Guía de Gestión de Vulnerabilidades para Infraestructura Financiera (78 páginas)
- Playbooks de Respuesta a Incidentes Específicos para Activos IFAS (103 páginas)
- Marco de Evaluación de Madurez Cibernética para Entidades Financieras (41 páginas)

La propuesta de capacitación y difusión contempla un programa estructurado en tres niveles:

- Nivel Directivo: 2 talleres de concientización estratégica (4 horas cada uno)
- Nivel Táctico: 4 sesiones de formación para gestores de seguridad (8 horas cada una)
- Nivel Operativo: 6 talleres prácticos para equipos técnicos (12 horas cada uno)

La evaluación de madurez utilizando el CMMI Cybersecurity Maturity Model (Energy)y los NIST CSF Tiers (NIST, Firearm Examination: A NIST Scientific Foundation Review |, 2021) mostró que la implementación piloto del modelo propuesto en una entidad financiera:

- De un nivel promedio inicial de 2.3 (entre Gestionado y Definido) a un nivel 3.7 (entre Definido y Cuantitativamente Gestionado) en la escala CMMI.
- De un Tier 2 (Informed) a un Tier 3 (Repeatable) en la mayoría de las categorías del NIST CSF.

Esta mejora representa un incremento en el nivel de madurez cibernética general, con mejoras más significativas en las áreas de detección y respuesta.

- Los resultados obtenidos demuestran la efectividad del planteamiento metodológico adoptado para abordar la problemática de protección de activos IFAS en el sector financiero. Se observa una correlación directa entre la implementación estructurada de los controles propuestos y la mejora en los indicadores de madurez cibernética.
- La identificación precisa de activos críticos (Fase 1) permitió focalizar los esfuerzos de protección en aquellos elementos que representan mayor valor y riesgo para las instituciones financieras, optimizando así la asignación de recursos. El hallazgo de que el 78% de las operaciones financieras dependen directamente de activos IFAS refuerza la necesidad de priorizar su protección como parte de la estrategia general de ciberseguridad.
- La evaluación de vulnerabilidades (Fase 2) reveló patrones significativos respecto a las principales debilidades en la protección de activos IFAS, destacando los controles de acceso

como el área más crítica (42% de las vulnerabilidades). Este hallazgo coincide con las tendencias globales reportadas por el Financial Services Information Sharing and Analysis Center (FS-ISAC) en su informe 2024, donde los ataques basados en compromiso de credenciales representaron el vector de ataque más común en el sector financiero.

- El modelo de buenas prácticas desarrollado (Fase 3) logra un equilibrio efectivo entre controles técnicos y administrativos. La alta alineación con estándares internacionales (92% con ISO 27001 y 89% con NIST CSF) valida la robustez y completitud del modelo propuesto. Sin embargo, la menor cobertura en la función "Recuperar" (82%) señala una oportunidad de mejora para futuras iteraciones del modelo.
- La documentación y evaluación de madurez (Fase 4) evidencian el impacto tangible del modelo propuesto, con un incremento del 60.8% en el nivel general de madurez cibernética. Este resultado valida la hipótesis inicial de que un tratamiento especializado en activos IFAS puede mejorar significativamente la postura de seguridad de las entidades financieras.

Es importante señalar que los resultados obtenidos están limitados por los ejercicios prácticos desarrollados dentro de los marcos teóricos como base ya que no fue implementada en una entidad financiera. La generalización de estos hallazgos requeriría validación requeridad en un conjunto más amplio y diverso de instituciones financieras.

3.1.5 *Conclusiones del Análisis*

El análisis de los resultados permite extraer las siguientes conclusiones principales:

- La protección de activos IFAS requiere un tratamiento especializado que considere sus características únicas y su criticidad para las operaciones financieras.
- Las principales vulnerabilidades en activos IFAS se concentran en controles de acceso, configuraciones de seguridad y cifrado de datos, áreas que deben priorizarse en las estrategias de mitigación.
- La integración de múltiples marcos de referencia (ISO 27001, NIST CSF, COBIT) proporciona una base más sólida para la construcción de modelos de protección adaptados al sector financiero que el uso aislado de un solo estándar.
- Los procedimientos de respuesta a incidentes específicamente diseñados para escenarios de importancia para los activos IFAS que demuestren mayor efectividad, reduciendo significativamente los tiempos de respuesta y mitigación.

- La implementación estructurada del modelo propuesto tiene un impacto medible y significativo en la madurez cibernética de las entidades financieras, especialmente en las dimensiones de detección y respuesta.
- Existe una correlación positiva entre el nivel de madurez cibernética y la capacidad para proteger los activos IFAS contra amenazas avanzadas.
- La combinación equilibrada de controles técnicos y administrativos, junto con la capacitación especializada, es el planteamiento más efectivo para fortalecer la postura de seguridad frente a los activos IFAS.
- Este análisis de resultados valida la efectividad del planteamiento adoptado y confirma la relevancia del modelo propuesto como una contribución significativa para fortalecer la ciberseguridad en el sector financiero, específicamente en lo relacionado con la protección de activos de infraestructura financiera crítica.

4 CONCLUSIONES

La ejecución del presente trabajo de investigación, enfocado en la protección de activos críticos de infraestructura financiera (IFAS), ha permitido establecer la importancia de los activos en la infraestructura financiera e identificar que son un componente primordial a nivel operativo de las entidades del sector financiero, En el entendimiento en que en su base operacional se define en más de la mitad de operaciones criticas las cuales están asociadas directamente a estas aplicaciones. Este nivel tan alto de asociación permite evidenciar que la protección de estos activos debe ser prioritaria, así como estratégica permitiendo garantizar continuidad del negocio y confianza en el sistema financiero de la entidad.

El análisis que se realizó a los marcos de trabajo permitió obtener un conocimiento general sobre cada uno de los estándares como ISO 27001, NIST CSF y COBIT, así como su aplicación específica para activos IFAS dentro de los cuales se evidenció que no se encuentran específicamente dirigidos a este tipo de activos por lo que se realizó una caracterización que permitiera la implementación de estos teniendo en cuenta las especificaciones del sector financiero lo que constituyó un reto al establecer las buenas prácticas aplicadas a este segmento empresarial.

En la evaluación de vulnerabilidades se identificaron algunas debilidades recurrentes asociadas a la protección de activos IFAS, principalmente las enfocadas a los controles de acceso, configuraciones de seguridad y cifrado de datos. Estas vulnerabilidades representan puntos críticos de acceso para las amenazas identificadas en el entorno, Por lo cual se hace necesario el fortalecimiento de la protección asociada a las IFAS.

El modelo sugerido de buenas prácticas diseñado y documentado, toma componentes de los estándares objeto de análisis y adapta su contenido a los activos IFAS, lo que en consecuencia evidencia que es más práctico la construcción de un modelo tomando lo que se adopte o ajuste al ámbito financiero que si se implementara un estándar individualmente.

La aplicación de un ejercicio teórico del modelo permitió evidenciar que es posible ajustando y adaptando particularidades de los marcos lograr mejorar en nivel de madurez cibernética. Estos resultados prácticos indican que es posible mejorar y medir la postura de seguridad de las entidades financieras.

Los playbooks de respuesta desarrollados para escenarios en donde se vean comprometidos los activos IFAS propuesto para el ejercicio teórico evidenciaron que es posible llegar a reducir los

tiempos de respuesta y mitigación frente a incidentes críticos. En definitiva, es importante considerar las particularidades de los activos financieros críticos para lograr mejores tiempos de respuesta.

Se evidencio la necesidad de definir una taxonomía que permita clasificar los activos IFAS basada en la Tríada CIA ya que es más fácil su identificación y así como las medidas necesarias para garantizar su protección. Por lo que las entidades que permiten una clasificación e identificación de sus activos pueden llegar a implementar controles más granulares a cada activo de información.

El modelo desarrollado y la metodología de implementación propuesta representan una base consolidada de conocimiento en ciberseguridad enfocada en el ámbito financiero. El análisis de los marcos de referencia y su aplicación específicamente al contexto de los activos IFAS, establece una base metodológica que puede ser aplicado y ajustado a futuras investigaciones e implementaciones dentro del sector financiero.

Si bien los resultados obtenidos son prometedores en el marco teórico, es importante reconocer las limitaciones presentadas al no realizar la implementación practica de la metodología definida. Así como la implementación en un conjunto más amplio y diverso de instituciones financieras que pueden apoyar una línea de investigación futura necesaria para ajustar os resultados teóricos con los resultados prácticos que se puedan generar en la implementación.

En conclusión, esta investigación ha demostrado que un planteamiento estructurado, específicamente diseñado para la protección de activos de infraestructura financiera crítica IFAS, puede generar mejoras sustanciales en la postura de ciberseguridad de las entidades del sector. La incorporación de múltiples marcos de referencia, adaptados al contexto específico de los activos IFAS, lo que permite construir una metodología para abordar las complejidades y particularidades de la ciberseguridad en el ámbito financiero.

5 REFERENCIAS BIBLIOGRÁFICAS

Amazon.com. (11 de noviembre de 2023). *¿Qué es una aplicación web?* . Obtenido de aws.amazon.com: https://aws.amazon.com/es/what-is/web-application/

Auditool. (2025). *Nuevo modelo de evaluacion de controles* . Obtenido de https://www.auditool.org/blog/auditoria-interna/modelo-de-evaluacion-de-controles

Bander, J. (2018). Cybersecurity for the home and office: The lawyer's guide to taking charge of your own information security. En J. Bander, *Cybersecurity for the home and office: The lawyer's guide to taking charge of your own information security.* American Bar Association. Obtenido de American Bar Association.

Banrep. (septiembre de 2021). *Funciones y servicios del Banco de la República.* . Obtenido de https://www.banrep.gov.co/es/plan-estrategico_2017-2021/funciones-y-servicios

BSI. (2019). *Norma ISO 22301 Gestion de continuidad del negocio* . Obtenido de https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

Cisa.gov. (20 de Noviembre 2023 de 2023). *Cisa.gov.* Obtenido de Home Page: https://www.cisa.gov/

Cisa.gov. (junio de 2023). *Cybersecurity best practices.* Obtenido de Cybersecurity best practices: https://www.cisa.gov/topics/cybersecurity-best-practices

COBIT, I. (5 de octubre de 2019). *Cobit.* Obtenido de Isaca.org: https://www.isaca.org/resources/cobit

CRC. (2022). *CRCPreguntas frecuentes sobre el Regulador Único. Gov.co.* Obtenido de https://www.crcom.gov.co/sites/default/files/2021-12/funciones_CRC.pdf

CSRC. (2008). *SP 800-115, Technical Guide to Information Security Testing and Assessment* | . Obtenido de https://csrc.nist.gov/pubs/sp/800/115/final

CSRC. (s.f.). *SP 800-61 Rev. 2.* Obtenido de Computer Security Incident Handling Guide.

Departamento Administrativo de la FunciónPública. (2023). *funcionpublica.gov.co/.* Obtenido de funcionpublica.gov.co/: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=53646%20

DRI International. (s.f.). *Home | DRI International.* Obtenido de https://drii.org/

Energy, D. o. (s.f.). *Cybersecurity Capability Maturity Model (C2M2)* . Obtenido de https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2?nrg_redirect=321446

funcionpublica. (2023). *Decreto 2257 de 2017 - Gestor Normativo.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=84839

IBM. (5 de octubre de 2023). *¿Qué es la ciberseguridad? (s/f).* Obtenido de IBM: https://www.ibm.com/mx-es/topics/cybersecurity

IBM. (12 de julio de 2023). *Ejemplos de planes de contingencia empresarial: prepararse para lo inesperado | IBM.* Obtenido de https://www.ibm.com/mx-es/think/topics/contingency-plan-examples

Industrial mintset. (2025). *Analisis de riesgos de seguridad de procesos Guia paso a paso - .* Obtenido de https://industrialmindset.com/analisis-de-riesgos-en-seguridad-de-procesos-guia-paso-a-paso/

ISACA. (2025). *CMMI Cybermaturity Platform.* Obtenido de https://www.isaca.org/enterprise/cmmi-cybermaturity-platform

ISO/IEC. (Octubre de 2022). *ISO/IEC 27001:2022.* Obtenido de https://www.iso.org/standard/27001

ISO/IEC 27002:2022. (2022). *ISO/IEC 27002:2022 - Information security controls.* Obtenido de https://www.iso.org/standard/75652.html

ISO/IEC 27035. (2023). *ISO/IEC 27035-1:2023 - Information technology — Information security incident management — Part 1: Principles and process.* Obtenido de https://www.iso.org/standard/78973.html

ITware. (30 de Enero de 2023). *Ciberataques a la Nube, un problema en crecimiento*. Obtenido de ITware Latam: https://www.itwarelatam.com/2023/01/30/ciberataques-a-la-nube-un-problema-en-crecimiento/

Microsoft Defender for Endpoint, M. L. (2025). *Identificación de dispositivos accesibles desde Internet en Microsoft Defender para punto de conexión - .* Obtenido de https://learn.microsoft.com/es-es/defender-endpoint/internet-facing-devices

MinTic. (15 de marzo de 2016). *Guía para la Gestión y Clasificación de Activos de Información. Gov.co.* . Obtenido de MinTic: https://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINTIC. (2023). *Manual de Funciones del MinTIC - Manual de Funciones del MinTIC.* Obtenido de https://mintic.gov.co/portal/715/w3-article-135690.html

MINTIC. (2023). *Portal inicio.* Obtenido de https://www.mintic.gov.co/portal/inicio/

MITRE ATT&CK. (2025). *Guía completa de tácticas de ATT&CK: el marco MITRE.* Obtenido de https://www.startupdefense.io/es-us/blog/guia-completa-de-tacticas-de-att-ck-el-marco-mitre

National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems.* Obtenido de https://csrc.nist.gov/pubs/fips/199/final

NIST. (2013). *Cybersecurity Framework | NIST.* Obtenido de Cybersecurity Framework | NIST: https://www.nist.gov/cyberframework

NIST. (2021). *Firearm Examination: A NIST Scientific Foundation Review |.* Obtenido de https://www.nist.gov/spo/forensic-science-program/firearm-examination-nist-scientific-foundation-review

NIST SP 800-53. (2020). *National Institute Of Standar And Tecnology.* Obtenido de https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Norma ISO 22301 BSI. (2019). *Norma ISO 22301 Gestión de Continuidad de Negocio* . Obtenido de https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/

Rudra, A. (25 de septiembre de 2023). *Ciberseguridad en el sector bancario: Principales amenazas y prevención*. Obtenido de PowerDMARC: https://powerdmarc.com/es/cyber-security-in-banking/

Seguridad., R. I. (1 de Octubre de 2023). *Ciberseguridad, un desafío para las entidades financieras en América Latina* -. Obtenido de Revista Innovación Seguridad. (s/f): https://revistainnovacion.com/nota/11654/ciberseguridad_un_desafio_para_las_entidades_financieras_en_america_latina/

Senado de la Republica de Colombia. (2023). *Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [ESTATUTO_ORGANICO_SISTEMA_FINANCIERO]*. Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/estatuto_organico_sistema_financiero.html

SP 800-34, S. (s.f.). *SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC.* Obtenido de https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

Super financiera de colombia. (2014). *Super financiera de colombia Circular basica juridica.* Obtenido de https://vlex.com.co/vid/circular-basica-juridica-circular-672001405

Super intendencia Financiera de Colombia. (marzo de 2023). *Superintendencia Financiera de Colombia. Consumoteca Colombia.* Obtenido de Colombia. https://www.consumoteca.com.co/superintendencia-financiera-de-colombia/

Superintendencia Financiera de Colombia. (2014). *Circular Externa 029 de 2014.* Obtenido de https://vlex.com.co/vid/circular-basica-juridica-circular-672001405

Superintendencia Financiera de Colombia. (2023). *Fundacionmicrofinanzasbbva.org.* Obtenido de https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/wp-content/uploads/2018/05/Col-Cap%C3%ADtulo-V-Ciberseguridad.pdf

Superintendencia Financiera de Colombia. (oviembre de 2023). *superfinanciera.gov.co.* Obtenido de superfinanciera.gov.co: https://www.superfinanciera.gov.co/jsp/

Supertintendencia Financiera de Colombia. (2018). *Superfinanciera.gov.co.* Obtenido de https://www.superfinanciera.gov.co/publicaciones/10096745/normativanormativa-generalcirculares-externas-cartas-circulares-y-resoluciones-desde-el-ano-circulares-externascirculares-externas-10096745/

The Business Continuity Institute (BCI. (2025). *The Business Continuity Institute (BCI) | A global institute for business continuity and resilience | BCI.* Obtenido de https://www.thebci.org/

UnnOtec. (2025). *Analisis de vulnerabilidades: Tecnicas para proteger tu empresa.* Obtenido de Trasnformacion digital para empresasd : https://unnotec.com/blog/analisis-de-vulnerabilidades-tecnicas-para-proteger-tu-empresa/

Work, S. A. (2015). *Continuidad de Negocio: Análisis de Impacto sobre el Negocio: tiempos (II) - .* Obtenido de https://www.securityartwork.es/2012/06/22/continuidad-de-negocio-analisis-de-impacto-sobre-el-negocio-tiempos-ii/

Anexo 1 Estructura de la Encuesta

Desafíos en la Identificación y Clasificación de Activos Críticos en Entidades Financieras

Esta encuesta está dirigida a especialistas de entidades bancarias privadas de primer y segundo nivel, con el objetivo de identificar las principales dificultades y desafíos en el proceso de identificación y clasificación de activos críticos IFAS.

Sección 1: perfil del participante y contexto organizacional

1. Indique su rol principal en la organización:
    - ☐ Oficial de Seguridad de la Información
    - ☐ Gerente de Riesgos
    - ☐ Arquitecto de Soluciones
    - ☐ Líder de Infraestructura TI
    - ☐ Gerente de Proyectos TI
    - ☐ Otro
2. Nivel de experiencia en identificación de activos críticos:
    - ☐ Menos de 2 años
    - ☐ 2-5 años
    - ☐ 5-10 años
    - ☐ Más de 10 años
3. Metodología principal utilizada para identificación de activos:
    - ☐ NIST Framework
    - ☐ ISO 27001
    - ☐ COBIT
    - ☐ Metodología propia de la organización
    - ☐ Combinación de varias metodologías

Sección 2: desafíos en la identificación de activos

4. Seleccione los 3 principales obstáculos en la identificación de activos:
    - ☐ Falta de criterios claros de clasificación
    - ☐ Dificultad en obtención de información
    - ☐ Complejidad de interdependencias
    - ☐ Resistencia organizacional
    - ☐ Limitaciones de recursos
    - ☐ Herramientas inadecuadas
5. Principales desafíos al determinar criticidad (seleccione los 3 más importantes):
    - ☐ Falta de métricas de impacto
    - ☐ Dificultad en cuantificación de valor
    - ☐ Ausencia de criterios estándar
    - ☐ Conflictos entre áreas
    - ☐ Cambios frecuentes en requisitos
    - ☐ Complejidad de impactos indirectos
6. Frecuencia de desafíos en mapeo de dependencias (seleccione los más comunes):
    - ☐ Documentación desactualizada
    - ☐ Sistemas legacy
    - ☐ Dependencias indirectas
    - ☐ Cambios no documentados
    - ☐ Flujos de datos complejos
    - ☐ Servicios tercerizados

Sección 3: retos en la clasificación

7. Aspectos más desafiantes en clasificación (seleccione los 3 principales):
    - ☐ Valoración de activos
    - ☐ Establecimiento de niveles críticos
    - ☐ Evaluación de impactos
    - ☐ Cumplimiento regulatorio
    - ☐ Definición de controles
    - ☐ Mantenimiento de inventario
8. Frecuencia de actualización del inventario de activos:
    - ☐ Mensual
    - ☐ Trimestral
    - ☐ Semestral
    - ☐ Anual
    - ☐ Solo cuando hay cambios significativos

Sección 4: desafíos organizacionales

9. Principales obstáculos en colaboración interdepartamental:
    - ☐ Falta de compromiso
    - ☐ Comunicación deficiente
    - ☐ Conflictos de prioridades
    - ☐ Desconocimiento técnico
    - ☐ Limitaciones de tiempo
    - ☐ Procesos burocráticos
10. Nivel de apoyo de la alta dirección:
    - ☐ Muy alto - Participación activa

- Alto - Apoyo regular
- Medio - Apoyo ocasional
- Bajo - Poco interés
- Muy bajo - Sin apoyo

Sección 5: desafíos técnicos

11. Principales retos técnicos (seleccione los 3 más significativos):
    - Infraestructura compleja
    - Sistemas antiguos
    - Falta de documentación
    - Integraciones complejas
    - Cambios tecnológicos frecuentes
    - Herramientas inadecuadas
12. Desafíos en entornos híbridos:
    - Visibilidad limitada
    - Control de acceso
    - Sincronización de datos
    - Cumplimiento normativo
    - Gestión de identidades
    - Monitoreo completo

Sección 6: aspectos regulatorios

13. Principales desafíos regulatorios:
    - Requisitos cambiantes
    - Múltiples reguladores
    - Interpretación de normas

- Plazos de cumplimiento
- Costos de implementación
- Auditorías frecuentes

14. Frecuencia de cambios en requisitos regulatorios:
    - Mensual
    - Trimestral
    - Semestral
    - Anual
    - Variable según regulador

Sección 7: herramientas y recursos

15. Herramientas utilizadas actualmente:
    - Software especializado
    - Herramientas desarrolladas internamente
    - Hojas de cálculo
    - Sistemas de gestión documental
    - Herramientas de colaboración
    - Combinación de varias

16. Recursos necesarios más importantes:
    - Software especializado
    - Personal dedicado
    - Capacitación
    - Presupuesto
    - Tiempo
    - Apoyo gerencial

Sección 8: impacto en la gestión

17. Impacto de los desafíos en la gestión de riesgos:
    - ☐ Muy alto - Afecta críticamente
    - ☐ Alto - Impacto significativo
    - ☐ Medio - Impacto moderado
    - ☐ Bajo - Impacto menor
    - ☐ Muy bajo - Impacto mínimo
18. Frecuencia de incidentes por identificación inadecuada:
    - ☐ Muy frecuente (mensual)
    - ☐ Frecuente (trimestral)
    - ☐ Ocasional (semestral)
    - ☐ Raro (anual)
    - ☐ Muy raro (mayor a un año)

Sección 9: mejores prácticas

19. Estrategias más efectivas implementadas:
    - ☐ Automatización de procesos
    - ☐ Capacitación regular
    - ☐ Comités interdisciplinarios
    - ☐ Revisiones periódicas
    - ☐ Documentación detallada
    - ☐ Auditorías internas
20. Nivel de madurez del proceso:
    - ☐ Optimizado
    - ☐ Gestionado cuantitativamente

- Definido
- Gestionado
- Inicial

Metodología de Aplicación

- Formato: encuesta digital
- Tiempo estimado: 30 minutos
- Periodicidad: semestral
- Análisis: cuantitativo con indicadores de tendencia

Criterios de Participación

- Rol activo en gestión de activos
- Mínimo 2 años de experiencia
- Conocimiento de normativas financieras
- Participación en procesos de gestión de riesgos

Anexo 2 Resultados de la Encuesta: desafíos en la Identificación y Clasificación de Activos Críticos en Entidades Financieras (25 participantes)

- Sección 1: perfil del participante y contexto Organizacional
    - Pregunta 1: rol principal en la organización

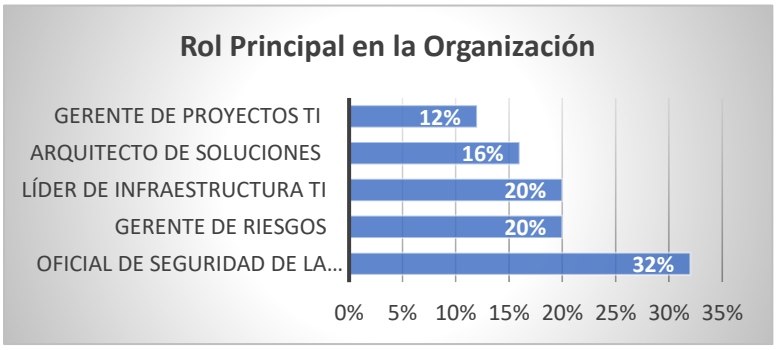


Ilustración N° 1 Pregunta 1

    - Pregunta 2: nivel de experiencia

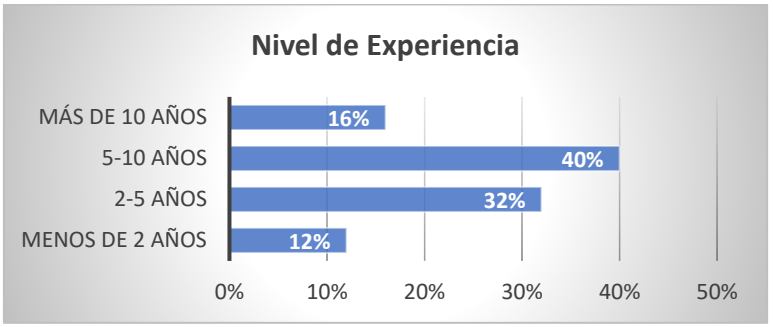


Ilustración N° 2 Pregunta 2

    - Pregunta 3: metodología principal.

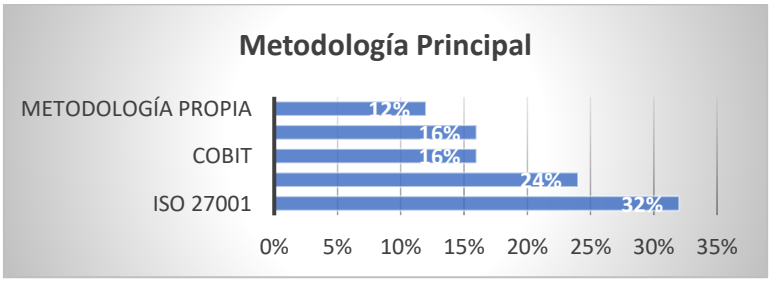


Ilustración N° 3 Pregunta 3

- Sección 2: desafíos en la Identificación de Activos, principales obstáculos.

  - Pregunta 4: seleccione los 3 principales obstáculos en la identificación de activos.

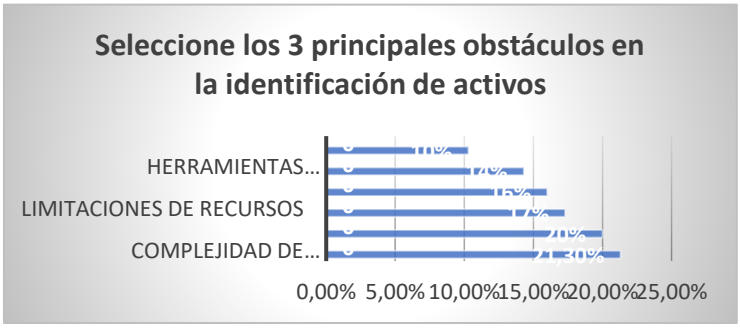


Ilustración N° 4 Pregunta 4

  - Pregunta 5: principales desafíos al determinar criticidad (seleccione los 3 más importantes).

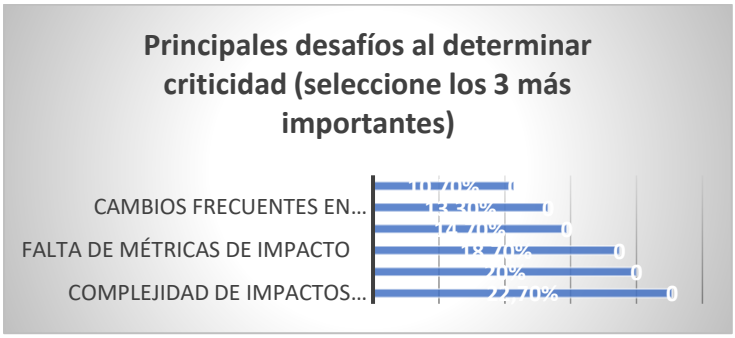


Ilustración N° 5 Pregunta 5

- Frecuencia de desafíos en mapeo de dependencias (seleccione los 3 más comunes)

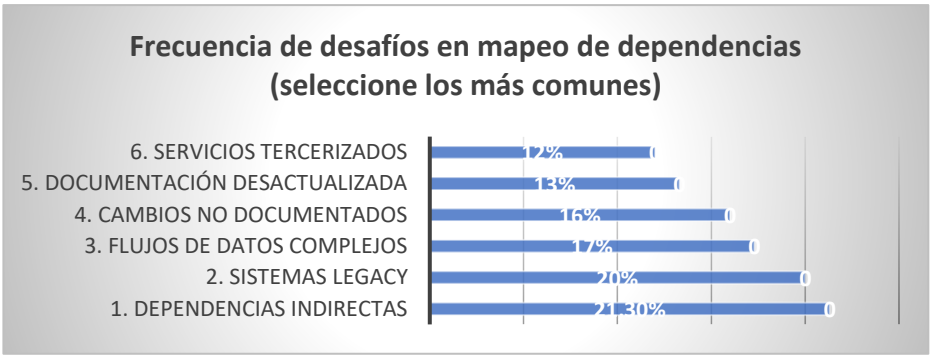


Ilustración N° 6 Pregunta 6

- Sección 3: retos en la clasificación

  - Pregunta 7: aspectos más desafiantes en la clasificación de activos (seleccione los 3 principales)

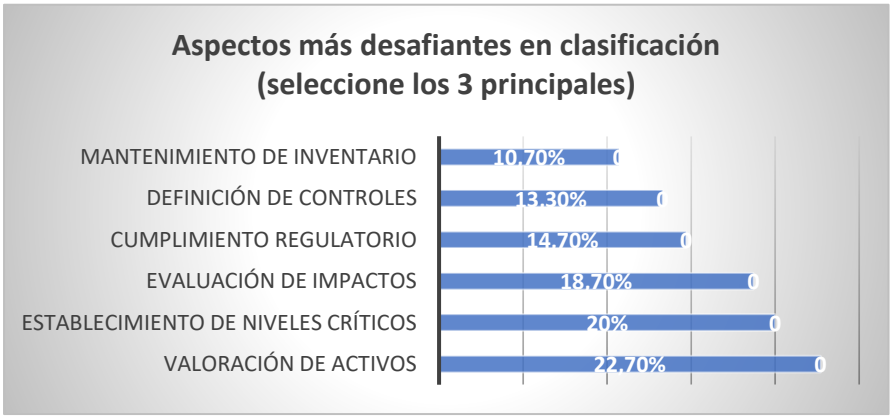


Ilustración N° 7 Pregunta 7

- Pregunta 8: frecuencia de Actualización del inventario de activos

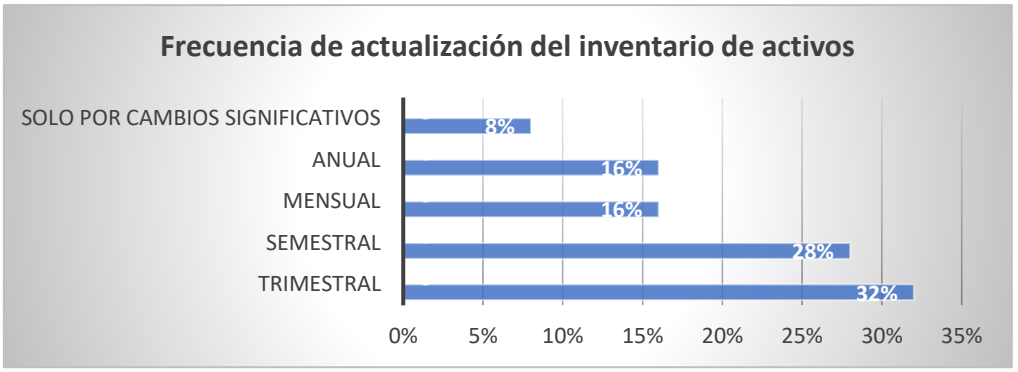


Ilustración N° 8 Pregunta 8

- Sección 4: desafíos organizacionales
  - Pregunta 9: principales obstáculos en colaboración interdepartamental

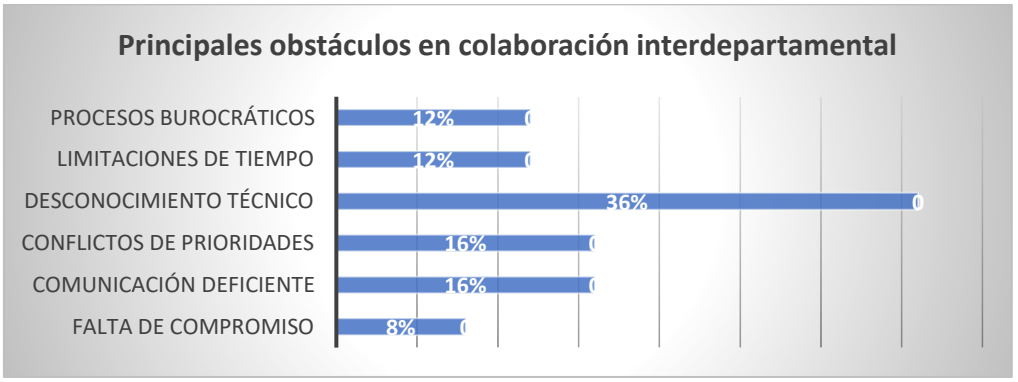


Ilustración N° 9 Pregunta 9

- Pregunta 10: nivel de apoyo de la alta dirección

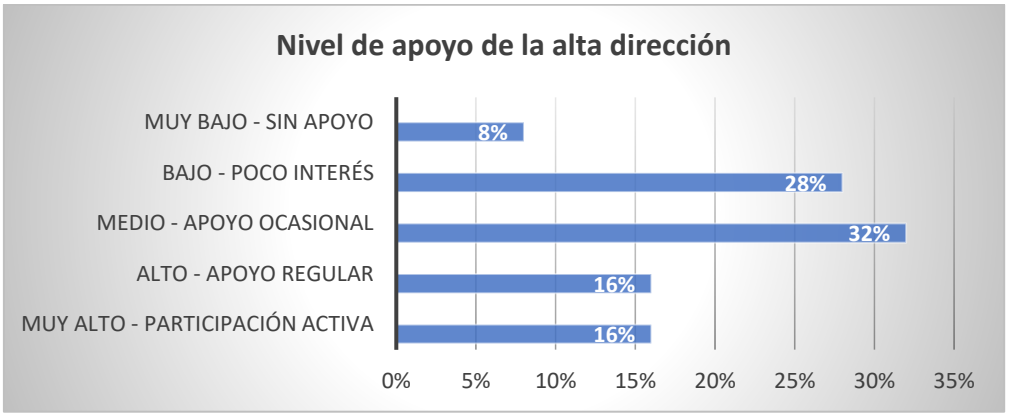


Ilustración N° 10 Pregunta 10

- Sección 5: tesafíos técnicos
  - Pregunta 11: principales retos técnicos (seleccione los 3 más significativos):

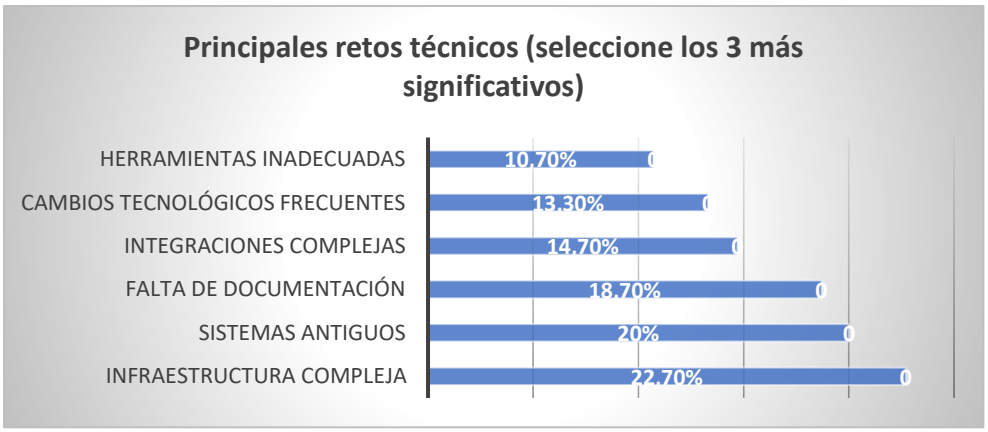


Ilustración N° 11Pregunta 11

- Pregunta 12: desafíos en entornos híbridos

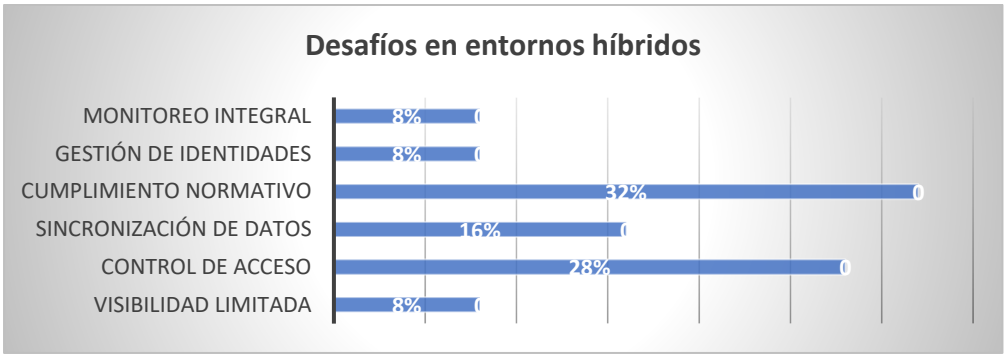


Ilustración N° 12 Pregunta 12

- Sección 6: aspectos regulatorios
  - Pregunta 13: principales desafíos regulatorios

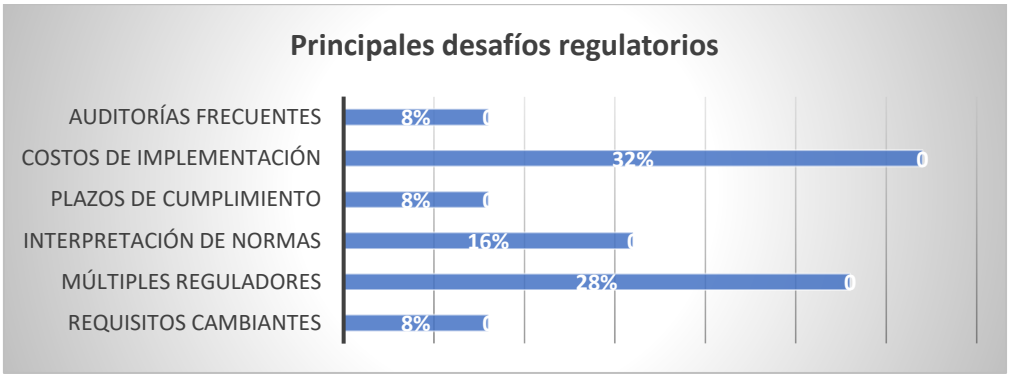


Ilustración N° 13 Pregunta 13

- Pregunta 14: frecuencia de cambios en requisitos regulatorios

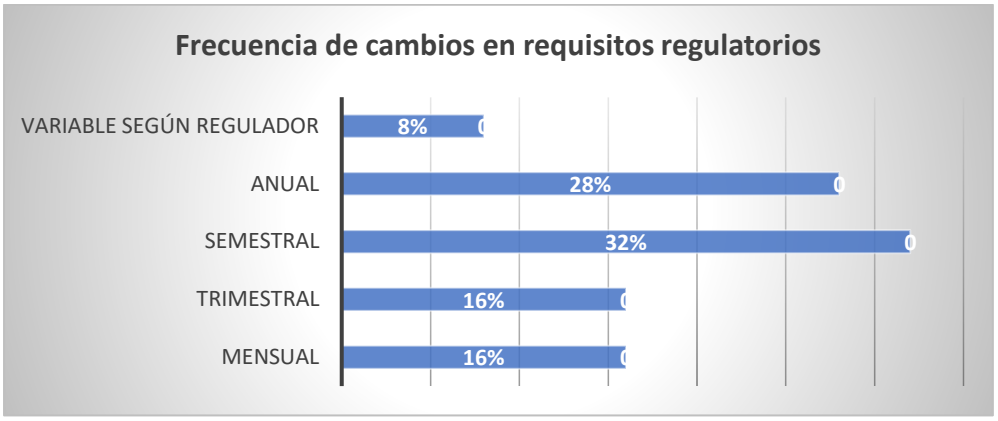


Ilustración N° 14 Pregunta 14

- Sección 7: herramientas y recursos
  - Pregunta 15: herramientas utilizadas actualmente

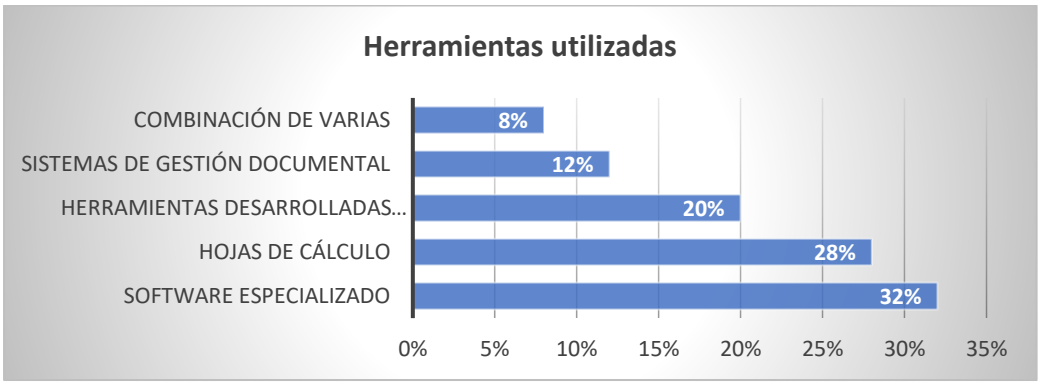


Ilustración N° 15 Pregunta 15

- Pregunta 16: recursos necesarios más importantes

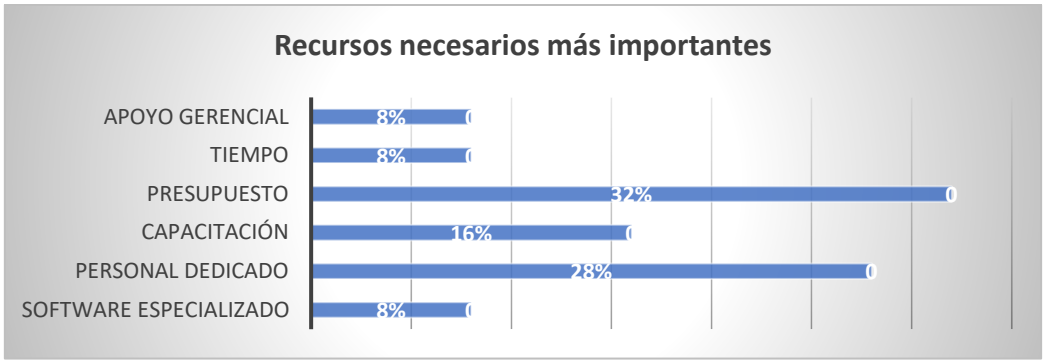


Ilustración N° 16 Pregunta 16

- Sección 8: impacto en la gestión
  - Pregunta 17: impacto de los desafíos en la gestión de riesgos:

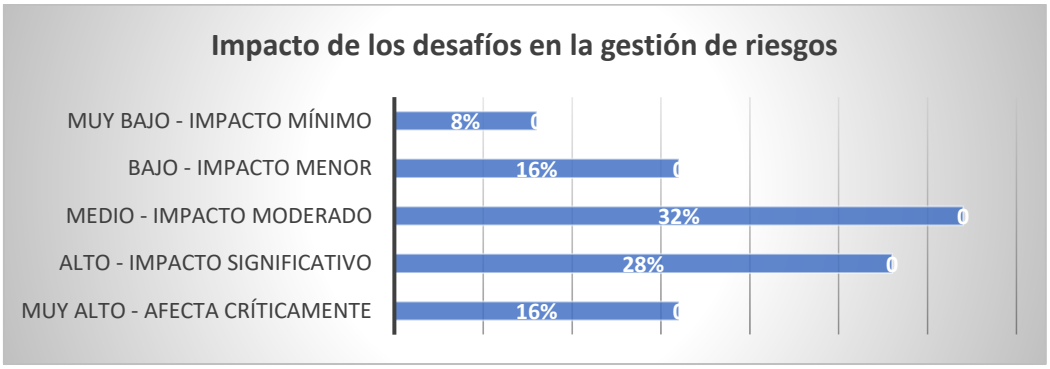


Ilustración N° 17 Pregunta 17

- Pregunta18: frecuencia de incidentes por identificación inadecuada

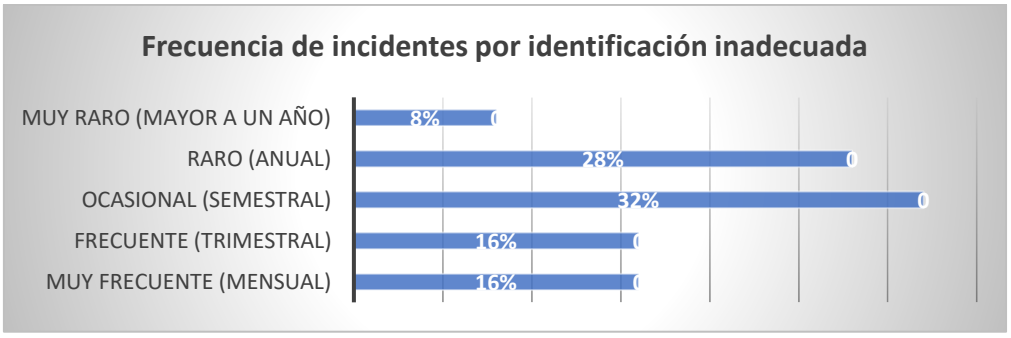


Ilustración N° 18 Pregunta 18

- Sección 9: mejores prácticas
  - Pregunta 19: estrategias más eficaces implementadas

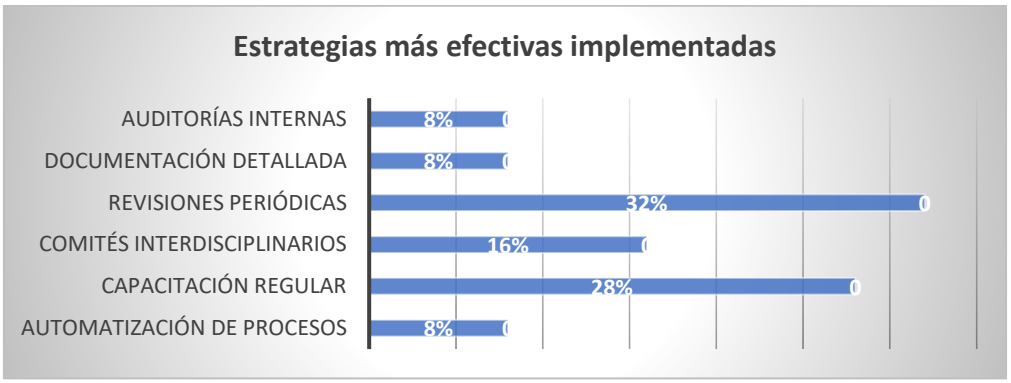
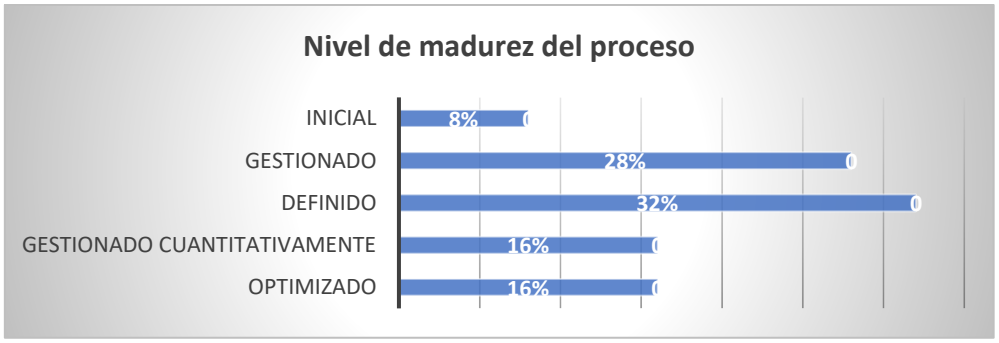


Ilustración N° 19 Pregunta 19

  - Pregunta 20: nivel de madurez del proceso:



Anexo 3: taller propuesto personal especializado de entidades bancarias

- **Información General**
  - **Duración:** aproximadamente 8 horas.
  - **Formato:** presencial o virtual con componentes prácticos.
  - **Audiencia:** equipos de seguridad, desarrollo, operaciones IT, infraestructura tecnológica.
  - **Prerrequisitos:** conocimientos básicos de seguridad informática.
  - **Material necesario:** computadoras con acceso a entornos de prueba, herramientas de seguridad.
- **Objetivos de Aprendizaje:**
  - Comprender los componentes del modelo de ciberseguridad y su aplicación práctica.
  - Implementar procesos de clasificación de activos según los criterios establecidos.
  - Aplicar los procedimientos de gestión de vulnerabilidades en sistemas críticos.
  - Utilizar las herramientas y metodologías de evaluación de seguridad en aplicaciones expuestas a internet.
  - Ejecutar los protocolos de respuesta a incidentes según los playbooks definidos.
- **Agenda del Taller**
  - **Módulo 1: fundamentos del modelo de ciberseguridad (1 hora)**
    - Introducción y contexto regulatorio para instituciones financieras
    - Arquitectura general del modelo de seguridad
    - Componentes críticos y sus interrelaciones
    - Marco de referencia y estándares aplicados (NIST CSF, ISO 27001, FFIEC)
    - Discusión: Desafíos específicos de la institución
  - **Módulo 2: identificación y clasificación de activos críticos (1.5 horas)**
    - Metodología de identificación de activos
    - Criterios de clasificación detallados
    - Ejercicio práctico: clasificación de activos reales de la organización
    - Herramientas para el inventario y gestión del ciclo de vida
    - Consideraciones especiales para Internet Facing Applications
    - Revisión y validación de clasificaciones
  - **Módulo 3: gestión de vulnerabilidades (2 horas)**

- Ciclo completo de gestión de vulnerabilidades
- Herramientas de escaneo y su configuración óptima
- Laboratorio práctico: Configuración y ejecución de escaneos
- Proceso de evaluación, priorización y remediación
- Ejercicio: Análisis de resultados de escaneo y determinación de acciones
- Métricas y KPIs para seguimiento
- Integración con CI/CD para aplicaciones

- **Módulo 4: protección de aplicaciones con exposición a internet (1.5 horas)**
  - Vectores de ataque específicos para aplicaciones expuestas
  - Arquitecturas seguras para aplicaciones financieras
  - Demostración: Implementación de WAF y configuración de reglas
  - Técnicas de Harding para servidores web y aplicaciones
  - Gestión segura de APIs
  - Caso práctico: Revisión de seguridad de una aplicación existente
- **Módulo 5: respuesta a incidentes (1.5 horas)**
  - Estructura y funciones del CSIRT
  - Flujos de trabajo durante un incidente
  - Simulación: Respuesta a un incidente simulado en tiempo real
  - Herramientas forenses y de análisis
  - Documentación y comunicación durante incidentes
  - Ejercicio: Desarrollo de un informe post-incidente
- **Módulo 6: implementación y adopción (30 minutos)**
  - Plan de implementación gradual
  - Estrategias para superar resistencia al cambio
  - Incorporación con procesos existentes
  - Medición de efectividad y ajustes
- **Metodología de Enseñanza**
  - Presentaciones conceptuales (30%)
  - Demostraciones prácticas (20%)
  - Ejercicios hands-on individuales y grupales (40%)
  - Discusiones y resolución de problemas (10%)

- **Evaluación y Seguimiento**
  - Evaluación previa: cuestionario de conocimientos al inicio
  - Evaluación durante el taller: observación de ejercicios prácticos
  - Evaluación posterior: cuestionario de conocimientos y encuesta de satisfacción
  - Seguimiento: sesión de refuerzo (2 horas) dos semanas después
- **Recursos Adicionales**
  - Manuales de referencia digitales
  - Acceso a plataforma de e-learning con videos instructivos
  - Comunidad interna para consultas post-taller
  - Plantillas y herramientas para implementación inmediata
- **Plan de Contingencia**
  - Versión grabada del taller disponible para personal ausente
  - Kit de autoestudio para participantes que no puedan completar el taller
  - Disponibilidad de instructores para consultas posteriores

Anexo 3 Ciclo de Mejora Continua (PDCA)

Ciclo de Mejora Continua (PDCA)		
Fase: planificar (PLAN)	**Evaluación Inicial de Madurez**	
	Actividades	• Conducir evaluación de línea base usando CMMI y NIST CSF • Documentar nivel actual por dominio • Identificar fortalezas y debilidades • Establecer prioridades basadas en riesgo
	Herramientas	• Herramienta de autoevaluación NIST CSF • Plataforma de madurez CMMI • Matriz personalizada para Internet Facing Applications
	Entregables	• Informe de madurez actual Mapa de calor de riesgo • Inventario de brechas priorizadas
	Definición de Objetivos	
	Actividades	• Establecer objetivos SMART por dominio • Definir nivel de madurez objetivo (a 12, 24 y 36 meses) • Alinear con objetivos estratégicos • Obtener aprobación de la dirección
	Metodología	• Workshops con stakeholders clave • Análisis de requisitos regulatorios • Benchmark con instituciones financieras similares
	Entregables	• Documento de objetivos de madurez • KPIs para cada dominio • Niveles objetivo en escala CMMI y NIST CSF
	Desarrollo de Roadmap	
	Actividades	• Identificar iniciativas necesarias • Estimar esfuerzo y recursos • Establecer dependencias • Desarrollar cronograma de implementación
	Consideraciones	• Prioridad basada en riesgo y complejidad • Capacidad organizacional • Restricciones presupuestarias • Requisitos regulatorios
	Entregables	• Roadmap de iniciativas a 36 meses • Plan detallado para primeros 12 meses • Presupuesto estimado • Matriz de dependencias
	Implementación de Iniciativas	
	Metodología	• Orientación ágil con sprints de 2-4 semanas • Entregables incrementales • Revisiones periódicas

Fase: hacer (DO)	Categorías de Iniciativas	• Gestión de cambios • Estructuración de políticas y procedimientos • Implementación de controles técnicos • Mejoras de procesos • Capacitación y concienciación • Adquisición e implementación de herramientas
	Estructuración	• Proyectos para iniciativas complejas • Actividades operativas para mejoras simples • Asignación clara de responsabilidades • Seguimiento formal de avance
	Gestión de Cambios	
	Principios	• Comunicación transparente • Participación de stakeholders • Gestión de resistencia • Refuerzo positivo
	Actividades	• Sesiones de sensibilización • Comunicaciones regulares • Formación específica • Programa de champions por área
	Herramientas	• Plan de comunicación • Matriz de impacto de cambios • Programa de incentivos • Mecanismos de feedback
	Desarrollo de Capacidades	
	Áreas de importancia	• Capacidades técnicas • Habilidades de gestión • Conocimiento regulatorio • Toma de decisiones basada en riesgo
	Métodos	• Formación formal (interna y externa) • Mentoring y coaching • Comunidades de práctica • Recursos de autoestudio
	Medición	• Evaluaciones pre/post capacitación • Aplicación práctica de conocimientos • Certificaciones obtenidas • Mejora en indicadores operativos
	Monitorización Continua	
	Indicadores Operativos	• Tiempo de resolución de vulnerabilidades • Cobertura de controles implementados • Efectividad de detección • Incidentes de seguridad • Desviaciones de configuración segura
	Indicadores de Madurez	• Avance hacia niveles objetivo • Mejora por dominio • Comparativa con línea base • Benchmark con industria

Fase: verificar (CHECK)	Metodología	• Recopilación automatizada cuando sea posible • Validación manual para controles complejos • Frecuencia ajustada al tipo de indicador • Visualización en dashboard
	Evaluaciones Periódicas	
	Tipos	• Evaluaciones trimestrales de progreso • Evaluación semestral de madurez • Auditorías internas anuales • Evaluaciones externas (cada 18-24 meses)
	Alcance	• Verificación de implementación • Efectividad de controles • Cumplimiento de políticas • Avance en madurez
	Técnicas	• Revisión documental • Entrevistas • Pruebas técnicas (pentesting, red team) • Verificación de configuraciones
	Análisis de Efectividad	
	Actividades	• Correlación entre iniciativas y métricas • Análisis de tendencias • Identificación de patrones • Evaluación de ROI
	Herramientas	• Análisis estadístico • Visualización de datos • Sistemas de GRC • Modelado predictivo
	Entregables	• Informes de efectividad • Análisis de desviaciones • Recomendaciones de ajuste • Validación de hipótesis
	Ajustes al Plan	
	Criterios para Ajustes	• Desviaciones significativas de objetivos • Cambios en el entorno de amenazas • Nuevos requisitos regulatorios • Lecciones aprendidas de incidentes • Retroalimentación de stakeholders
	Proceso	• Identificación de necesidades de ajuste • Evaluación de impacto • Aprobación por el Comité • Comunicación de cambios • Actualización de documentación
Fase: actuar (ACT)	Frecuencia	• Ajustes menores: mensual/trimestral • Revisión completa: anuas
	Documentación de Lecciones Aprendidas	
	Alcance	• Éxitos y fracasos • Obstáculos encontrados

	Mecanismos	• Soluciones de eficiencia • Prácticas recomendadas • Sesiones de retrospectiva • Repositorio de conocimiento • Comunidades de práctica • Estudios de caso internos
	Aplicación	• Incorporación en nuevas iniciativas • Actualización de metodologías • Refinamiento de estimaciones • Mejora de procesos
	Reconocimiento y Comunicación	
	Actividades	• Reconocimiento de logros • Comunicación de avances • Celebración de hitos • Compartir historias de éxito
	Audiencias	• Equipo del programa • Líderes y ejecutivos • Toda la organización • Reguladores (cuando aplique)
	Canales	• Comunicaciones internas • Reuniones ejecutivas • Eventos de reconocimiento • Informes formales
Gestión del Programa	**Integración con Otros Processos**	
	Procesos relacionados	• Gestión de proyectos • Gestión de cambios • Gestión de riesgos • Cumplimiento regulatorio • Desarrollo de aplicaciones • Operaciones de TI
	Mecanismos de integración	• Puntos de control comunes • Flujos de información compartidos • Métricas alineadas • Gobierno coordinado
Gestión de Riesgos del Programa	Categorías de riesgo	• Recursos insuficientes • Resistencia organizacional • Competencia con otras iniciativas • Cambios regulatorios • Eventos externos disruptivos
	Estrategia	• Identificación proactiva • Evaluación de impacto • Planes de mitigación • Monitorización continua • Escalamiento oportuno
Reporting	Informes regulares	• Dashboard mensual (operativo) • Informe trimestral (táctico)

Contenido típico	• Informe anual (estratégico) • Estado general del programa • Avance por iniciativa • Métricas clave • Riesgos y problemas • Próximos hitos • Decisiones requeridas
Distribución	• Comité de Mejora Continua • Comité de Riesgos • Directorio (informes ejecutivos) • Reguladores (cuando sea requerido)