Modelo de buenas prácticas en seguridad de la información para proveedores críticos en TI.

Patricia Leal Cáceres

Universidad Distrital Francisco José de Caldas

Maestría en gestión y seguridad de la información

MSc. Miguel Ángel Leguizamón Páez

Abril de 2026

TABLA DE CONTENIDO

Resumen 11

Abstract 12

1. INTRODUCCIÓN 13

1.1 Contextualización del tema 14

1.2 Problemática actual 15

1.3 El problema de investigación 20

1.4 Justificación 22

1.5 Objetivos 24

1.5.1 Objetivo general 24

1.5.2 Objetivos específicos 24

1.6 Alcances y limitaciones del modelo 25

1.7 Metodología 26

1.7.1 Fases del desarrollo metodológico 28

1.7.2 Técnicas e instrumentos de recolección. 29

2. ESTADO DEL ARTE 32

2.1 Contextualización de la seguridad de la información 32

2.2 Principales modelos teóricos y normativos orientados al factor humano en seguridad. 34

2.2.1 Modelo AET (concienciación, educación, formación). 35

2.2.2 Modelo de cumplimiento conductual (BC). 36

2.3 Cultura organizacional y seguridad de la información. 38

2.4 Modelos de madurez en gestión de seguridad de la información 39

2.4.1 Modelos generales de madurez (CMM, CMMI, C2M2). 39

2.4.2 Modelos específicos orientados a la cadena de suministro y terceros. 41

2.4.3 Implicaciones para la gestión de proveedores críticos. 45

2.5 Normativas y marcos internacionales relevantes. 46

2.5.1 ISO/IEC 27001, 27002 y NIST CSF. 46

2.6 Antecedentes de incidentes relevantes. 52

2.6.1 *Contexto sectorial de referencia* 53

2.7 Análisis de Caso de Estudio en la Literatura. 54

2.7.1 Importancia de la Comprensión de la Cadena de Ataque para la Defensa Cibernética. 55

La comprensión detallada del modelo de la cadena de ataque es fundamental para una defensa cibernética eficaz por varias razones cruciales: 55

2.7.2 El Rol del Factor Humano (Empleados y Proveedores) en Romper la Cadena de Ataque. 58

2.8 Brechas comunes y limitaciones identificadas en la literatura. 60

2.9 Arquitectura de Gestión de Riesgos 63

2.9.1 Arquitectura de Confianza Cero (Zero Trust Architecture - ZTA) 64

3. DISEÑO Y DESARROLLO DE LA INTEGRACIÓN DEL MODELO (AET+BC) PARA PROVEEDORES CRÍTICOS EN TI. 65

3.1. Introducción al modelo integrado (AET+BC) 65

3.1.1 Fundamentación del Modelo 66

3.2. Determinación de elementos críticos de los modelos (AET + BC). 68

3.3 Características para Proveedores Críticos. 70

3.4 Compromiso de Cultura y Seguridad Conductual (AET+BC) en Proveedores Críticos según estándares ISO/NIST. 71

3.4.1 Cláusula de Compromiso en Cultura de Seguridad y Gestión Conductual (Modelo AET+BC) 72

3.5 Principales causas de las desviaciones asociadas a las prácticas inseguras de los proveedores. 73

3.5.1 Inconsistencias y riesgos en la gestión de proveedores críticos. 75

3.6 Evaluación documental de prácticas actuales bajo estándares ISO/NIST. 77

3.6.1 Análisis de controles ISO 27002 y NIST 77

3.6.2 Evaluación cualitativa de efectividad. 78

3.6.3 Análisis conceptual del impacto potencial en la evaluación de proveedores. 80

3.6.4 Brechas identificadas en la relación con los proveedores. 81

3.7 Identificación de Riesgos y Priorización. 82

3.7.1 Matriz de riesgos identificados. 82

3.7.2 Análisis de priorización. 83

3.7.3 Matriz de calor de riesgos con estrategias de mitigación integradas. . 84

3.8 Arquitectura integrada del modelo (AET+BC). 90

3.8.1 Documentación del modelo propuesto. 92

3.8.2 Arquitectura conceptual del modelo 92

3.8.3 Sinergias identificadas en el modelo integrado. 96

3.8.4 Arquitectura Basada en Riesgos del modelo integrado (AET+BC). 97

3.8.5 Dominios y controles específicos del modelo (AET+BC) 101

3.9 Propuesta de marco de métricas e indicadores. 102

3.9.1 Diseño del sistema de métricas. 102

3.9.2 Sistema de Scoring o puntuación de Proveedores. 104

3.9.3 Mecanismo de Recategorización de Riesgo basado en Comportamiento. 105

3.10. Metodología de Calificación y Niveles de Cumplimiento (Score Integrado)..... 107

3.10.1. Algoritmo de Cálculo del ICSP 107

3.10.2. Definición de Niveles de Madurez del Proveedor 109

4. EVALUACIÓN E IMPACTO DE LA INTEGRACIÓN DE LOS MODELOS AET Y BC EN LA GESTIÓN DE RIESGOS DE LOS PROVEEDORES DE TI. 111

4.1 Dimensiones del impacto a evaluar..... 111

4.2 Componente de Verificación y Mejora Continua. 113

4.2.1 Programa de Auditoría Escalonado 113

4.2.2 Protocolo de Ejecución de Auditoría. 113

4.2.3 Gestión de No Conformidades 114

4.3 Análisis de Impacto y Simulación Financiera (Modelo AET+BC). 115

4.3.1 Simulación Cuantitativa Pre/Post AETBC 116

4.3.2 Coeficiente de correlación de Pearson en el modelo (AET+BC) en el enfoque DSR. 118

4.4 Análisis Costo-Beneficio del Modelo (MBP-SI-PC). 119

4.4.1 Beneficios cuantificables 120

4.5 Resultados. 121

4.6 Síntesis y hallazgos principales 126

4.6.1 Hallazgos Documentales 126

4.6.2 Limitaciones del análisis 127

4.6.3 Valor del Análisis Realizado 128

CONCLUSIONES 130

REFERENCIAS 133

ANEXOS 146

Lista de Tablas

Tabla 1. Estadísticas relevantes sobre incidentes de seguridad cibernética con foco en Colombia versus Latinoamérica en 2024-2026. ..... *16*

Tabla 2. Comparación con Modelos Existentes (CMMI y C2M2). *45*

Tabla 3. Comparativa entre los estándares ISO27002 Y NIST CSF. *46*

Tabla 4. Comparativa de Controles ISO/IEC 27002:2022 vs NIST CSF *48*

Tabla 5. Correspondencia entre ISO/IEC 27002:2022, NIST CSF 2.0 y NIST SP 800-53 con enfoque en proveedores críticos *50*

Tabla 6. Estadísticas sectoriales de Colombia y Latinoamérica (2024). *53*

Tabla 7. Mapeo de Elementos Críticos de los Modelos AET y BC *68*

Tabla 8. Características y controles por tipo de proveedor. *70*

Tabla 9. Características que definen a un proveedor como 'crítico'. *71*

Tabla 10. Discrepancias o desviaciones en la cultura de seguridad de la información. *73*

Tabla 11. Riesgos e impactos en la gestión de proveedores en entornos de TI. *75*

Tabla 12. Mapeo de controles y medidas mitigantes. *78*

Tabla 13. Niveles de madurez integrados (ISO 27001 / NIST CSF / Modelo AET+BC) para la evaluación de proveedores críticos según el nivel de madurez. *79*

Tabla 14. Impactos conceptuales en la evaluación de proveedores. *81*

Tabla 15. Matriz de evaluación y priorización de riesgos. *82*

Tabla 16. Matriz de calor de riesgos con estrategias de mitigación (AET+BC). *84*

Tabla 17. Arquitectura integrada del modelo (AET+BC) para proveedores críticos. *90*

Tabla 18. Dominios Integrados: (AET+BC) vs. ISO 27001 vs. NIST CSF *101*

Tabla 19. Propuesta de Indicadores Estratégicos. *102*

Tabla 20. Indicadores estratégicos (C-Level). *103*

Tabla 21. Propuesta de indicadores tácticos. *103*

Tabla 22. Indicadores tácticos (Management). *103*

Tabla 23. Indicadores operativos. *104*

Tabla 24. Modelo de puntuación multidimensional: 104

Tabla 25. Re-categorización de desempeño de proveedores....106

Tabla 26. Matriz de correlación entre los niveles de capacitación (X) y el cumplimiento de políticas de seguridad (Y) 108

Tabla 27. Niveles de madurez de proveedores críticos. 109

Tabla 28. Dimensiones del impacto a evaluar. 111

Tabla 29. Matriz de escalamiento....115

Tabla 30. Simulación cuantitativa Pre/Post (AETBC). 116

Tabla 31. Simulación de KPIs (de Tablas 19-21 y Anexo 3). 117

Tabla 32. Trazabilidad de indicadores y madurez del modelo. 118

Tabla 34. Costos de Implementación USD (Año 1):....119

Tabla 35. Beneficios directos y ahorros proyectados anuales por tamaño de organización (USD). 120

Tabla 36. Métricas 125

Lista de Figuras

Figura 1. Intentos de ciberataque en Colombia vs. Latinoamérica (2024-2026). 17

Figura 2. Tipos de estudios incluidos en una revisión sistemática mixta. 27

Figura 3. Investigación mediante ciclos de relevancia, rigor y diseño. 28

Figura 4. Modelo AET (concienciación, educación, formación). 35

Figura 5. Modelo behavior compliance (BC) con ciclo de monitoreo, alimentación, refuerzo y mejora continua. 37

Figura 6. Cadena de ataque para la defensa cibernética de Lockheed Martin (LM-CIRT) en 2009. 56

Figura 7. Mapa de calor de riesgos con estrategias de mitigación (AET+BC). 86

Figura 8. Interpretación de la matriz de calor. 87

Figura 9. Modelo Conceptual de buenas prácticas para Proveedores Críticos (MBP-SI-PC). 92

Figura 10. Arquitectura de Seguridad desde las Dimensiones del modelo. 100

Figura 11. Flujo de Gestión de No Conformidades. 114

Lista de Anexos

Tabla Anexos 1. Encuesta de percepción frente a la seguridad de la información. 146

Tabla Anexo 2 Plantilla básica de auditoría de cumplimiento conductual (BC). 148

Tabla Anexo 3. Matriz de evaluación de indicadores PRE y POST con acciones de mejora. 149

Tabla Anexo 4 Matriz de Seguimiento, tablero y hoja de ruta por Proveedor. 151

Tabla Anexos 5 Hoja de Ruta para la Evolución del Modelo.....153

RESUMEN

En la era digital actual, la seguridad de la información se ha consolidado como un pilar fundamental para la resiliencia y la continuidad operativa de las organizaciones. Se requiere establecer cómo avalar que los proveedores de TI que gestionan funciones críticas cumplan con los estándares de seguridad y fomenten una cultura de seguridad de la información en la organización. El objetivo es proponer un modelo de buenas prácticas de seguridad de la información en un marco de gestión de riesgos integral para los proveedores en funciones críticas, en áreas de TI a partir de los modelos Awareness, Education and Training Model (AET) y Behavior Compliance Model (BC). El enfoque fue mixto. El diseño fue de tipo no experimental y de corte transversal. El proyecto se guio por los principios de la Investigación Basada en Diseño (Design Science Research - DSR). Como técnica e instrumentos, se utilizaron fichas de registro bibliográfico para organizar la información clave, además, se emplearon matrices de análisis comparativo para contrastar los elementos de los modelos AET y BC, así como los controles de los estándares NIST e ISO 27001/27002. La exploración confirmó que la principal vulnerabilidad en la gestión de proveedores críticos de TI no reside únicamente en los controles técnicos, sino en las brechas culturales que dificultan la traducción de la conciencia en prácticas sostenibles. El modelo (AET+BC) permite abordar estas brechas mediante programas estructurados de concienciación, educación y cumplimiento conductual.

Palabras clave: Seguridad de la información, proveedores críticos, cultura de seguridad, concientización, comportamiento de cumplimiento, modelo de seguridad de la información.

ABSTRACT

In the current digital landscape, information security has emerged as a critical pillar for organizational resilience and operational continuity. This research addresses the challenge of ensuring that third-party IT providers managing critical functions comply with established security standards while fostering an organizational security culture. The primary objective is to propose a comprehensive information security best-practice model within an integrated risk management framework for critical IT providers. This model is built upon the synthesis of the Awareness, Education, and Training (AET) and the Behavior Compliance (BC) models.

Adopting a mixed-methods approach, the study utilized a non-experimental, cross-sectional design guided by the principles of Design Science Research (DSR). Data collection and analysis involved bibliographic record sheets and comparative analysis matrices to contrast the components of the AET and BC models against the control frameworks of NIST and ISO/IEC 27001/27002. The findings confirm that the predominant vulnerability in critical IT vendor management is not limited to technical controls; rather, it lies in the cultural gaps that hinder the translation of security awareness into sustainable practices. The resulting integrated model (AET+BC) provides a structured path to bridge these gaps through systematic awareness, education, and behavioral compliance programs.

Keywords*:* Information Security, Critical Vendors, Security Culture, Awareness, Compliance Behavior, Information Security Model.

1. INTRODUCCIÓN

La gestión de la seguridad de la información ha evolucionado significativamente en las últimas décadas, impulsada por la digitalización, la interconectividad global y la creciente sofisticación de las amenazas cibernéticas. Sin embargo, a pesar del avance en tecnologías de protección y marcos normativos, los incidentes de seguridad continúan evidenciando que la efectividad de los controles no depende únicamente de su diseño técnico, sino del comportamiento de las personas que los operan y cumplen.

En muchas organizaciones persiste una brecha entre la cultura de seguridad declarada y las prácticas reales que se ejecutan en el día a día. Esta discrepancia se acentúa cuando las funciones críticas de TI son delegadas a proveedores externos, quienes acceden a información sensible, infraestructuras estratégicas y procesos esenciales para la continuidad del negocio. En este escenario, los proveedores dejan de ser actores periféricos y se convierten en extensiones operativas de la organización, compartiendo tanto capacidades como riesgos.

La experiencia reciente en Colombia y en el contexto latinoamericano ha puesto de manifiesto que una proporción significativa de los incidentes de seguridad se origina en terceros, y que el factor humano continúa siendo uno de los principales catalizadores de estos eventos. El énfasis exclusivo en controles técnicos o en el cumplimiento documental de estándares resulta insuficiente cuando no se acompaña de mecanismos que promuevan una comprensión real de los riesgos y comportamientos consistentes de cumplimiento.

Frente a este panorama, se plantea la necesidad de un modelo que permita evaluar y fortalecer la cultura de seguridad en la relación con proveedores críticos de TI. Este trabajo propone un enfoque integrado que articula concienciación, educación, capacitación y cumplimiento conductual, alineado con estándares internacionales como ISO/IEC 27001, ISO/IEC 27002 y el NIST Cybersecurity Framework, con el objetivo de reducir las brechas entre conocimiento, intención y acción en materia de seguridad de la información.

1.1 Contextualización del tema

En el entorno empresarial actual, la dependencia de proveedores externos de Tecnologías de la Información (TI) para la gestión de funciones críticas se ha consolidado como una estrategia operativa fundamental para organizaciones en Colombia y a nivel global. Esta tendencia responde a la necesidad de optimizar costos, acceder a profesionales especializados y agilizar procesos, pero también introduce nuevos y complejos desafíos en la seguridad de la información (Grupo ASD, 2025)

Organizaciones de todos los tamaños y sectores enfrentan un panorama de amenazas cibernéticas en constante evolución, que incluyen ataques sofisticados, vulnerabilidades internas y errores humanos. En Colombia, incidentes recientes como el ciberataque masivo a IFX Networks en 2023 evidencian la vulnerabilidad de la infraestructura digital nacional y la urgencia de fortalecer la seguridad informática para garantizar la continuidad operativa y proteger la confianza de los usuarios (Grupo ASD, 2025).

La externalización y colaboración con proveedores críticos de TI implica que estos actores tengan acceso a sistemas, datos y procesos sensibles, convirtiéndolos en potenciales vectores de riesgo que pueden ser explotados por actores maliciosos o causar incidentes no intencionales (Impacto TIC, 2025). Por ello, la gestión eficaz de la seguridad en este contexto requiere un enfoque holístico que trascienda la implementación de controles técnicos y políticas aisladas, incorporando la cultura de seguridad organizacional como un elemento clave para la prevención y mitigación de riesgos (PwC Colombia, 2023).

Una cultura de seguridad sólida promueve la conciencia, educación, entrenamiento continuo y un comportamiento proactivo de cumplimiento entre todos los miembros de la organización, incluyendo a los proveedores. Sin embargo, muchas organizaciones aún enfrentan dificultades para traducir la conciencia en prácticas sostenibles, debido a diferencias

culturales, niveles de madurez en seguridad y falta de mecanismos adecuados de alineación y supervisión (Impacto TIC, 2025).

En este sentido, la necesidad de un modelo de buenas prácticas que integre la cultura de seguridad como pilar fundamental para la gestión de la seguridad de la información con proveedores críticos de TI es apremiante. Este modelo debe fomentar la concienciación, educación, entrenamiento y promover comportamientos de cumplimiento consistentes, tanto dentro de la organización como en sus relaciones con aliados estratégicos (Minciencias, 2025).

El presente proyecto propone un modelo que combina el enfoque Awareness, Education and Training (AET) Model con orientación en el Behavior and Compliance (BC) Model, adaptado al contexto de proveedores críticos de TI. Se espera que esta propuesta contribuya a una comprensión más profunda de los desafíos culturales en la seguridad de la información y ofrezca una guía práctica para fortalecer la postura de seguridad organizacional mediante la gestión de la cultura en las relaciones con proveedores estratégicos.

1.2 Problemática actual

En el escenario actual, la gestión de la seguridad de la información enfrenta desafíos crecientes derivados de la evolución constante de las amenazas cibernéticas, la digitalización acelerada y la complejidad creciente de las cadenas de suministro, especialmente en el ámbito de los proveedores críticos de Tecnologías de la Información (TI). Esta realidad ha generado una brecha significativa entre la intención declarada de las organizaciones respecto a su cultura de seguridad y las prácticas efectivas que se llevan a cabo en el día a día, tanto internamente como en la interacción con sus socios externos. Una de las problemáticas más destacadas es la alta ocurrencia de incidentes de seguridad originados en proveedores críticos.

Tabla 1.

Estadísticas relevantes sobre incidentes de seguridad cibernética con foco en Colombia versus Latinoamérica en 2024-2026.

Indicador	Colombia (2024)	Latinoamérica (2024)	Colombia/LatAm (2026)	Fuente
Intentos de ciberataques reportados	+36,000 millones	Aprox. 215,000 millones	42,000M proyectado anual (Colombia 4° LatAm); top 5 malware: Perú, México, ARG, BR, CO	CCN-CERT/ENISA/ACSI; Minciencias PESI 2025; Fortinet 2026
% de incidentes regionales que afectan Colombia	17%	—	20-22% (top 4 malware LatAm)	CCN-CERT; Infobae/Kaspersky 2026; Minciencias PESI 2025
Sectores más afectados	Salud, educación, gobierno	Salud, financiero, gobierno	Salud, gobierno, finanzas, TI/proveedores críticos (ransomware IA +85%)	CCN-CERT/ENISA; Fortinet/TecnoSeguro 2026;
Proporción de incidentes por terceros	54% - 65% de organizaciones afectadas por fallos en proveedores	51% promedio regional	62-65% (cadena suministro TI crítica)	SecureFrame/ENISA; Global Outlook 2026
% de incidentes asociados al factor humano	74–95%	74–95% (tendencia similar)	70% (phishing IA +42%, errores configuración)	SoSafe/UOC/Verizon; Top Stats 2025/26; NIST CSF 2.0 2025
Principales vectores de ataque	Robo de credenciales, phishing, ransomware, explotación de vulnerabilidades, ingeniería social	Phishing, malware, ransomware, explotación de vulnerabilidades, ataques a cadena de suministro	Ransomware IA +89%, phishing sofisticado, supply chain TI	ENISA/CCN-CERT; Fortinet 2026;Minciencias PESI 2025

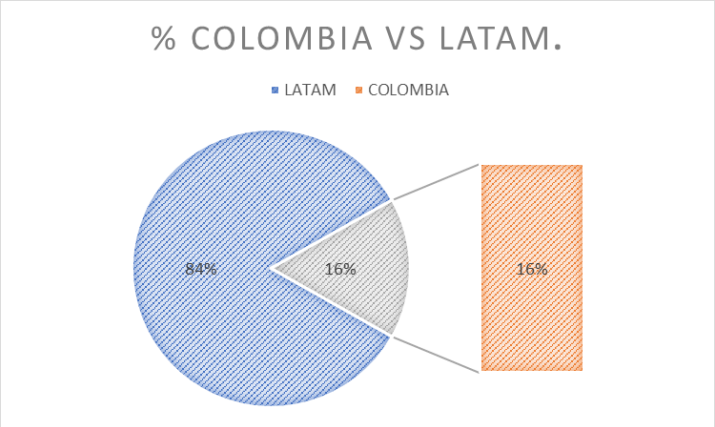
Indicador	Colombia (2024)	Latinoamérica (2024)	Colombia/LatAm (2026)	Fuente
Aumento de ciberataques vs. año anterior	30%	+28% promedio regional	+32-38% (IA sofisticación, proveedores TI)	ENISA; ACIS/Fortinet 2026;Minciencias PESI 2025

Nota: elaboración con base en (ACIS, 2025); (CCN-CERT Colombia, 2024); (ENISA, 2025); (FORTINET, 2025); (Fortinet, 2026); (Minciencias, 2025); (NIST CSF 2.0, Febrero 26, 2024).

Como se evidencia en la Tabla 1, Colombia registra 36B intentos de ciberataques (4° LatAm) con 54-65% de incidentes originados en terceros/proveedores críticos y 74-95% asociados al factor humano (Minciencias, 2025); (NIST CSF 2.0, 2024). La proyección 2026 (+32-38%, ransomware IA +89%) confirma la urgencia de modelos híbridos AETBC para mitigar las brechas culturales en las cadenas de suministro de TI (ENISA, 2025).En el contexto latinoamericano y colombiano en particular, esta situación implica no solo pérdidas económicas significativas, sino también impactos reputacionales difíciles de recuperar.

Figura 1.

Intentos de ciberataque en Colombia vs. Latinoamérica (2024-2026).



Nota: Colombia el cuarto país con más ciberataques en América Latina: 36.000 millones de intentos en 2024. **(ACIS, 2025)**; **(Minciencias, 2025)**.

Colombia se destaca como uno de los países con mayor volumen de intentos de ciberataque en la región y fuerte incidencia en el sector salud y gobierno, como se puede observar en la **Fig. 1.** La proporción de incidentes vinculados al factor humano es alta en toda América Latina y supera el 74% en la mayoría de los estudios. Tanto a nivel local como regional, los incidentes relacionados con terceros/proveedores críticos representan más de la mitad de los casos reportados. El crecimiento de los ataques y su sofisticación se consideran tendencia convergente en Colombia y Latinoamérica.

A nivel organizacional, esta problemática se profundiza por la evidente discrepancia entre la cultura de seguridad declarada y las conductas reales de empleados y proveedores. Muchas políticas y procedimientos estrictos existen formalmente, pero su adopción y cumplimiento efectivo presentan deficiencias atribuibles a la falta de capacitación especializada, incongruencias culturales y ausencia de mecanismos adecuados de supervisión y retroalimentación (Von Solms & Von Solms, 2004).

Además, la externalización y dependencia crítica de proveedores de TI aumentan los vectores de riesgo y dificultan la supervisión directa, dada la heterogeneidad en los niveles de madurez en seguridad de estos actores externos. La insuficiente alineación cultural y de procesos puede traducirse en brechas de seguridad que comprometen la confidencialidad, integridad y disponibilidad de la información, por ende, la continuidad de las operaciones organizacionales.

La materialización de incidentes de seguridad en proveedores puede tener consecuencias severas en múltiples dimensiones:

- **Reputacional**: El daño a la imagen institucional por asociación con proveedores inseguros o negligentes puede erosionar la confianza de clientes y socios estratégicos, afectando la competitividad de la organización.

- **Legal y regulatorio:** El incumplimiento de las normativas vigentes puede derivar en sanciones, litigios y responsabilidad compartida, que implican costos financieros y limitan la capacidad operativa.
- **Operativa:** La interrupción de servicios críticos afecta la continuidad del negocio, con impacto directo en la productividad y el cumplimiento de compromisos contractuales.

Frente a esta problemática, se hace evidente la necesidad de implementar un enfoque integral que trascienda los controles técnicos e incluya la transformación cultural, la capacitación continua y la evaluación del cumplimiento conductual tanto en la organización como en sus proveedores críticos. La adopción de modelos integradores, que contemplan la concienciación, educación, entrenamiento (AET) y el cumplimiento conductual (BC), se presenta como una vía efectiva para cerrar la brecha entre intención y práctica, fortaleciendo así la postura de seguridad y mitigando los riesgos estructurales presentes en la cadena de suministro digital.

En síntesis, la gestión actual de la seguridad de la información enfrenta un escenario altamente complejo, caracterizado por la sofisticación creciente de las amenazas cibernéticas, la acelerada digitalización y la vulnerabilidad estructural de las cadenas de suministro, especialmente en relación con proveedores críticos de Tecnologías de la Información (TI). Esta situación ha evidenciado una brecha significativa entre la cultura de seguridad declarada por las organizaciones y las prácticas efectivas implementadas, tanto a nivel interno como en la interacción con actores externos. En este contexto, se vuelve imperativo adoptar un enfoque integral, fundamentado en evidencia práctica y alineado con estándares internacionales, que articule estratégicamente la cultura organizacional, el capital humano, los procesos y las tecnologías. Tal articulación debe orientarse a fortalecer la resiliencia institucional, mitigar los riesgos derivados de terceros y garantizar la protección efectiva de los activos de información frente a un entorno de amenazas dinámicas y en constante evolución.

1.3 El problema de investigación

Para dimensionar la magnitud de este desafío, es imperativo analizar la situación estadística actual, donde la convergencia entre la sofisticación técnica y la vulnerabilidad humana que posiciona a Colombia en un escenario crítico dentro de la región, se caracteriza por la creciente digitalización de los procesos organizacionales, las entidades en Colombia, al igual que en el ámbito global, han incrementado su dependencia de proveedores de Tecnologías de la Información (TI) para la gestión de funciones críticas. Esta tendencia ha permitido optimizar recursos, mejorar la eficiencia operativa y acceder a niveles más altos de especialización. No obstante, dicha interdependencia también ha generado nuevos desafíos, especialmente en lo que respecta a la seguridad de la información. La delegación de funciones sensibles a terceros implica riesgos que, si no son gestionados adecuadamente, pueden comprometer la confidencialidad, integridad y disponibilidad de los activos informáticos de la organización. En este sentido, surge la necesidad de abordar una problemática central: ¿cómo evaluar que los proveedores de TI que administran funciones críticas cumplan con los estándares de seguridad establecidos y, al mismo tiempo, fomenten una cultura organizacional orientada a la protección de la información? Esta pregunta guía el presente proyecto y responde a una preocupación creciente en el entorno digital contemporáneo, donde la seguridad de la información se ha convertido en un pilar fundamental para la sostenibilidad y la confianza de las organizaciones.

La capacidad de las organizaciones para garantizar la seguridad de sus activos informacionales y la continuidad de sus operaciones está intrínsecamente ligada a la postura de seguridad de sus proveedores críticos. Las desviaciones en el cumplimiento de estándares y la ausencia de una cultura de seguridad alineada representan vulnerabilidades latentes con consecuencias potencialmente graves (LatinPyme, 2024).

Esta complejidad se agrava por la creciente sofisticación de las amenazas cibernéticas y la expansión de las cadenas de suministro digitales, que aumentan la exposición a riesgos. La inteligencia artificial también está siendo usada para potenciar ataques, lo que incrementa la complejidad del panorama (IBM, 2024).

El factor humano continúa siendo el principal eslabón débil, involucrado en el 74% de las infracciones de seguridad (Cano, 2023); (Forbes, 2023). Colombia, como foco de estos incidentes en Latinoamérica, enfrenta pérdidas financieras millonarias y daños reputacionales significativos (LatinPyme, 2024).

Aunque existen marcos para la gestión de riesgos de terceros, la literatura carece de modelos integrales que aborden cómo fomentar y medir una cultura de seguridad compartida entre la organización y sus proveedores críticos; a la fecha no existen modelos que integren lo humano (**AET**) con lo conductual (**BC**) específicamente para proveedores, considerando las diferencias culturales y la relación particular con estos actores. Este vacío dificulta la promoción de un comportamiento de cumplimiento sostenible y alineado con la cultura organizacional, más allá del cumplimiento técnico.

El proponer un modelo de buenas prácticas que integre los principios de los modelos Awareness, Education and Training (AET) y Behavior and Compliance (BC) ofrecerá una herramienta práctica y adaptable para fortalecer la relación con proveedores críticos desde una perspectiva cultural. La definición de métricas clave facilitará medir el desempeño en seguridad y monitorear el progreso, apoyando la toma de decisiones y la mejora continua.

Finalmente, abordar las vulnerabilidades en la cadena de suministro digital contribuirá a mejorar la resiliencia organizacional, protegiendo sus activos más valiosos: la información y la reputación. La materialización de incidentes de seguridad en proveedores críticos puede acarrear consecuencias graves en varios ámbitos:

Financiero: Costos directos de contención, recuperación, multas y sanciones regulatorias.

Operacional: Interrupciones en servicios esenciales, pérdida de productividad y retrasos en procesos críticos.

Reputacional: Daño a la imagen institucional por asociación con proveedores inseguros o negligentes.

Legal y regulatorio: Sanciones por incumplimiento normativo, responsabilidades compartidas y litigios (LatinPyme, 2024); (PwC Colombia, 2023).

Pregunta de Investigación. ¿Cómo evaluar que los proveedores de TI que manejan funciones críticas cumplan con los estándares de seguridad y fomenten una cultura de seguridad de la información en la organización?

1.4 Justificación

La creciente dependencia de las organizaciones, tanto en Colombia como a nivel global, de proveedores críticos de Tecnologías de la Información (TI) ha generado retos significativos en la gestión de la seguridad de la información. La cadena de suministro digital se ha convertido en un vector clave de riesgo, donde las vulnerabilidades de los proveedores pueden comprometer la confidencialidad, integridad y disponibilidad de los activos organizacionales (ISO/IEC 27001:2022); (NIST SP 800-53:2020).

Este proyecto se justifica por su aporte teórico y práctico al proponer un modelo integral de buenas prácticas de seguridad de la información para proveedores críticos de TI que, a diferencia de enfoques tradicionales, incorpora no solo controles técnicos sino también elementos culturales basados en los modelos AET (Awareness, Education, Training) y BC (Behavior Compliance). La literatura actual destaca la carencia de marcos que aborden de manera holística la dimensión humana y cultural en la gestión de riesgos de terceros (ENISA, 2022); e (ISACA, 2023), aspecto que esta tesis abordará mediante la definición de métricas y estrategias para evaluar y fortalecer la cultura de seguridad en proveedores (Diveti, 2025); e (NinjaOne, 2024).

En términos prácticos, el modelo propuesto permitirá a las organizaciones de TI:

Gestionar de forma más efectiva los riesgos asociados a proveedores, integrando la cultura de seguridad en la relación contractual y operativa (Diveti, 2022).

Optimizar la asignación de recursos y facilitar el cumplimiento de normativas nacionales e internacionales, como la ISO 27001, el GDPR y la Ley 1581 de 2012 en Colombia (Diveti, 2022).

Fortalecer la resiliencia cibernética, reduciendo vulnerabilidades introducidas por la cadena de suministro digital (ENISA, 2022).

Desde una perspectiva social, la mejora en la seguridad de la cadena de suministro digital contribuirá a:

Proteger la información sensible de clientes, ciudadanos y otras partes interesadas, mitigando riesgos de filtraciones y daños reputacionales (Ponemon Institute, 2023).

Fomentar un entorno digital más seguro y confiable, impulsando la confianza en las transacciones electrónicas y el comercio digital (ISACA, 2023).

Reducir pérdidas económicas derivadas de incidentes de seguridad, fortaleciendo la sostenibilidad y competitividad empresarial (NinjaOne, 2024).

El modelo propuesto ofrece beneficios directos a diversos grupos de interés:

Organizaciones de TI: Obtienen una herramienta de gobernanza para mitigar riesgos en la cadena de suministro y facilitar el cumplimiento de marcos internacionales como ISO 27001 y NIST.

Proveedores Críticos: Se ven beneficiados al recibir lineamientos claros que mejoran su madurez en seguridad, permitiéndoles convertirse en aliados estratégicos más confiables.

Partes Interesadas (Clientes/Usuarios): Se ven favorecidas indirectamente por una mayor protección de sus datos sensibles, lo que fortalece la confianza en los servicios digitales de la organización.

Por estas razones, este proyecto responde a una necesidad crítica y actual, aportando conocimiento relevante y soluciones prácticas para la gestión integral de la seguridad en la cadena de suministro de TI.

1.5 Objetivos

1.5.1 Objetivo general

Proponer un modelo de buenas prácticas de seguridad de la información en un marco de gestión de riesgos integral para los proveedores en funciones críticas, en áreas de TI a partir de los modelos Awareness, Education and Training Model (AET) y Behavior Compliance Model (BC).

1.5.2 Objetivos específicos

1. Determinar los elementos de los modelos AET y BC que son relevantes para las organizaciones de TI, en cuanto al manejo de proveedores y sus respectivos procesos.
2. Analizar los elementos de los modelos propuestos en el contexto del funcionamiento de la organización respecto a la evaluación de los proveedores, determinando su impacto en la efectividad de los procesos propios de la compañía.
3. Identificar las principales causas de las desviaciones asociadas a las prácticas inseguras de los proveedores, con el fin de mitigar los riesgos asociados a dichas prácticas.
4. Evaluar las medidas de seguridad actuales, bajo los lineamientos de los modelos AET y BC, con el propósito de mejorar la gestión de riesgos.
5. Documentar la implementación del nuevo modelo basado en las prácticas analizadas de los modelos AET y BC.

6. Medir el impacto de la integración de los modelos AET y BC en la gestión de riesgos de los proveedores de TI.

1.6 Alcances y limitaciones del modelo

Alcance. Proponer un modelo sobre la aplicación de las mejores prácticas en seguridad de la información a partir de los modelos (AET) y (BC) por medio del estudio del comportamiento de los proveedores al prestar sus servicios en organizaciones de TI, con el fin de mejorar la cultura organizacional asegurando que se comprendan las políticas, procedimientos y responsabilidades de seguridad de la información. Esta evaluación de los modelos busca promover una mayor concienciación de la seguridad y garantizar el cumplimiento de los requisitos legales en materia de seguridad. Las contramedidas asociadas están enfocadas puntualmente a reducir la variabilidad no deseada del comportamiento de los proveedores críticos.

La compañía puede requerir que sus aliados y/o proveedores accedan a información interna, la copien, la modifiquen, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos, la compañía debe exigir a los proveedores que tengan medidas adecuadas para la protección de la información de acuerdo con su clasificación y análisis de riesgo.

Limitaciones del proyecto. Si bien el modelo propuesto constituye un aporte conceptual relevante para la gestión de la seguridad de la información en proveedores críticos de TI, es importante reconocer las limitaciones inherentes al alcance y enfoque del presente trabajo.

En primer lugar, la investigación se desarrolló desde una perspectiva **conceptual y documental**, sin la implementación empírica completa del modelo en un entorno organizacional real. En consecuencia, los resultados obtenidos reflejan una validación teórica y analítica basada en la literatura especializada, marcos normativos y buenas prácticas

internacionales, mas no una medición directa del impacto del modelo en indicadores reales de reducción de incidentes o cambio conductual.

En segundo lugar, el análisis de impacto cuantitativo del modelo (AET+BC) se plantea de manera **proyectiva y simulada**, apoyándose en escenarios hipotéticos y correlaciones reportadas en estudios previos, lo que limita la posibilidad de generalizar resultados numéricos específicos. La ausencia de datos primarios provenientes de encuestas aplicadas, auditorías reales o métricas operativas impide afirmar con certeza el grado exacto de efectividad del modelo en contextos organizacionales particulares.

Otra limitación relevante radica en la **heterogeneidad de los proveedores críticos**. Las organizaciones proveedoras difieren significativamente en tamaño, sector, madurez en seguridad, cultura organizacional y capacidades técnicas, lo que implica que la aplicación del modelo podría requerir ajustes sustanciales para adaptarse a contextos específicos. Por tanto, el modelo no debe interpretarse como una solución rígida, sino como un marco de referencia flexible susceptible de adaptación.

Finalmente, el estudio no abarca de manera exhaustiva los **factores externos** que pueden influir en la conducta de los proveedores, tales como presiones comerciales, restricciones presupuestales, relaciones contractuales asimétricas o dinámicas regulatorias cambiantes. Estos elementos, aunque reconocidos, no fueron analizados en profundidad y podrían incidir en la efectividad real de las estrategias de concienciación y cumplimiento conductual propuestas.

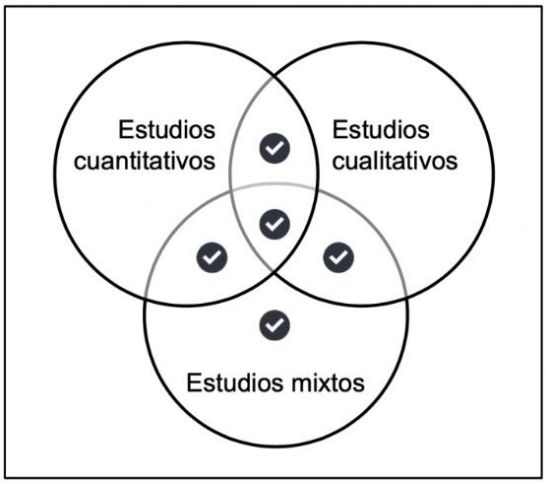
1.7 Metodología

A nivel de la metodología propuesta para el desarrollo de la tesis, se plantea un enfoque mixto ya que se integran los métodos cuantitativos y cualitativos, véase la **fig. 2**, que incluyen encuestas a empleados, proveedores y entrevistas con la alta dirección de la organización. Los

datos recopilados se analizaron cuantitativamente y cualitativamente para obtener una visión completa de las brechas y sus causas.

Figura 2.

Tipos de estudios incluidos en una revisión sistemática mixta.



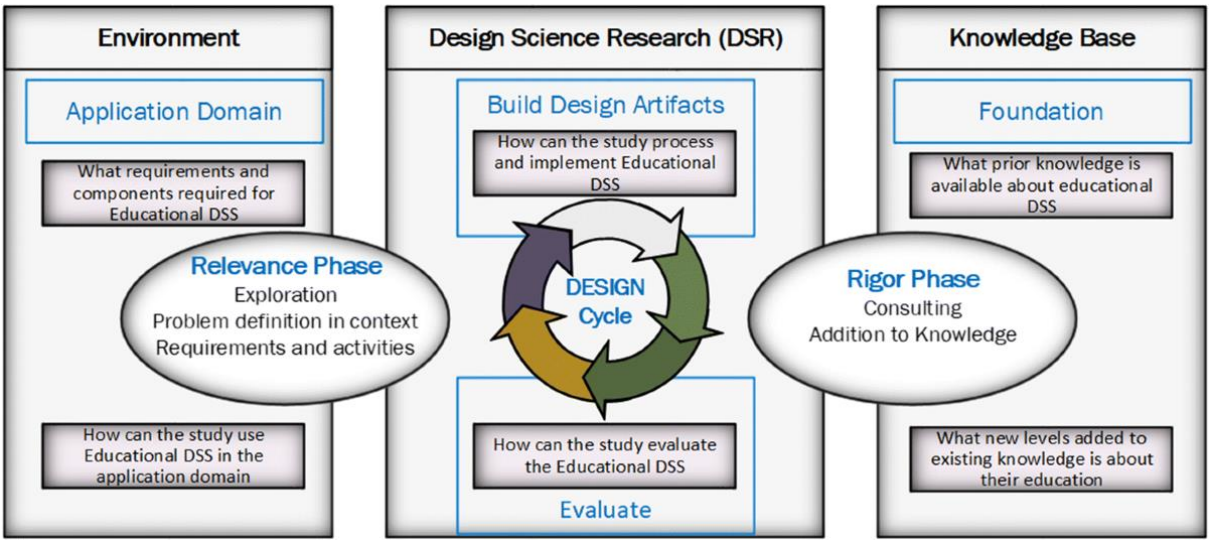
Nota: Tomado de (Hong, Turcotte-Tremblay, & Pluye, 2020)**.**

Enfoque o Metodología Específica: Investigación Basada en Diseño (Design Science Research). La investigación se guio por los principios de la Investigación Basada en Diseño (Design Science Research - DSR), véase **Fig. 3.** Este enfoque metodológico es idóneo para el desarrollo del Modelo de buenas prácticas en seguridad de la información para proveedores críticos, ya que se divide en 3 ciclos fundamentales.

1. **Ciclo de Relevancia:** Identifica las necesidades del entorno, específicamente las brechas en la gestión de proveedores críticos de TI y el impacto del factor humano.
2. **Ciclo de Rigor:** Fundamenta la investigación en el conocimiento existente, utilizando los modelos **AET** (Conciencia, Educación, Entrenamiento) y **BC** (Cumplimiento Conductual), además de estándares como **ISO 27001** y **NIST CSF**.
3. **Ciclo de Diseño:** Es la fase de construcción y evaluación del modelo integrado **MBSI-PC**, donde se desarrollan los instrumentos y la arquitectura del artefacto.

Figura 3.

Investigación mediante ciclos de relevancia, rigor y diseño.



Nota: Tomado de (Hevner, 2007).

1.7.1 Fases del desarrollo metodológico

Fase cualitativa dentro de DSR: Identificación del problema y justificación: Esta fase inicial de DSR es fuertemente cualitativa. Implicó una revisión exhaustiva de la literatura de los modelos (AET, BC y los estándares NIST e ISO 27001 y 27002) para comprender las discrepancias en la cultura organizacional y los vacíos de conocimiento en proveedores críticos de TI. También se incluye un análisis de estudios de caso y la identificación de prácticas inseguras a través de la interpretación de datos contextuales. El objetivo de esta fase es obtener una comprensión profunda de la causa raíz del problema.

Diseño y desarrollo del artefacto: La creación del modelo de buenas prácticas (el artefacto) es un proceso iterativo y creativo, que se alimenta de la síntesis de conocimientos existentes (marcos teóricos, estándares como NIST e ISO 27001 y 27002) y de la perspectiva de expertos (tal como se refleja en la literatura especializada). Esta fase implica tomar

decisiones cualitativas sobre cómo integrar los modelos AET y BC para maximizar su impacto en el contexto específico de la gestión de proveedores críticos en TI.

Evaluación Inicial (demostración conceptual): Las primeras etapas de evaluación de un artefacto (modelo) en la metodología DSR pueden ser de naturaleza cualitativa, como la validación conceptual del modelo a través de su alineación con las mejores prácticas y la lógica esperada, tal como sería presentado a un grupo de expertos para obtener retroalimentación y validación conceptual en una fase posterior.

Fase cuantitativa dentro de DSR: Evaluación y medición del impacto: Aunque la implementación completa del modelo no forma parte del alcance total de esta tesis, la metodología DSR exige que se demuestre la utilidad del artefacto (modelo). Aquí es donde los elementos cuantitativos entran en juego. Se describe cómo, en una eventual implementación, se buscaría medir la efectividad de las medidas de seguridad, el impacto en la reducción de incidentes, o la mejora en los niveles de cumplimiento o conciencia, utilizando indicadores clave de desempeño (KPIs). Para esta propuesta, se describe conceptualmente cómo se mediría este impacto, lo que le confiere un componente cuantitativo al diseño del modelo y su potencial validación.

1.7.2 Técnicas e instrumentos de recolección.

Fichas de registro bibliográfico: para organizar la literatura científica y técnica. Incluyó artículos de revistas especializadas, tesis doctorales y de maestría, libros y publicaciones de congresos en las áreas de ciberseguridad, gestión de riesgos de terceros, cultura organizacional en seguridad, concienciación y comportamiento de cumplimiento. Adicionalmente, el análisis se alimenta de la revisión conceptual de tipos de documentos organizacionales (políticas de seguridad, procedimientos internos, registros de incidentes - si fueran accesibles en un contexto real de implementación) que ilustran las discrepancias y vacíos de conocimiento previamente identificados.

Matrices de análisis comparativo: para contrastar los modelos AET/BC con los estándares NIST e ISO. Donde la muestra principal de datos para estas fases proviene de una selección amplia y relevante de publicaciones académicas, estándares internacionales (como NIST CSF 2.0 y NIST Special Publications serie 800 y la familia ISO/IEC 27000), guías de la industria y estudios de caso. La selección de esta literatura se basó en criterios de autoridad de la fuente, su pertinencia temática con los modelos AET, BC y la gestión de proveedores, y la actualidad de la información para reflejar las mejores prácticas actuales.

Juicio de Expertos (Conceptual): El diseño del modelo incorpora implícitamente el conocimiento colectivo y las mejores prácticas propuestas por expertos de la industria y la academia, tal como se documenta en las fuentes secundarias. Para una futura validación práctica del modelo, esta fuente se materializaría a través de entrevistas o encuestas a un panel de expertos.

En síntesis, la adopción de la metodología Design Science Research (DSR) garantiza que el modelo MBSI-PC no sea solo un planteamiento teórico, sino un artefacto diseñado sistemáticamente para resolver una problemática real en la gestión de proveedores críticos de TI. Mediante el equilibrio entre el Ciclo de Relevancia (necesidades del entorno de las organizaciones frente a la relación con los proveedores críticos), el Ciclo de Rigor (estándares ISO/NIST y modelos (AET+BC)) y el Ciclo de Diseño (iteración y validación), se asegura la coherencia técnica y la aplicabilidad del modelo. Esta estructura metodológica proporciona el rigor necesario para que los resultados obtenidos sean medibles y escalables, permitiendo que los siguientes capítulos se centren detalladamente en la arquitectura, integración y componentes específicos de la propuesta de solución.

En síntesis, este capítulo establece las bases del problema de investigación, evidenciando la brecha crítica entre cultura declarada de seguridad y prácticas reales en proveedores de TI críticos, exacerbada por los 36 millones de intentos de ciberataques en Colombia (2024). La metodología DSR asegura relevancia práctica, preparando el terreno para

una propuesta integral que mitigue riesgos humanos (74% de incidentes), alineada con los objetivos y estándares propuestos como ISO/NIST.

2. ESTADO DEL ARTE

El análisis de la literatura especializada constituye un insumo fundamental para comprender la evolución de los enfoques utilizados en la gestión de la seguridad de la información y, en particular, en la administración de riesgos asociados a proveedores críticos. Este capítulo tiene como propósito revisar de manera crítica los principales modelos teóricos, marcos normativos y propuestas de madurez que han abordado la dimensión técnica, organizacional y humana de la seguridad.

La revisión se estructura en torno a tres ejes conceptuales: el factor humano y cultural en seguridad (modelos AET y BC), los modelos de madurez aplicados a la gestión de la seguridad y de terceros, y los estándares internacionales que proporcionan lineamientos formales para la gestión del riesgo. Esta aproximación permite identificar coincidencias, vacíos y oportunidades de integración entre los enfoques existentes.

Si bien marcos como ISO/IEC 27001 y el NIST CSF ofrecen una base sólida para la implementación de controles, la literatura coincide en que su efectividad se ve condicionada por el nivel de concienciación, capacitación y comportamiento de las personas involucradas. En el caso de los proveedores críticos de TI, estas condiciones se complejizan debido a la heterogeneidad organizacional, cultural y operativa, lo que exige modelos más flexibles y centrados en la conducta real.

El estado del arte evidencia, por tanto, una carencia de propuestas integrales que articulen de forma sistemática la formación en seguridad con mecanismos de cumplimiento conductual específicamente orientados a proveedores críticos. Esta brecha conceptual constituye el punto de partida para el desarrollo del modelo propuesto en la presente investigación.

2.1 Contextualización de la seguridad de la información

En la era digital actual, la seguridad de la información se ha convertido en un elemento estratégico imprescindible para la continuidad, competitividad y sostenibilidad de las organizaciones. El creciente uso de tecnologías de la información y la interconectividad global ha ampliado las superficies de ataque y las vulnerabilidades, generando un entorno cada vez más complejo y dinámico frente a las amenazas cibernéticas.

La seguridad de la información involucra la protección de la confidencialidad, integridad y disponibilidad de los activos de información, haciendo frente a riesgos que pueden originarse tanto desde fuentes externas como internas, como ataques maliciosos, ataques por errores, negligencias o incumplimientos. En este contexto, la gestión eficaz de la seguridad no puede basarse exclusivamente en controles técnicos, sino que debe considerar factores humanos, culturales y organizacionales que influyen decisivamente en el nivel real de protección.

Un aspecto clave en la actualidad es la integración de proveedores externos, especialmente aquellos considerados críticos para las operaciones de la organización. Esta externalización amplifica la complejidad de la gestión de la seguridad, debido a que los proveedores tienen acceso a información y sistemas sensibles, por lo que representan un eslabón vulnerable que puede ser explotado para comprometer la infraestructura organizacional.

Los incidentes de seguridad vinculados a proveedores críticos han aumentado de manera significativa en los últimos años. Por ejemplo, Colombia se ha posicionado como el cuarto país con más ciberataques en América Latina, enfrentando una crisis de seguridad digital. Durante 2024, el país registró más de 36 mil millones de intentos de ciberataques y se reportaron 22.086 vulnerabilidades, lo que evidencia el creciente riesgo para empresas y gobierno, concentrando el 17% de los ataques en Latinoamérica (Infobae, 2024), con el sector salud como uno de los más afectados, según la Asociación Colombiana de Informática, Sistemas y Tecnologías Afines (ACIS, 2025). La prevalencia de ataques mediante credenciales comprometidas y la creciente sofisticación de las técnicas, como el uso de

inteligencia artificial para potenciar estas amenazas, aumentan la urgencia de fortalecer las estrategias de seguridad ante la cadena de suministro digital.

El factor humano se mantiene como el eslabón más débil en la defensa de la seguridad de la información, estando involucrado en aproximadamente el 74% de las infracciones de seguridad reportadas (ENISA, 2025). Esto se debe a que las personas son quienes deben aplicar y cumplir las políticas, actuando como la primera línea de defensa efectiva contra amenazas internas y externas. Sin embargo, existe frecuentemente una discrepancia entre la cultura declarada de seguridad de la organización y la práctica concreta de los empleados y proveedores, generando brechas que deben ser abordadas mediante modelos de concienciación, educación y cumplimiento conductual.

De esta manera, la cultura organizacional de seguridad, junto con la capacitación continua y la evaluación del cumplimiento de normas y buenas prácticas, son pilares fundamentales para transformar a todos los actores internos y externos en agentes activos de protección. En particular, la colaboración segura con proveedores críticos de TI requiere una gestión rigurosa y adaptada a la criticidad de sus funciones, que no solo garantiza el cumplimiento normativo, sino que también fomenta una cultura común de seguridad y responsabilidad compartida.

En conclusión, la contextualización de la seguridad de la información en el entorno actual evidencia la necesidad de un enfoque integral que considere tanto los aspectos técnicos como los humanos, culturales y relacionales. Este enfoque es el fundamento sobre el cual se construye la propuesta del presente trabajo, orientado a fortalecer la cultura de seguridad en la interacción con proveedores críticos, contribuyendo a mitigar riesgos, proteger activos y aumentar la resiliencia organizacional frente a las amenazas digitales.

2.2 Principales modelos teóricos y normativos orientados al factor humano en seguridad.

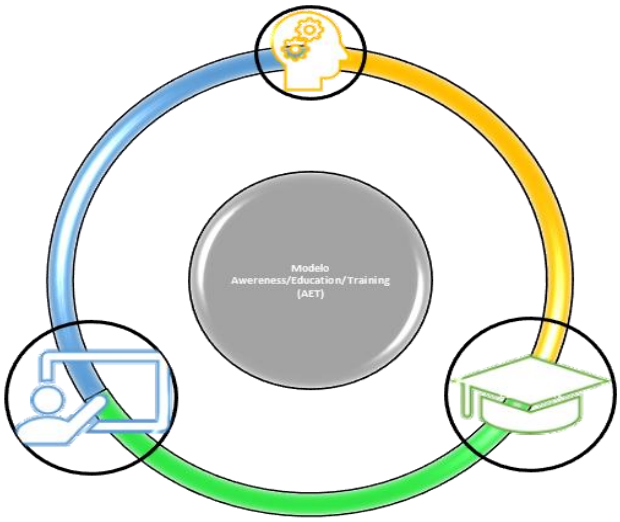
En el ámbito de la gestión de la seguridad de la información, la integración de modelos teóricos que abordan tanto el desarrollo de la cultura organizacional como el comportamiento de las personas es fundamental para lograr un entorno seguro y sostenible. Este proyecto se centra en particular en dos modelos que complementan esta visión: el modelo AET (Awareness, Education, Training) y el modelo de Behavior Compliance (BC). Asimismo, se reconoce el papel esencial de las normativas internacionales como la ISO/IEC 27001, el Anexo A de la ISO/IEC 27002 y el marco NIST, que formalizan los principios y controles necesarios para una gestión eficaz.

2.2.1 Modelo AET (concienciación, educación, formación).

El modelo AET se basa en la premisa de que la mejora continua en la seguridad de la información depende directamente del desarrollo progresivo de conciencia, educación y capacitación entre todos los actores involucrados. Este modelo comprende tres etapas interrelacionadas, como se muestra en la siguiente figura 4:

Figura 4.

Modelo AET (concienciación, educación, formación).



Nota: elaboración propia basada en el modelo AET.

Awareness (Concienciación): Consiste en sensibilizar a los miembros de la organización y proveedores críticos respecto a los riesgos y amenazas, así como sobre la importancia de las prácticas de seguridad. Esta fase tiene un alcance general y busca motivar el interés y la responsabilidad.

Education (Educación): Implica la profundización del conocimiento mediante información estructurada y detallada sobre políticas, procedimientos, normativas y buenas prácticas. Esta etapa aporta fundamentos teóricos y normativos que sustentan la cultura de seguridad.

Training (Capacitación): Se focaliza en el desarrollo de habilidades prácticas mediante entrenamientos específicos adaptados a roles y responsabilidades, fortaleciendo la capacidad de respuesta y cumplimiento de las medidas de seguridad.

Este modelo destaca la necesidad de un enfoque integral y continuo, donde cada etapa se refuerza mutuamente para consolidar una cultura sólida y activa frente a los riesgos cibernéticos (Puhakainen & Siponen, 2010).

2.2.2 Modelo de cumplimiento conductual (BC).

Complementando al modelo AET, el modelo de Behavior Compliance (BC) se enfoca en asegurar que los conocimientos adquiridos se traduzcan en comportamientos reales y sostenibles en el tiempo. Este modelo reconoce que la formación por sí sola no garantiza el cumplimiento efectivo de las políticas, por lo que incorpora mecanismos de observación, monitoreo, retroalimentación y refuerzo conductual.

El modelo de comportamiento de cumplimiento de la Figura 5**.** Describe los principales métodos y las métricas con el fin de validar el cumplimiento y la eficacia de los mismos. Se mide combinando la reducción real de incidentes, el cumplimiento de normas, la participación activa, el seguimiento de KPIs específicos y la evaluación de la cultura de seguridad, adicionalmente, el refuerzo positivo por buen desempeño conductual y la mejora continua de los proveedores.

El BC se basa en teorías del comportamiento organizacional y psicológico que analizan los factores que influyen en la adopción o rechazo de prácticas seguras, incluyendo incentivos, sanciones, normas sociales y cultura organizacional. Su objetivo es cerrar la brecha entre la intención declarada y la práctica efectiva, promoviendo la adherencia mediante intervenciones conductuales y evaluaciones periódicas (Hu, Maimon, Koh, & Park, 2021).

En el contexto de proveedores críticos de TI, el modelo BC es especialmente relevante debido a la heterogeneidad de entornos y niveles de compromiso, exigiendo estrategias personalizadas que aseguren el cumplimiento dentro del marco contractual y operativo.

Figura 5.

Modelo behavior compliance (BC) con ciclo de monitoreo, alimentación, refuerzo y mejora continua.



Nota: elaboración propia basada en las dimensiones del modelo BC.

2.3 Cultura organizacional y seguridad de la información.

La cultura organizacional de seguridad se define como el conjunto de valores, actitudes, creencias y comportamientos compartidos que influyen en la forma en que los miembros de una organización perciben, implementan y mantienen las prácticas de seguridad de la información (Von Solms & Von Solms, 2004). Es un factor determinante en la efectividad real de las políticas y controles, dado que es el comportamiento humano quien finalmente ejecuta o ignora las medidas definidas.

Una cultura sólida promueve la concienciación, la responsabilidad y el compromiso continuo con la seguridad, no solo desde el cumplimiento normativo, sino también desde la adopción voluntaria de buenas prácticas en todos los niveles jerárquicos y funcionales.

La cultura de seguridad de la información es el fundamento sobre el cual se construye la protección de los activos y la confianza en el entorno laboral. Al fomentar una cultura de seguridad, no solo se está fortaleciendo las defensas contra las amenazas cibernéticas, sino que también se está cultivando una mentalidad de responsabilidad y cuidado entre todos los miembros de la organización. Esto no solo protege los datos y la reputación de la empresa, sino que también contribuye a un ambiente laboral más seguro y productivo. (AICHE, 2020). Una cultura de seguridad de la información puede definirse como la forma en que se hacen las cosas en la organización para proteger los activos de información.

El factor humano es reconocido como el eslabón más vulnerable y, a la vez, más valioso en la gestión de la seguridad (ENISA, 2025). Las personas pueden ser tanto un riesgo por acciones negligentes, errores o conductas maliciosas, como una defensa efectiva si cuentan con conciencia, educación y compromiso adecuados.

Por esta razón, la gestión del factor humano como sensor implica implementar estrategias de capacitación, sensibilización y evaluación continua para transformar a los

empleados y proveedores en agentes activos de protección, capaces de identificar y reaccionar adecuadamente frente a riesgos y amenazas.

2.4 Modelos de madurez en gestión de seguridad de la información

Los modelos de madurez representan marcos estructurados que permiten a las organizaciones evaluar su nivel actual de capacidad en seguridad de la información y establecer una ruta evolutiva hacia estados superiores de desempeño. A diferencia de los estándares normativos como ISO/IEC 27001 que establecen requisitos de cumplimiento binario (cumple/no cumple), los modelos de madurez reconocen que las organizaciones progresan a través de niveles graduales de sofisticación y efectividad. Esta perspectiva evolutiva resulta particularmente relevante para la gestión de proveedores críticos, donde la heterogeneidad en niveles de madurez puede representar riesgos significativos si no se identifica y gestiona apropiadamente.

2.4.1 Modelos generales de madurez (CMM, CMMI, C2M2).

Modelo de Madurez de Capacidades (CMM) y sus Derivaciones. El concepto de modelo de madurez tiene sus raíces en el Capability Maturity Model (CMM) desarrollado por el Software Engineering Institute (SEI) de la Universidad Carnegie Mellon en 1986, originalmente para procesos de desarrollo de software (Paulk, 1993). Este modelo pionero estableció cinco niveles de madurez:

(1) Inicial - procesos impredecibles y reactivos,

(2) Gestionado - procesos proyectados con disciplina básica,

(3) Definido - procesos organizacionales estandarizados,

(4) Gestionado Cuantitativamente - procesos medidos y controlados, y

(5) Optimizado - mejora continua, basada en datos cuantitativos.

La aplicación del enfoque CMM a la ciberseguridad dio origen a múltiples modelos especializados. El CMMI-Cybermaturity (CMMI, 2018) extiende el marco CMMI tradicional incorporando dominios específicos de ciberseguridad como gestión de activos, controles de acceso, respuesta a incidentes y gestión de riesgos de terceros. Este modelo resulta particularmente relevante para el contexto de este proyecto, ya que incluye un dominio específico de "Gestión de Riesgos de la Cadena de Suministro" que evalúa capacidades para identificar, valorar y mitigar riesgos asociados a proveedores críticos a través de cinco niveles de madurez progresivos.

Modelo de Madurez de Ciberseguridad del Departamento de Energía (C2M2). El Cybersecurity Capability Maturity Model (C2M2) desarrollado por el Departamento de Energía de Estados Unidos (DOE, 2014), representa otro marco significativo que ha sido adoptado ampliamente en infraestructuras críticas. El C2M2 organiza las prácticas de ciberseguridad en diez dominios que incluyen Gestión de Riesgos, Gestión de Activos, Configuración y Gestión del Cambio, Gestión de Identidad y Acceso, y crucialmente, Gestión de la Cadena de Suministro y Dependencias Externas.

Para cada dominio, el C2M2 define cuatro niveles de madurez (MIL 0 a MIL 3): MIL 0 representa prácticas inexistentes o ad-hoc; MIL 1 indica prácticas iniciales realizadas, pero no documentadas consistentemente; MIL 2 refleja prácticas documentadas, comunicadas y ejecutadas de manera confiable; y MIL 3 denota prácticas institucionalizadas con mejora continua, basada en métricas. El dominio de Gestión de la Cadena de Suministro en C2M2 aborda específicamente la evaluación y gestión continua de riesgos asociados a proveedores, productos y servicios externos, estableciendo que en MIL 3 las organizaciones deben tener procesos maduros para: (a) identificar y priorizar proveedores críticos, (b) establecer requisitos de seguridad en contratos, (c) verificar el cumplimiento de proveedores mediante auditorías, (d) monitorear continuamente el desempeño de seguridad de proveedores, y (e) gestionar incidentes que involucren la cadena de suministro (DOE, 2014).

Modelos de Madurez en Concienciación y Cultura de Seguridad. El Security Culture Maturity Model (SCMM) propuesto por Van Niekerk y Von Solms (2010) representa un enfoque específico para evaluar y desarrollar la madurez de la cultura de seguridad organizacional. Este modelo establece cinco niveles: (1) Ausencia de cultura de seguridad donde no existe conciencia ni políticas formales, (2) Cultura de seguridad básica con políticas documentadas, pero sin internalización, (3) Cultura de seguridad en desarrollo con concienciación creciente y adopción parcial, (4) Cultura de seguridad establecida donde las prácticas seguras son la norma, y (5) Cultura de seguridad dinámica con mejora continua, impulsada por todos los niveles organizacionales.

La relevancia del SCMM para el presente proyecto radica en su reconocimiento explícito de que la cultura de seguridad no surge espontáneamente del cumplimiento normativo, sino que requiere un desarrollo intencional y progresivo que evoluciona desde la ausencia de conciencia hasta la optimización continua. Este modelo valida el enfoque integrado (AET+BC) propuesto, donde los elementos formativos (AET) contribuyen a la transición entre niveles culturales, mientras que los elementos conductuales (BC) aseguran la consolidación e institucionalización de cada nivel antes de avanzar al siguiente.

2.4.2 Modelos específicos orientados a la cadena de suministro y terceros.

Sistema de Gestión de Madurez de Seguridad (SGMS) para Proveedores**.** Investigaciones recientes han propuesto modelos de madurez específicamente diseñados para evaluar la seguridad en proveedores. El Supply Chain Cybersecurity Maturity Model desarrollado por Boyson (2014) establece cuatro niveles de madurez enfocados en la gestión de riesgos cibernéticos en cadenas de suministro: (1) Nivel Ad-hoc donde las organizaciones tienen conciencia mínima de riesgos cibernéticos en su cadena de suministro, (2) Nivel Básico donde existen políticas pero sin verificación sistemática de cumplimiento en proveedores, (3) Nivel Avanzado con evaluaciones formales de seguridad de proveedores y monitoreo continuo,

y (4) Nivel Predictivo donde se utilizan análisis avanzados para anticipar y prevenir amenazas emergentes en la cadena de suministro.

Este modelo se alinea directamente con la problemática abordada en este proyecto, ya que reconoce que la madurez en la gestión de proveedores críticos requiere evolucionar desde evaluaciones puntuales de cumplimiento (Nivel Básico) hacia sistemas integrados de concienciación, capacitación, monitoreo y mejora continua (Niveles Avanzado y Predictivo). La transición entre estos niveles demanda precisamente los elementos identificados en los modelos AET y BC: no se puede alcanzar madurez avanzada sin programas efectivos de concienciación y educación para proveedores (AET), ni se puede mantener esa madurez sin sistemas robustos de monitoreo, medición y refuerzo conductual (BC).

NIST Cybersecurity Framework (CSF). Dentro del amplio espectro de marcos de referencia para la gestión de la seguridad de la información, el NIST Cybersecurity Framework (CSF) se presenta como una herramienta particularmente pertinente para este proyecto, dada su orientación hacia la gestión de riesgos y su aplicabilidad transversal a organizaciones de distintos tamaños y sectores. Este modelo, desarrollado por el National Institute of Standards and Technology (NIST), estructura sus lineamientos en seis funciones clave: Governar, Identificar, Proteger, Detectar, Responder y Recuperar, las cuales permiten establecer un enfoque integral y dinámico frente a las amenazas cibernéticas. A diferencia de otros modelos más prescriptivos o centrados en procesos específicos, el NIST CSF promueve una madurez progresiva basada en la mejora continua, la alineación con objetivos estratégicos y la adaptación al contexto organizacional. Su flexibilidad metodológica y su énfasis en la resiliencia lo convierten en un marco idóneo para evaluar y fortalecer las capacidades de seguridad de los proveedores de TI que gestionan funciones críticas, aspecto central en el planteamiento del problema de esta tesis.

La adopción del modelo NIST Cybersecurity Framework (CSF) se alinea directamente con los objetivos específicos de este proyecto, al proporcionar una estructura metodológica

clara para evaluar y fortalecer las capacidades de seguridad de los proveedores de TI que gestionan funciones críticas.

En primer lugar, el modelo permite gobernar e identificar y categorizar los riesgos asociados a la tercerización de servicios tecnológicos, lo cual responde al objetivo de diagnosticar el nivel de exposición de la organización frente a amenazas externas.

En segundo lugar, sus funciones de proteger y detectar ofrecen lineamientos concretos para analizar los controles implementados por los proveedores y su efectividad en la prevención de incidentes, contribuyendo así al objetivo de evaluar el cumplimiento de estándares de seguridad.

Finalmente, las funciones de Responder y Recuperar permiten valorar la capacidad de reacción y resiliencia ante eventos de seguridad, lo que se vincula con el objetivo de proponer mecanismos de mejora continua y fortalecimiento de la cultura de seguridad de la información. En conjunto, el NIST CSF no solo facilita una evaluación integral, sino que también orienta la formulación de estrategias sostenibles y alineadas con las mejores prácticas internacionales.

Integración de Modelos de Madurez con Marcos Normativos**.** La literatura académica establece que los modelos de madurez y los estándares normativos son complementarios, no alternativos (Proença & Borbinha, 2016). Mientras que estándares como ISO/IEC 27001 definen "qué" controles implementar y NIST SP 800-53 detalla "cómo" implementarlos, los modelos de madurez proporcionan la dimensión evolutiva del "dónde estamos y hacia dónde vamos", permitiendo a las organizaciones:

Evaluación del estado actual: Determinar el nivel de madurez presente en la gestión de seguridad con proveedores críticos, identificando brechas específicas respecto a prácticas de niveles superiores.

Priorización de inversiones: Focalizar recursos en las capacidades que mayor impacto tendrán en la elevación del nivel de madurez, evitando la dispersión de esfuerzos en controles de baja prioridad según el contexto organizacional.

Establecimiento de roadmap evolutivo: Definir una secuencia lógica de desarrollo de capacidades, reconociendo que ciertos niveles de madurez son prerrequisitos para otros (por ejemplo, no se puede alcanzar madurez en monitoreo conductual sin previamente tener madurez básica en políticas documentadas y comunicadas).

Benchmarking sectorial: Comparar el nivel de madurez organizacional con pares del sector, identificando áreas de ventaja competitiva o exposición relativa a riesgos.

Para el modelo (AET+BC) propuesto, esta integración se materializa en la vinculación de elementos específicos del modelo con niveles de madurez esperados:

Nivel 1 (Inicial): Concienciación (AET) básica mediante comunicaciones esporádicas; Cumplimiento (BC) definido en contratos, pero sin verificación sistemática.

Nivel 2 (Gestionado): Educación (AET) formal con evaluaciones de conocimiento; Monitoreo (BC) periódico con indicadores básicos de cumplimiento.

Nivel 3 (Definido): Capacitación (AET) diferenciada por roles y riesgos; Sistema estructurado de Reconocimiento y Consecuencias (BC) con feedback regular.

Nivel 4 (Cuantitativo): Optimización de programas AET basada en métricas de efectividad; Monitoreo (BC) continuo con KPIs integrados a cuadros de mando organizacionales.

Nivel 5 (Optimizado): Mejora Continua (BC) con ajustes proactivos de elementos AET según análisis predictivo de riesgos emergentes; cultura de seguridad completamente institucionalizada donde los proveedores son verdaderos socios estratégicos en la protección de activos organizacionales.

Para contextualizar el valor agregado del modelo propuesto, se presenta la siguiente comparación (véase la tabla 2) directa con dos marcos reconocidos internacionalmente: CMMI y C2M2. Esta comparación permite evidenciar las diferencias en enfoque, dimensión humana y aplicabilidad.

Tabla 2.

Comparación con Modelos Existentes (CMMI y C2M2).

Aspecto	Modelo (AET+BC)	CMMI	C2M2
Enfoque	Cultura + Comportamiento	Madurez de procesos	Madurez en ciberseguridad
Dimensión Humana	Alta (Concienciación, Capacitación, Cumplimiento)	Baja (orientado a procesos)	Media (incluye roles y responsabilidades)
Medición	KPIs conductuales y culturales	Niveles de madurez (1-5)	Niveles MIL (0-3)
Aplicabilidad	Proveedores críticos TI	Desarrollo de software	Infraestructuras críticas
Fortaleza	Integración cultural y normativa	Estandarización de procesos	Resiliencia y respuesta ante incidentes

Nota: Elaboración basada en los modelos AET, BC, CMMI y C2M2.

2.4.3 Implicaciones para la gestión de proveedores críticos.

El reconocimiento de niveles de madurez tiene implicaciones prácticas significativas para la gestión de proveedores críticos. Primero, permite segmentar a los proveedores no solo por criticidad funcional (qué tan importantes son para el negocio) sino también por madurez de seguridad (qué tan desarrolladas están sus capacidades de protección), facilitando estrategias de gestión diferenciadas donde los proveedores de alta criticidad pero baja madurez reciben apoyo intensivo para elevar rápidamente sus capacidades, mientras que proveedores de madurez avanzada pueden gestionar mayor autonomía con supervisión menos intensiva.

Segundo, establece expectativas realistas sobre los tiempos requeridos para desarrollar capacidades efectivas. La evidencia empírica de implementaciones de CMM y C2M2 demuestra que la transición entre niveles de madurez típicamente requiere 12 a 24 meses de esfuerzo sostenido (CMMI, 2018), lo que subraya que la gestión efectiva de proveedores críticos no es un proyecto puntual sino un compromiso estratégico de desarrollo de capacidades a mediano plazo.

Tercero, proporciona un lenguaje común entre la organización y sus proveedores para discutir objetivos de seguridad. En lugar de exigir "cumplimiento total" de manera binaria, las

organizaciones pueden establecer planes de desarrollo de madurez consensuados con proveedores, donde se acuerdan niveles objetivo, plazos razonables y métricas intermedias de progreso, reduciendo fricciones y promoviendo relaciones colaborativas en lugar de únicamente transaccionales.

Finalmente, los modelos de madurez validan empíricamente la propuesta central de este proyecto: que la gestión efectiva de seguridad con proveedores críticos requiere un modelo integrado que combine elementos formativos (AET) y conductuales (BC) desplegados de manera evolutiva según el nivel de madurez actual y objetivo. Los modelos de madurez revisados consistentemente identifican que las organizaciones en niveles superiores se caracterizan por tener tanto programas robustos de capacitación como sistemas efectivos de monitoreo y mejora continua, confirmando que ningún elemento por sí solo es suficiente para alcanzar madurez avanzada en seguridad.

2.5 Normativas y marcos internacionales relevantes.

2.5.1 ISO/IEC 27001, 27002 y NIST CSF.

A continuación, se muestra en las tablas 3, 4 y 5, comparativa entre los estándares ISO27002 Y NIST CSF.

Tabla 3.

Comparativa entre los estándares ISO27002 Y NIST CSF.

Aspecto	ISO/IEC 27002 (Anexo A de ISO/IEC 27001)	NIST (CSF y SP 800-53)
Propósito principal	Proporcionar un conjunto de controles y mejores prácticas para la implementación de un SGSI enfocado en proteger la confidencialidad, integridad y disponibilidad de la información (ISO, 2022a).	Proveer un marco flexible para gestionar y reducir el riesgo cibernético, estructurado en funciones clave y controles detallados (NIST, 2018; NIST, 2020).
Estructura	14 dominios con 114 controles en el Anexo A, que abarcan aspectos técnicos, organizacionales y humanos.	Cinco funciones (Identificar, Proteger, Detectar, Responder, Recuperar) en CSF; familias de

Aspecto	ISO/IEC 27002 (Anexo A de ISO/IEC 27001)	NIST (CSF y SP 800-53)
		control en SP 800-53 con extensa granularidad.
Gestión de proveedores y terceros	Dominio A.15 "Relaciones con proveedores" cubre acuerdos, gestión de riesgos y monitoreo continuo de terceros.	Controles relacionados en familia "Supply Chain Risk Management" y funciones de gestión de proveedores dentro del CSF y SP 800-53.
Factor humano	Dominio A.7 enfocado en la gestión de recursos humanos: concienciación, formación, roles y responsabilidades.	Controles específicos sobre capacitación, monitoreo y evaluación del comportamiento humano en familias como "Concienciación y Capacitación".
Enfoque de implementación	Basado en la evaluación de riesgos e implementación de controles seleccionados para el SGSI; orientado a procesos y políticas definidas.	Enfoque basado en la gestión continua del riesgo, con evaluación, monitoreo y mejora continua; adaptable a diferentes sectores y tamaños.
Cobertura de riesgos	Riesgos técnicos, organizativos y humanos centrados en activos y procesos internos y externos.	Enfoque integral, cubriendo riesgos desde la identificación hasta la recuperación con procesos dinámicos y resilientes.
Mejora continua	Integrada en el ciclo PDCA (Planificar, Hacer, Verificar, Actuar) para el SGSI (ISO, 2022a).	Considerada a través del ciclo de vida del Framework y actualizaciones periódicas de controles y estrategias.
Relevancia para proveedores críticos	Enfatiza contratos, monitoreo y alineación de políticas con proveedores para asegurar la seguridad del ecosistema.	Detalla métodos para evaluar, monitorear y gestionar riesgos en la cadena de suministro y terceros, incluyendo protocolos de respuesta a incidentes.
Normatividad y reconocimiento	Es estándar internacional reconocido globalmente, utilizado para certificación y cumplimiento regulatorio.	Referencia primaria en Estados Unidos, adoptada también internacionalmente, especialmente en el gobierno y sectores críticos.

Nota: elaboración propia basada en los estándares ISO/IEC 27002 Y NIST CSF 2.0.

El marco normativo aporta un soporte esencial para la gestión estructurada de la seguridad de la información. Entre los principales estándares destacan:

ISO/IEC 27001: Establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en un enfoque de gestión de riesgos. Su Anexo A presenta controles específicos para diversos dominios, incluyendo la gestión de proveedores y la capacitación del personal (ISO, 2022b).

ISO/IEC 27002: Complementa la ISO 27001 con recomendaciones y prácticas para implementar los controles del Anexo A, especialmente en áreas como la cultura organizacional, la concienciación y la relación con terceros (ISO, 2022b).

Marco del NIST (Cybersecurity Framework y SP 800-53): Proporciona un enfoque pragmático y flexible mediante cinco funciones (Identificar, Proteger, Detectar, Responder y Recuperar) que cubren el ciclo completo de gestión del riesgo cibernético. Los controles del NIST incluyen aspectos técnicos, humanos y operativos, haciendo especial énfasis en la resiliencia y la mejora continua (NIST, 2018); (NIST SP 800-53:2020).

NIST Cybersecurity Framework (NIST CSF 2.0), El NIST es más orientado a resultados. La gestión de proveedores reside principalmente en la función GOVERNANCE (GV), específicamente en la categoría de Cybersecurity Supply Chain Risk Management (GV.SC). (NIST CSF 2.0, Febrero 26, 2024)

Tabla 4.

Comparativa de Controles ISO/IEC 27002:2022 vs NIST CSF

Tema ISO 27002	**Control Específico ISO 27002**	**Subcategoría NIST CSF 2.0 (Equivalente)**	**Objetivo del Control Comparado**
1. Organizacional	**5.19** Relaciones con proveedores	**GV.SC-01**: Estrategia y políticas C-SCRM.	Establecer el marco de gobernanza y reglas de compromiso.
	5.20 Acuerdos con proveedores	**GV.SC-05**: Requisitos en contratos.	Formalizar legalmente las obligaciones de ciberseguridad.
	5.21 Cadena de suministro TIC	**GV.SC-04**: Riesgos de sub-proveedores.	Gestionar el riesgo de la procedencia tecnológica y terceros.
	5.22 Seguimiento y revisión	**GV.SC-07**: Evaluaciones periódicas.	Verificar el cumplimiento mediante auditorías y métricas.
	5.23 Gestión de cambios	**GV.SC-08**: Gestión de cambios en la cadena.	Evaluar el impacto de cambios técnicos o de proveedores.
	5.24 Gestión de incidentes	**RS.MA-01/02**: Respuesta coordinada.	Garantizar que el proveedor reporte brechas oportunamente.

Tema ISO 27002	Control Específico ISO 27002	Subcategoría NIST CSF 2.0 (Equivalente)	Objetivo del Control Comparado
2. Personas	**6.1** Tamizado (Verificación de antecedentes)	**PR.AT-01**: Concienciación y formación.	Asegurar la confiabilidad de los empleados del proveedor.
	6.2 Términos de empleo	**GV.PO-02: Políticas de RRHH.**	**Mantener la confidencialidad post-empleo.**
	6.3 Concienciación y formación	**PR.AT-01: Entrenamiento en riesgos.**	**Reducir el riesgo de ingeniería social en el tercero.**
3. Físico	**7.2** Entrada física	**PR.PS-02**: Acceso físico seguro.	Limitar el acceso solo a personal autorizado del proveedor.
	7.4 Monitoreo físico	**PR.PS-05**: Vigilancia de instalaciones.	Detectar actividades no autorizadas en sitio.
	7.6 Trabajo en áreas seguras	**PR.PS-03**: Protección de áreas críticas.	Evitar la fuga de datos por observación o manipulación física.
4. Tecnológico	**8.2** Privilegios de acceso	**PR.AA-03**: Mínimo privilegio.	Restringir el acceso del proveedor solo a lo necesario.
	8.5 Autenticación (MFA)	**PR.AA-05**: Autenticación fuerte.	Prevenir el uso de credenciales robadas por terceros.
	8.23 Ciclo de vida de desarrollo	**PR.SD-01**: Seguridad en desarrollo.	Garantizar que el software entregado sea seguro por diseño.
	8.30 Segregación de redes	**PR.IR-02**: Segmentación de red.	Impedir el movimiento lateral del proveedor en la red interna.

Nota: elaboración basada en los estándares ISO/IEC 27002:2022 y NIST CSF. 2.0. Frente a los proveedores críticos.

Esta tabla comparativa vincula los controles específicos de los 4 temas de **ISO/IEC 27002:2022** con las subcategorías equivalentes del **NIST CSF 2.0**.

La integración de estos marcos normativos con los modelos AET y BC permite una gestión integral y alineada con las mejores prácticas reconocidas internacionalmente, garantizando que las políticas y procedimientos se traduzcan en comportamientos efectivos y sostenidos en el ecosistema conformado por la organización y sus proveedores críticos, como se muestra en la tabla 5.

Tabla 5.

Correspondencia entre ISO/IEC 27002:2022, NIST CSF 2.0 y NIST SP 800-53 con enfoque en proveedores críticos.

Control / Tema	ISO/IEC 27002:2022	NIST CSF 2.0	NIST SP 800-53 (Rev. 5)
Gestión de proveedores	**5.19**	**GV.SC**	SR-3, SA-12
Monitoreo de actividades	**8.16**	**DE.CM**	AU-6, SI-4
Identidad y Autenticación	**8.5**	**PR.AA**	IA-2, AC-2
Criptografía	**8.24**	**PR.DS**	SC-12, SC-13
Inteligencia de amenazas	**5.7**	**ID.RA**	RA-5, PM-15
Concienciación y formación	**6.3**	**PR.AT**	AT-2, AT-3
Respuesta a incidentes	**5.24**	**RS.MA**	IR-1, IR-4
Recuperación ante desastres	**5.30**	**RC.RP**	CP-2, CP-10
Servicios en la nube	**5.23 / 5.21**	**GV.SC**	SA-9, SR-5
Desarrollo seguro	**8.25**	**PR.SD**	SA-11, SA-15

Nota: Se genera de acuerdo con los controles de la ISO/IEC 27002 y NIST CSF 2.0 y SP 800-53.

Normatividad y Estándares para el Modelo de Madurez en Gestión de Proveedores Críticos en TI. En la implementación y desarrollo de un modelo de madurez orientado a la gestión de proveedores críticos en áreas de TI, es fundamental considerar un marco normativo basado en estándares internacionales ampliamente reconocidos que garantizan un enfoque integral de seguridad, cumplimiento y mejora continua.

Entre los principales estándares que sustentan este modelo se encuentran:

- ISO/IEC 27001:2013, que establece los requisitos para un sistema de gestión de seguridad de la información que protege la confidencialidad, integridad y disponibilidad de los datos (ISO/IEC 27001:2022).
- ISO/IEC 27036, que proporciona directrices específicas para la gestión segura de la relación con proveedores, incluyendo selección, evaluación y monitoreo (ISO/IEC 27002:2022).
- Publicación especial del NIST 800-53 Revisión 5, que define controles de seguridad y privacidad aplicables a sistemas federales, enfocados en la protección mediante controles técnicos, administrativos y operacionales (NIST SP 800-53:2020)
- NIST SP 800-161 Revisión 1, que aborda la gestión de riesgos en la cadena de suministro de tecnología de la información, ofreciendo buenas prácticas para reforzar la resiliencia y continuidad (NIST, 2020).
- NIST CSF 2.0. Proporcionar un lenguaje común y una guía flexible para que las organizaciones gestionen y reduzcan el riesgo de ciberseguridad, alineando la estrategia empresarial con la gestión de riesgos tecnológicos (NIST CSF 2.0, 2024)
- COBIT 2019, que ofrece un marco para el gobierno y la gestión de TI, incluyendo la supervisión de proveedores y el alineamiento con los objetivos del negocio (ISACA, 2019).
- Reglamentos y leyes nacionales e internacionales sobre protección de datos y privacidad, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 2016) que

establecen requisitos legales para la gestión de la información y los proveedores.

Estos estándares son pilares esenciales para la construcción de un modelo de madurez que aborde de manera integral las capacidades organizacionales en relación con la seguridad, formación y cumplimiento conductual de proveedores críticos en TI. La combinación de los modelos AET (concienciación, educación, capacitación) y BC (cumplimiento, monitoreo, reconocimiento, mejora continua) se apoya en estos marcos para garantizar resultados efectivos y alineados con las mejores prácticas internacionales.

2.6 Antecedentes de incidentes relevantes.

Diversos incidentes internacionales y latinoamericanos han evidenciado la criticidad de la gestión de proveedores en la seguridad de la información. Por ejemplo, el ataque a la cadena de suministro de SolarWinds en 2020 impactó a miles de organizaciones públicas y privadas a nivel global, demostrando cómo la vulnerabilidad en un proveedor permitió la infiltración masiva de sistemas sensibles (ENISA, 2025).

En América Latina, Colombia ha registrado cifras de alarma: en 2024 se reportaron más de 36.000 millones de intentos de ciberataques, concentrando el 17% de los incidentes de la región y afectando de manera especial al sector salud. (ACIS, 2025). El uso de credenciales comprometidas y el robo de datos configuran los principales vectores de ataque en la región.

Uno de los hallazgos clave en múltiples investigaciones y reportes es que el 74% de las infracciones de seguridad están relacionadas con errores o incumplimientos humanos (ENISA, 2025). Estos incidentes no solo generan pérdidas financieras, sino también daños reputacionales y sanciones regulatorias severas.

Casos documentados en el sector salud, financiero y gubernamental muestran que la falta de alineación entre la cultura organizacional y la actuación real de empleados/proveedores

incrementa la probabilidad de incidentes —por ejemplo, ataques de ransomware facilitados por ingeniería social o la falta de controles básicos por negligencia o desconocimiento de protocolos (Harold, Lee, & Martinez , 2021).

El 77% de las empresas que sufrieron una violación de datos en 2023 atribuyen esta violación a un proveedor comprometido. (SECUREFRAME, 2025).

En particular, incidentes recientes en Colombia han motivado la inclusión en contratos de cláusulas más estrictas sobre capacitación y cumplimiento conductual, auditorías conjuntas y la exigencia de certificaciones en seguridad para el personal de proveedores críticos, buscando mitigar la brecha entre intención y práctica.

2.6.1 *Contexto sectorial de referencia*

Para contextualizar la relevancia del modelo propuesto, se analizaron estadísticas sectoriales como lo muestra la tabla 6, que evidencian la magnitud del desafío en la gestión de seguridad con proveedores:

Tabla 6.

Estadísticas sectoriales de Colombia y Latinoamérica (2024).

Indicador	Colombia	Latinoamérica	Fuente
Organizaciones afectadas por fallos en proveedores	54%	51% promedio regional	(SecureFrame, 2024; ENISA, 2024)
Incidentes con factor humano involucrado	74-95%	74-95%	(SoSafe, 2024; Verizon, 2024)
Intentos de ciberataques reportados	+36,000 millones	~215,000 millones	(CCN-CERT Colombia, 2024; ENISA, 2024)
% de incidentes regionales en Colombia	17%	-	(CCN-CERT Colombia, 2024)
Aumento de ciberataques vs. año anterior	30%	28% promedio	(ENISA, 2024)

Nota: elaboración basada en (ENISA, 2025); (SECUREFRAME, 2024); (CCN-CERT Colombia, 2024).

Estas estadísticas revelan que más de la mitad de las organizaciones experimentan incidentes originados en sus proveedores (SECUREFRAME, 2024) y que el factor humano está presente en la gran mayoría de las brechas de seguridad (Verizon, 2026). Esta realidad

sectorial justifica la necesidad de un modelo integral que aborde tanto los aspectos formativos como conductuales en la gestión de proveedores críticos.

Los principales vectores de ataque identificados en el contexto regional incluyen: robo de credenciales, phishing, ransomware, explotación de vulnerabilidades e ingeniería social, todos ellos con componentes significativos de factor humano que pueden ser mitigados mediante la aplicación sistemática de los elementos (AET+BC) identificados.

2.7 Análisis de Caso de Estudio en la Literatura.

Como parte del Ciclo de Rigor de esta investigación, se analizó el caso de estudio de Lockheed Martin (LM-CIRT) en 2009. (Hutchins, Cloppert, & Amin, 2009), donde se evidencia que la implementación aislada de controles técnicos en proveedores críticos no garantiza la reducción del riesgo humano. Este antecedente permite identificar la necesidad de un modelo que, además de la educación (AET), considere las dimensiones del cumplimiento conductual (BC).

Caso: Aplicación del Modelo de Cadena de Ataque para Fortalecer la Defensa Proactiva del Factor Humano.

A continuación, se explicará en detalle uno de los modelos que enfatiza en la importancia de la conciencia y la capacitación de los usuarios, enfocándose principalmente en el factor humano y su conexión con una defensa activa al tomar acciones proactivas.

Un caso ilustrativo del beneficio de este enfoque es el estudio observado por el Equipo de Respuesta a Incidentes Informáticos de Lockheed Martin (LM-CIRT) en 2009 (Hutchins, Cloppert, & Amin, 2009). Mediante el análisis detallado de las cadenas de eliminación de intrusiones, los defensores lograron detectar y mitigar con éxito tres intentos de intrusión de un adversario, incluso ante una vulnerabilidad de 'día cero'. La conciencia y la capacitación del equipo de respuesta fueron fundamentales, ya que su preparación y conocimiento de nuevas

técnicas de intrusión facilitaron la identificación de comportamientos anómalos y la implementación de acciones estratégicas para proteger la red.

Este enfoque es fundamental para capacitar a empleados y proveedores críticos, ya que al comprender las técnicas, tácticas y procedimientos que utilizan los atacantes, estos actores pueden actuar como una línea de defensa activa, detectando indicios tempranos de intrusión y neutralizando el ataque en cualquier eslabón de la cadena. Un ejemplo paradigmático es el trabajo del Equipo de Respuesta a Incidentes Informáticos de Lockheed Martin en 2009, donde su conocimiento detallado del modelo kill chain facilitó la detección y mitigación exitosa de múltiples intrusiones, incluso frente a vulnerabilidades 'día cero' (Hutchins, Cloppert, & Amin, 2009).

Integrar esta perspectiva estratégica en los programas de concienciación, educación y entrenamiento (modelo AET), junto con la supervisión y refuerzo del cumplimiento conductual (modelo BC), transforma al factor humano en un recurso activo y resiliente frente a ataques deseados. Además, la doctrina F2T2EA (Find, Fix, Track, Target, Engage, Assess) complementa esta visión al ofrecer un marco sistemático para las acciones preventivas y reactivas en cada etapa del ataque, consolidando un enfoque integral que vincula cultura, comportamiento e inteligencia de amenazas (Spitzner, 2016).

En consecuencia, capacitar a los proveedores críticos no solo en políticas y procedimientos, sino también en la comprensión profunda del proceso de ataque, potencia la defensa organizacional y reduce significativamente el riesgo de comprometer la continuidad operativa y la integridad de los activos de información.

2.7.1 Importancia de la Comprensión de la Cadena de Ataque para la Defensa Cibernética.

La comprensión detallada del modelo de la cadena de ataque es fundamental para una defensa cibernética eficaz por varias razones cruciales:

Figura 6.

Cadena de ataque para la defensa cibernética de Lockheed Martin (LM-CIRT) en 2009.



Nota: La figura 6 simboliza el Diagrama de cadena de ataque (kill chain): Representación gráfica con las fases y puntos de intervención para acciones proactivas del factor humano. Fuente: (Vargas, 2021).

Visualización del Proceso de Intrusión: La cadena de ataque ofrece una representación clara y secuencial de las etapas típicas que un atacante debe seguir para lograr sus objetivos en un sistema o red. Esta visualización permite a los defensores entender la progresión de un ataque, desde el reconocimiento inicial hasta la exfiltración de datos o el logro de la persistencia. Al conocer estas fases, los equipos de seguridad pueden anticipar los posibles movimientos de un adversario.

Identificación de Puntos de Interrupción: Cada etapa de la cadena de ataque representa una oportunidad para que los defensores detecten, interrumpan o frustren la intrusión. Al analizar cada fase (reconocimiento, armamentización, entrega, explotación, instalación, comando y control, y acciones sobre los objetivos), las organizaciones pueden identificar los controles de seguridad más efectivos para prevenir el avance del ataque en cada punto. Por ejemplo, una fuerte autenticación y la segmentación de red pueden obstaculizar la fase de movimiento lateral después de una explotación inicial.

Priorización de Controles de Seguridad: No todos los controles de seguridad son igualmente efectivos contra todas las etapas de un ataque. La comprensión de la cadena de ataque ayuda a las organizaciones a priorizar sus inversiones y esfuerzos en aquellos controles que tienen el mayor impacto en la interrupción de las etapas más tempranas o críticas de una intrusión. Por ejemplo, invertir en la concienciación y capacitación de los usuarios puede ser crucial para prevenir la fase de "entrega" a través de phishing.

Detección Temprana de Actividades Maliciosas: Al conocer los indicadores típicos asociados con cada etapa de la cadena de ataque, los equipos de seguridad pueden configurar sus sistemas de monitorización y detección (IDS, SIEM) para identificar actividades sospechosas en las fases iniciales de un ataque, mucho antes de que se produzcan daños significativos. La detección temprana permite una respuesta más rápida y la contención del incidente antes de que se extienda.

Información para la Inteligencia de Amenazas: El análisis de las cadenas de ataque observadas en incidentes reales proporciona información valiosa para la inteligencia de amenazas. Al comprender las tácticas, técnicas y procedimientos (TTPs) comunes utilizados por diferentes tipos de atacantes en cada etapa, las organizaciones pueden mejorar sus capacidades de predicción y adaptación de sus defensas contra amenazas futuras.

Desarrollo de Estrategias de Respuesta a Incidentes: La comprensión de la cadena de ataque es esencial para desarrollar planes de respuesta a incidentes efectivos. Al saber en qué etapa se encuentra un ataque detectado, los equipos de respuesta pueden aplicar los procedimientos más apropiados para contener, erradicar y recuperarse del incidente, evitando una mayor propagación y minimizando el impacto.

Evaluación de la Madurez de la Seguridad: El modelo de la cadena de ataque puede utilizarse como un marco para evaluar la madurez de las capacidades de seguridad de una organización en cada etapa del ciclo de vida de un ataque. Esto permite identificar áreas de fortaleza y debilidad y guiar las mejoras en la postura de seguridad general.

2.7.2 El Rol del Factor Humano (Empleados y Proveedores) en Romper la Cadena de Ataque.

Es común que las discusiones sobre ciberseguridad se centren en las herramientas tecnológicas y las vulnerabilidades de software. Sin embargo, la realidad demuestra que el factor humano es, con frecuencia, el eslabón más vulnerable de la cadena de seguridad, pero también el más crucial en la defensa. En el contexto del modelo de la cadena de ataque, los empleados y, fundamentalmente para esta investigación, los proveedores críticos, no son meros receptores pasivos de amenazas, sino agentes activos que pueden detectar y frustrar un ataque en sus etapas iniciales.

Cada fase de la cadena de ataque, desde el reconocimiento hasta las acciones sobre los objetivos, presenta oportunidades donde la vigilancia, la concienciación y el comportamiento adecuado de las personas pueden marcar la diferencia:

- Prevención en la Fase de Entrega: Muchos ciberataques, especialmente los de amenazas persistentes avanzadas (APT), comienzan con la entrega de malware a través de correos electrónicos de phishing o sitios web maliciosos. Un empleado o proveedor bien capacitado, con la conciencia de seguridad desarrollada, puede identificar señales de alerta en un correo sospechoso o en un enlace fraudulento, evitando hacer clic y rompiendo la cadena antes de que la explotación comience.
- Detección de Explotación e Instalación: Si una explotación ocurre, la observación y el reporte por parte del usuario pueden ser vitales. Un proveedor que nota comportamientos inusuales en sus sistemas o redes, incluso si parecen menores, puede alertar a la organización, permitiendo una investigación temprana. Esto convierte al personal en una especie de "sensor humano" dentro de la red.

- Interrupción del Comando y Control (C2): Tras una intrusión, los atacantes suelen establecer canales de comando y control para mantener el acceso y exfiltrar datos. Un empleado o proveedor que detecte conexiones de red anómalas o que observe actividades inusuales en un dispositivo puede reportarlas, permitiendo que los equipos de seguridad corten la comunicación del atacante y frustren sus objetivos.
- Mitigación de Acciones sobre los Objetivos: Si un atacante logra acceder a los sistemas, sus acciones finales (como el robo de datos o la destrucción de información) pueden ser limitadas si los usuarios y proveedores siguen políticas de seguridad robustas, como la gestión estricta de accesos, el uso de autenticación multifactor o la segmentación de datos. La adhesión a estas prácticas reduce el impacto potencial del ataque.

En esencia, la conciencia, la educación y el entrenamiento transforman a los individuos en la primera línea de defensa. No solo se trata de evitar ser víctimas, sino de entender cómo actúan los atacantes para poder identificar, detener y reportar posibles intrusiones. Esto es aún más crítico cuando se trata de proveedores críticos, ya que un fallo en sus sistemas puede tener un efecto cascada devastador en la organización para la cual se prestan los servicios, comprometiendo no solo datos sino también la continuidad operativa y la reputación. Capacitar y empoderar a este ecosistema de terceros es, por tanto, una estrategia fundamental para fortalecer la postura de seguridad global y aumentar la capacidad de la organización para romper la cadena de ataque en cualquier punto.

Para ilustrar el valor práctico de comprender la cadena de ataque, el estudio de caso observado por el Equipo de Respuesta a Incidentes Informáticos de Lockheed Martin (LM-CIRT) en 2009 es particularmente revelador (Hutchins, Cloppert, & Amin, 2009). En este escenario, los defensores lograron detectar y mitigar con éxito tres intentos de intrusión de un

adversario, incluso cuando estos ataques explotaban una vulnerabilidad de "día cero" previamente desconocida. La clave del éxito radicó no solo en las herramientas técnicas, sino crucialmente en la conciencia y capacitación de los defensores. Su preparación y conocimiento de las tácticas de intrusión les permitió identificar comportamientos anómalos y desplegar acciones estratégicas que cubrieron las brechas de seguridad. Este caso subraya que, a medida que los defensores se capacitan y familiarizan con las nuevas técnicas de ataque, su capacidad para identificar patrones y comportamientos de intrusión desconocidos aumenta exponencialmente.

La lección principal de este y otros incidentes es clara: el modelo de la cadena de ataque, si bien es una herramienta analítica poderosa, alcanza su máximo potencial cuando se conecta directamente con la necesidad de involucrar activamente a los usuarios en la detección y prevención. Los empleados, los proveedores críticos, al estar informados sobre las fases de un ataque y las tácticas comunes de los adversarios, se convierten en una extensión vital de las capacidades de seguridad de la organización. Pueden ser la primera línea de defensa para identificar correos de phishing (fase de entrega), reconocer comportamientos inusuales en sus sistemas (fase de explotación o instalación), o incluso detectar intentos de conexión de comando y control. Al dotar a estos "usuarios" del conocimiento y la capacidad para identificar, detener y/o reportar posibles amenazas, se crea una barrera humana proactiva que complementa las defensas tecnológicas, permitiendo una reacción temprana y efectiva que puede romper la cadena de ataque antes de que los adversarios logren sus objetivos.

2.8 Brechas comunes y limitaciones identificadas en la literatura.

Percepción vs. comportamiento real: Mientras la alta dirección puede asumir la existencia de prácticas robustas, las conductas diarias de empleados y proveedores a menudo no se alinean con las políticas establecidas. El modelo AET puede fortalecer la transferencia de conocimiento mediante actividades de concienciación y entrenamientos dirigidos; el modelo BC

refuerza este aprendizaje mediante auditorías, retroalimentación conductual y refuerzos positivos para cerrar la brecha entre lo esperado y lo realizado.

Cumplimiento normativo vs. conciencia legítima: El cumplimiento formalista de normas o estándares no garantiza la protección si no existe una conciencia real de su importancia. A través de campañas de sensibilización específicas y formación contextualizada (AET), junto con evaluaciones de comprensión y aplicación práctica (BC), se puede fomentar una adherencia consciente y sostenible a las políticas de seguridad (Hu, Maimon, Koh, & Park, 2021).

Expectativas del liderazgo vs. capacidad técnica real: La desconexión entre exigencias directivas y recursos disponibles puede abordarse mediante la alineación de expectativas, comunicación clara de riesgos y limitaciones, y el desarrollo de competencias específicas en los equipos técnicos y de proveedores, asegurando que las metas sean viables y realistas (Merritt, y otros, 2024).

Política escrita vs. cultura organizacional existente: Cuando las políticas de seguridad entran en conflicto con la cultura interna, es esencial involucrar a líderes de opinión y agentes de cambio en programas de concienciación, adaptar los requerimientos a la realidad operativa y promover la participación activa en la elaboración y revisión de controles (Smith & Jones, 2023).

Conocimiento vs. comportamiento diario: El modelo BC permite identificar y corregir la discrepancia entre saber y hacer, utilizando herramientas como simulacros, campañas de refuerzo y métricas de comportamiento observables, mientras que el modelo AET garantiza que la formación se repita y actualice de acuerdo a las amenazas emergentes.

Inversión tecnológica vs. conciencia del factor humano: La efectividad de cualquier solución tecnológica depende del nivel de concienciación y adecuada capacitación del personal que la ópera. El modelo AET proporciona programas escalonados y actualizados de formación,

y el BC garantiza su aplicación mediante seguimiento y mecanismos correctivos ante incumplimientos (ENISA, 2025).

Experiencia laboral vs. adherencia al entrenamiento: La sobre confianza por experiencia previa puede contrarrestarse mediante actualizaciones periódicas, retos prácticos personalizados y feedback constructivo, manteniendo vigente la motivación para respetar rutinas y protocolos (Von Solms & Von Solms, 2004).

Inconsistencias y vacíos de conocimiento: Se identifican y gestionan mediante encuestas, pruebas de conocimientos, análisis de incidentes y auditorías de prácticas cotidianas. El ciclo (AET+BC) permite adaptar los programas de formación y monitoreo a los vacíos específicos detectados, asegurando la mejora continua y la capacidad de respuesta ante amenazas emergentes (Merritt, y otros, 2024).

Impacto del factor humano en incidentes: Como el 74% de las infracciones de seguridad derivadas de errores o incumplimientos humanos (ENISA, 2025), la propuesta refuerza la necesidad de intervención continua tanto en la transferencia de conocimiento como en la influencia sobre actitudes y comportamientos, articulando campañas de sensibilización y entrenamiento con sistemas de monitoreo de cumplimiento y retroalimentación conductual.

Falta de mecanismos de retroalimentación y mejora continua: La propuesta incluye la medición periódica de actitudes, conocimientos y comportamientos, así como el ajuste de las acciones formativas y correctivas, fortaleciendo la cultura de mejora continua y resiliencia (Haney & Lutters, 2024).

La gestión proactiva y la evaluación continua permiten transformar a los proveedores de posibles eslabones débiles en aliados activos y alineados con los objetivos de seguridad de la empresa, tal como lo establecen las mejores prácticas internacionales (NIST SP 800-53:2020).

A partir de la revisión de la literatura y de los marcos normativos y modelos existentes, se evidencia una carencia de propuestas integrales que aborden de forma articulada la concienciación, la educación, la capacitación y el cumplimiento conductual en proveedores

críticos de TI. La mayoría de los enfoques identificados privilegian controles técnicos y evaluaciones formales de cumplimiento, dejando en segundo plano la dimensión cultural y comportamental del factor humano. Este vacío justifica la necesidad de un modelo integrado que permita fortalecer la cultura de seguridad compartida y gestionar de manera más efectiva los riesgos en la cadena de suministro digital. Con esta base teórica en firme, el siguiente capítulo detalla el diseño arquitectónico y la integración metodológica de los elementos AET y BC en el modelo propuesto.

2.9 Arquitectura de Gestión de Riesgos

La arquitectura de referencia propuesta se fundamenta en la convergencia de marcos internacionales de ciberseguridad, como NIST CSF 2.0 e ISO/IEC 27001:2022, y modelos de psicología organizacional aplicados a la seguridad de la información. Esta estructura no se limita a la implementación de controles técnicos perimetrales, sino que adopta un enfoque sociotécnico diseñado para mitigar los riesgos derivados de la interacción humana y la cadena de suministro. A través de una jerarquía de tres capas (Estratégica, Táctica y Operativa), el modelo permite alinear las políticas de gobernanza con el comportamiento real de los colaboradores y proveedores críticos. De este modo, la arquitectura trasciende el cumplimiento documental para enfocarse en la efectividad operativa, integrando dimensiones de Concientización, Educación y Entrenamiento (AET) como motores de un Comportamiento y Cumplimiento (BC) verificable, en conjunto con el control de "Concienciación y formación" (ISO 6.3 / NIST PR.AT), que es el disparador de las métricas de cumplimiento conductual en la capa operativa, garantizando que la seguridad sea una capacidad dinámica y no un estado estático de la organización.

- Capa Estratégica: Basada en ISO/IEC 27001:2022 para el cumplimiento normativo y legal (GDPR).

- Capa Táctica: Evaluación de proveedores y servicios (Cloud/MSP) mediante matrices de criticidad y puntuación de riesgo.
- Capa Operativa/Humana: Implementación del ciclo AET -> BC para garantizar que los controles técnicos no sean vulnerados por fallos en la cultura organizacional.

La gestión de riesgos de la seguridad de la información es un proceso iterativo que incluye el establecimiento del contexto, la valoración del riesgo, el tratamiento del riesgo, la aceptación del riesgo y la comunicación del riesgo. (ISO/IEC 27001:2022).

2.9.1 Arquitectura de Confianza Cero (Zero Trust Architecture - ZTA)

Basada en el estándar NIST SP 800-207, esta arquitectura es la respuesta moderna a la seguridad de perímetros diluidos (Nube y MSPs).

Principio: "Nunca confiar, siempre verificar".

Aplicación en Riesgo de Terceros: Resulta fundamental al evaluar cómo los proveedores de servicios gestionados acceden a la infraestructura crítica. No se valida al usuario por su ubicación, sino por una evaluación dinámica de su postura de seguridad. La gestión de riesgos de la cadena de suministro de ciberseguridad (C-SCRM) es el proceso de identificar, evaluar y mitigar los riesgos asociados con la naturaleza distribuida y compleja de los productos y servicios de TI/TO. y comportamiento. (NIST CSF, 2022).

En consecuencia, los fundamentos teóricos recolectados en este capítulo proporcionan el sustento necesario para el desarrollo del Modelo de Buenas Prácticas en SI para Proveedores Críticos (MBP-SI-PC). Este modelo no solo se apoya en los estándares robustos previamente analizados, sino que propone una estructura de capas (Gobernanza, Ejecución y Verificación) diseñada para mitigar las debilidades operativas observadas en el ecosistema de ciberseguridad actual.

3. DISEÑO Y DESARROLLO DE LA INTEGRACIÓN DEL MODELO (AET+BC) PARA PROVEEDORES CRÍTICOS EN TI.

3.1. Introducción al modelo integrado (AET+BC)

El Modelo de Buenas Prácticas en Seguridad de la Información para Proveedores Críticos de TI (MBSI-PC) surge como respuesta a las limitaciones identificadas en los enfoques tradicionales de gestión de proveedores, los cuales tienden a privilegiar controles técnicos y contractuales sin abordar de manera explícita el comportamiento humano y la cultura organizacional compartida.

Los hallazgos del análisis previo muestran que una proporción relevante de los incidentes de seguridad involucra fallos conductuales, tales como el incumplimiento de políticas, errores operativos o una comprensión insuficiente de los riesgos asociados al acceso privilegiado a sistemas e información crítica. Estos factores evidencian la necesidad de un modelo que no solo defina qué controles deben existir, sino cómo deben ser interiorizados y aplicados por quienes participan en la cadena de suministro digital.

En este contexto, el modelo propuesto integra los componentes de Concienciación, Educación y Capacitación (AET) con mecanismos de Cumplimiento Conductual (BC), estableciendo una relación directa entre el aprendizaje organizacional y la observación del comportamiento real. La integración no se concibe como una suma de elementos aislados, sino como una arquitectura coherente orientada a generar cambios sostenibles en la cultura de seguridad de los proveedores críticos.

El diseño del modelo se apoya en estándares internacionales reconocidos y en principios de mejora continua, incorporando métricas que permiten evaluar su efectividad y adaptar el nivel de intervención según el riesgo y el desempeño del proveedor. De esta manera, el MBSI-PC busca fortalecer la resiliencia organizacional, reduciendo la probabilidad y el impacto de incidentes asociados al factor humano en entornos de TI críticos.

3.1.1 Fundamentación del Modelo

El modelo se fundamenta en cuatro pilares teórico-prácticos:

Base Normativa: Alineación con ISO 27001:2022, ISO 27002:2022 y NIST CSF 2.0 y SP 800-53 Rev 5.

Base Empírica: Hallazgos del proyecto que demuestran una correlación de 0.72 entre capacitación y cumplimiento.

Base Conductual: Principios de psicología organizacional para el cambio de comportamiento.

Base Sistémica: Enfoque de mejora continua, basado en el ciclo PDCA (Plan-Do-Check-Act).

Como se menciona en el objetivo general de la propuesta, al integrar ambos modelos va a permitir: asegurar la formación, concienciación y educación continua del personal que labora en proveedores críticos de TI, fortaleciendo su comprensión de los riesgos y su rol en la seguridad. Adicionalmente, generar un apalancamiento efectivo en el comportamiento de cumplimiento de estos proveedores, transformando el conocimiento en acciones seguras y responsables.

Integración de los modelos AET y BC alineados a la hipótesis planteada. La integración de los modelos AET (Awareness, Education, Training) y BC (Behavior Compliance) está directamente alineada con los objetivos específicos de esta tesis y constituye la base conceptual y metodológica para responder a la pregunta principal de este proyecto y validar la hipótesis.

Hipótesis central: La aplicación sistemática de un modelo integrado (AET+BC) mejora significativamente la adherencia a políticas, reduce incidentes derivados del factor humano y promueve un alineamiento cultural efectivo entre la organización y sus proveedores críticos.

Esta integración reconoce que no basta con elevar el conocimiento o la concienciación (AET) si no se generan y mantienen comportamientos seguros y sostenidos en el tiempo (BC), especialmente en un entorno donde la heterogeneidad y la distancia operativa con proveedores críticos pueden favorecer la aparición de brechas culturales y conductuales.

Las preguntas específicas relacionadas con la efectividad de programas de formación, la influencia del factor humano en incidentes de seguridad y la alineación cultural entre la organización y sus proveedores son atendidas mediante el diseño de intervenciones que combinan sensibilización, educación formal, entrenamiento práctico y mecanismos de seguimiento y retroalimentación conductual. Esto permite evaluar la hipótesis de que la combinación (AET + BC) contribuirá a reducir las desviaciones conductuales y, al final, disminuir incidentes asociados al factor humano.

Asimismo, la articulación del modelo con la medición de resultados cognitivos (aprendizaje, conocimiento técnico y normativo) y conductuales (cumplimiento, reporte de incidentes, adherencia a políticas) facilita la validación práctica de las situaciones asociadas a la mejora continua y sostenibilidad cultural en seguridad. De esta forma, el modelo se conecta directamente con la necesidad de proveer indicadores que evidencien el impacto real de las acciones implementadas, cubriendo tanto la dimensión individual como colectiva.

Finalmente, la propuesta enfatiza la importancia de un enfoque integrado de gestión de riesgos que contempla aspectos técnicos, humanos y culturales, mostrando que la seguridad en la relación con proveedores críticos debe incluir tanto controles normativos y tecnológicos como una sólida cultura organizacional compartida. Esto responde directamente a la hipótesis, que señala que un modelo integral que incorpora (AET+BC) será más efectivo que iniciativas aisladas para mejorar la postura de seguridad y resiliencia organizacional.

En síntesis, la propuesta integradora (AET+BC) no solo da respuesta conceptual a la pregunta de este proyecto, sino que también estructura un marco metodológico para validar la

hipótesis, lo que permite orientar la toma de decisiones y la gestión estratégica en un contexto real y complejo, como la interacción con proveedores críticos de TI.

3.2. Determinación de elementos críticos de los modelos (AET + BC).

El análisis documental permitió identificar y caracterizar siete elementos fundamentales que conforman el modelo integrado (AET+BC) (Awareness, Education, Training + Behavior Compliance), organizados en dos dimensiones complementarias pero interdependientes que resultan críticas para la gestión de seguridad con proveedores de TI. La integración de ambos modelos no es una simple yuxtaposición de componentes, sino una arquitectura sinérgica donde los elementos formativos (AET) establecen la base cognitiva y de habilidades, mientras que los elementos conductuales (BC) aseguran la aplicación sostenida, la medición y la evolución cultural necesaria para una gestión efectiva de la seguridad con proveedores críticos, tal cual se muestra en la tabla 7.

Tabla 7.

Mapeo de Elementos Críticos de los Modelos AET y BC

Mapeo de Elementos Críticos de los Modelos AET y BC				
Modelo	**Elemento**	**Principio**	**Componentes / Directrices Fundamentales**	**Objetivo / Impacto**
AET	Concienciación	Captar atención y crear comprensión básica sobre riesgos y responsabilidades.	- Comunicación constante y relevante (emails, posters, banners) - Enfoque en el "por qué" (consecuencias directas) - Contenido variado y atractivo (videos, infografías, juegos)	Sensibilizar rápidamente y mantener alerta al personal.
AET	Educación	Proporcionar conocimiento profundo y contextualizado sobre seguridad.	- Contenido estructurado y teórico (módulos sobre criptografía, ingeniería social, etc.)	Facilitar la comprensión y el razonamiento sobre políticas.

Mapeo de Elementos Críticos de los Modelos AET y BC

Modelo	Elemento	Principio	Componentes / Directrices Fundamentales	Objetivo / Impacto
AET	Capacitación	Desarrollar habilidades prácticas para aplicar conocimientos en situaciones reales.	- Contextualización por roles - Recursos accesibles (manuales, guías) - Entrenamiento práctico basado en roles (simulaciones, talleres) - Refuerzo y retroalimentación inmediata - Evaluación de habilidades prácticas	Garantizar la aplicación efectiva y correcta del conocimiento.
BC	Cumplimiento	Definir claramente los comportamientos esperados en seguridad.	- Políticas accesibles y comprensibles - Procedimientos operativos estándar (SOPs) - Roles y responsabilidades definidas	Asegurar que todos conozcan y comprendan sus obligaciones.
BC	Monitoreo y medición	Observar y registrar el cumplimiento de comportamientos de seguridad.	- Auditorías y revisiones regulares - KPIs sobre comportamiento seguro (ej. tasa de clics en phishing, uso de MFA) - Canales para reporte de incidentes	Detectar brechas y medir adherencia a políticas.
BC	Reconocimiento y consecuencias	Promover comportamientos deseados y desincentivar los no deseados.	- Feedback constructivo - Reconocimiento e incentivos - Consecuencias claras y consistentes - Cultura de "No Blame" para reporte de errores	Fomentar el compromiso y el aprendizaje continuo.
BC	Mejora Continua	Integrar la seguridad como valor fundamental impulsado por la alta dirección.	- Liderazgo visible y activo - Integración en misión, visión y valores	Consolidar una cultura organizacional de seguridad.

Mapeo de Elementos Críticos de los Modelos AET y BC				
Modelo	**Elemento**	**Principio**	**Componentes / Directrices Fundamentales**	**Objetivo / Impacto**
			- Comunicación bidireccional abierta	

Nota: elaboración propia basada en las dimensiones de los modelos AET y BC.

3.3 Características para Proveedores Críticos.

El modelo reconoce diferentes categorías de proveedores críticos (véase la tabla 8), cada una con características y necesidades específicas:

Tabla 8.

Características y controles por tipo de proveedor.

Tipo de Proveedor Crítico	Características Clave	Controles Prioritarios
Acceso a sistemas y datos sensibles	Proveedores con acceso privilegiado a sistemas operativos, bases de datos, aplicaciones críticas	- Gestión de identidades (IAM) - MFA obligatorio - Registro y monitoreo exhaustivo
Desarrollo y mantenimiento	Proveedores que desarrollan, modifican o mantienen aplicaciones y sistemas	- Secure coding practices - Revisiones de código - Ambientes segregados
Gestión de infraestructura	Proveedores que administran infraestructura cloud, redes o hardware crítico	- Hardening de sistemas - Gestión de configuraciones - Monitoreo continuo
Servicios profesionales	Consultores y asesores con acceso a información estratégica	- NDAs reforzados - Acceso basado en proyectos - Auditorías de cumplimiento

Nota: elaboración basada en (ISO/IEC 27001:2022) e (NIST CSF 2.0, Febrero 26, 2024).

Para la aplicación efectiva del modelo (AET+BC), es imperativo delimitar las características que definen a un proveedor como 'crítico', ver tabla 9. Esta categorización no

solo responde al volumen de facturación, sino a la naturaleza del activo de información gestionado y al impacto potencial en la resiliencia organizacional ante una materialización de riesgos en la cadena de suministro.

Tabla 9.

Características que definen a un proveedor como 'crítico'.

Categoría de criticidad	Características Clave (Criterios de Selección)	Nivel de Madurez Sugerido	Alineación Normativa (ISO/NIST)	Impacto en el Modelo (AET+BC)
Acceso a datos sensibles	Proveedores con acceso a PII (Información de Identificación Personal), datos financieros o secretos industriales.	**Nivel 4 (Gestionado)**	**ISO 27001:** Control A.8.11 (Privacidad). **NIST:** ID.GV-3.	Requiere BC estricto para evitar fugas de información por ingeniería social.
Conectividad e infraestructura	Proveedores con túneles VPN, acceso a nubes privadas o administración de activos de red.	**Nivel 4 o 5 (Optimizado)**	**ISO 27001:** Control A.8.20 (Seguridad en redes). **NIST:** PR.AC-3.	Exige AET especializado en privilegios mínimos y gestión de identidades.
Continuidad del negocio	Servicios cuya caída detiene la operación (SLA > 99.9%), como MSPs o Cloud Providers.	**Nivel 3 (Definido) mín.**	**ISO 27001:** Control A.5.30 (Continuidad). **NIST:** PR.IP-9.	Foco en BC para respuesta ante incidentes y comunicación de crisis.
Cumplimiento legal / regulatorio	Proveedores sujetos a auditorías externas, leyes de protección de datos o normatividad bancaria.	**Nivel 3 (Definido)**	**ISO 27001:** Control A.5.36 (Cumplimiento). **NIST:** ID.GV-3.	AET enfocado en la responsabilidad legal y ética del manejo de información.

Nota: elaboración basada en los estándares (ISO/IEC 27001:2022) y (NIST CSF 2.0, 2024).

Esta tabla actúa como el **"Filtro de Entrada"** para decidir a qué proveedores se les aplicará el ciclo completo de intervención del modelo (AET+BC).

3.4 Compromiso de Cultura y Seguridad Conductual (AET+BC) en Proveedores Críticos según estándares ISO/NIST.

La gestión de la seguridad en la cadena de suministro digital exige una transición desde modelos de cumplimiento estático hacia marcos de gobernanza dinámica centrados en el factor humano. En este contexto, el presente apartado establece los lineamientos de cumplimiento para proveedores críticos, integrando los dominios de la norma ISO/IEC 27001 y el NIST CSF con los pilares del modelo (AET+BC).

3.4.1 Cláusula de Compromiso en Cultura de Seguridad y Gestión Conductual (Modelo AET+BC)

1. Alcance y Obligatoriedad (AET):

El PROVEEDOR se compromete formalmente a diseñar, implementar y mantener un programa robusto de Concienciación, Educación y Capacitación (AET). Este programa debe estar alineado con el control 6.3 de ISO/IEC 27001:2022 y las directrices del NIST CSF (PR.AT), garantizando una cobertura de ejecución verificable de al menos el 90% de la población asignada a la prestación del servicio. Los registros de asistencia y las métricas de aprobación de evaluaciones de conocimiento deberán estar a disposición de la organización para fines de auditoría.

2. Gestión del Cumplimiento Conductual (BC):

Complementariamente, el PROVEEDOR garantizará la transferencia de la política a la práctica mediante la gestión del Cumplimiento Conductual (BC). Esto implica no solo la adhesión formal a las políticas de seguridad (conforme al control 5.10 de ISO/IEC 27001), sino también la aceptación de que el desempeño de sus colaboradores será evaluado mediante indicadores de comportamiento real y ejercicios periódicos de simulacros de ingeniería social.

3. Correlación con la Gestión de Riesgos y Elasticidad Contractual:

El desempeño cultural del proveedor se integrará directamente en su Evaluación de Desempeño y Gestión de Riesgos. Los resultados obtenidos en los pilares AET y BC alimentarán el Indicador VSS (Vendor Security Score) definido en el modelo de la organización.

Esta cláusula posee un carácter "Elástico y Dinámico": la rigurosidad, periodicidad y profundidad de los controles de seguridad conductual se ajustarán de forma automática y proporcional al posicionamiento del proveedor en la Matriz de Criticidad y Riesgo según el (Mapa de Calor). Ante un incremento en el nivel de riesgo inherente o un deterioro en los indicadores de comportamiento, el PROVEEDOR acepta la aplicación de controles compensatorios más estrictos y una supervisión técnica intensificada, de acuerdo con los protocolos de intervención del Modelo (AET+BC). Esto se aplica bajo el marco de la Ley 1581 de 2012 en Colombia, especialmente si el proveedor maneja datos personales, para dar cumplimiento al principio de responsabilidad demostrada (Accountability).

3.5 Principales causas de las desviaciones asociadas a las prácticas inseguras de los proveedores.

La comprensión cualitativa de los vacíos de seguridad específicos de proveedores críticos es fundamental dada la criticidad en la continuidad de los servicios y la protección de datos de las organizaciones de TI. Por lo anterior, la identificación de las causas raíces de las prácticas inseguras por parte de los proveedores en entornos de TI es crítica, véase la tabla 10, ya que busca la mitigación efectiva de los riesgos; no es solo corregir un error superficial, sino evitar que vuelva a ocurrir. Identificar la causa permite implementar un control preventivo que solucione la raíz del problema, lo cual es la esencia de la gestión de riesgos.

Tabla 10.

Discrepancias o desviaciones en la cultura de seguridad de la información.

Discrepancia	Descripción de la Brecha	Riesgo Potencial y Ejemplo
Percepción vs. Comportamiento	La alta dirección cree que las políticas de seguridad se siguen, pero en la práctica, empleados y proveedores las ignoran por conveniencia o informalidad.	Anulación de políticas formales. Ejemplo: Ignorar una política de no compartir contraseñas.
Cumplimiento Normativo vs.	La organización cumple con estándares (ej. ISO/IEC	Cumplimiento frágil y vulnerable. Ejemplo: Adherencia a una regulación sin

Discrepancia	Descripción de la Brecha	Riesgo Potencial y Ejemplo
Conciencia de Seguridad	27001) de manera formal, sin que el personal comprenda la importancia estratégica de estas medidas.	entender por qué es vital para la protección de datos.
Liderazgo vs. Capacidad Técnica Real	Las expectativas de seguridad de la alta dirección son inalcanzables debido a la falta de recursos técnicos, personal cualificado o infraestructura adecuada.	Falsa sensación de seguridad. Ejemplo: Esperar una protección absoluta contra todas las amenazas sin contar con las herramientas o el personal necesario.
Política de Seguridad vs. Cultura Organizacional	Las políticas de seguridad chocan con la cultura predominante, como una cultura de agilidad que ve los procesos de seguridad como obstáculos burocráticos.	Evasión e ineficacia de las políticas. Ejemplo: Omitir pasos de aprobación en los flujos de trabajo por ser "demasiado lentos".
Conocimiento vs. Comportamiento Diario	Empleados y proveedores conocen las mejores prácticas de seguridad, pero no las aplican en sus tareas diarias por descuido o pereza.	Vulnerabilidad crítica. Ejemplo: Abrir un correo electrónico sospechoso a pesar de saber que no se debe.
Inversión Tecnológica vs. Factor Humano	Se invierte en tecnología de seguridad de vanguardia (SIEM, EDR) sin considerar la concientización del personal, que es el eslabón más débil.	Ineficacia de la inversión tecnológica. Ejemplo: Un firewall avanzado no puede mitigar el riesgo si un empleado es víctima de un ataque de phishing.
Experiencia vs. Adherencia a Políticas	El personal experimentado desarrolla una sobre confianza, creyendo que las políticas de seguridad son innecesarias para su nivel de pericia.	Evasión de procedimientos establecidos. Ejemplo: Un proveedor de TI con experiencia elude un proceso de autenticación por considerarlo redundante.

Nota: elaboración propia basada en la literatura sectorial. (Jimenez, 2024).

Una práctica insegura en un proveedor puede transferir un riesgo masivo a la organización (acceso no autorizado, incumplimiento normativo). Al identificar la causa, proteges tu ecosistema antes de que el riesgo se materialice. Al conocer las causas, puedes diseñar programas de Awareness, Education, and Training (AET) y de Behavior Compliance (BC) que aborden las debilidades humanas específicas de los proveedores que prestan servicios en funciones críticas en entornos de TI.

La identificación de las principales causas de las desviaciones asociadas a prácticas inseguras por parte de proveedores críticos en entornos de TI permite comprender con mayor

profundidad las vulnerabilidades estructurales que afectan la seguridad de la información organizacional. A través del análisis de discrepancias culturales, conductuales y operativas, se evidencia que dichas desviaciones no solo responden a fallas técnicas, sino a incongruencias entre la intención declarada y la práctica efectiva, lo que amplifica el riesgo en la cadena de suministro digital y constituyen la causa raíz que explica la materialización de riesgos operativos, legales y reputacionales en los entornos de TI.

3.5.1 Inconsistencias y riesgos en la gestión de proveedores críticos.

El riesgo en la cadena de suministro es la amenaza más sofisticada hoy en día, donde un atacante compromete a un proveedor pequeño para llegar a sus grandes clientes. Al identificar las inconsistencias en sus prácticas de seguridad, puedes evaluar si ese proveedor es un vector de ataque, permitiéndote tomar medidas como reforzar los controles contractuales y técnicos; véase la tabla 11.

Tabla 11.

Riesgos e impactos en la gestión de proveedores en entornos de TI.

Activo / Función Crítica	Riesgo específico	Elemento Crítico AET / BC	Control ISO 27002 (Anexo A)	Control NIST SP 800-53	Impacto / Consecuencia	Medidas / Controles Mitigantes
Administración de plataformas de usuarios	Acceso no autorizado por desconocimiento o negligencia	Concienciación (AET) / Expectativas claras (BC)	A.9.2 Gestión de acceso de usuarios	AC-2 Gestión de cuentas	Compromiso de cuentas, pérdida de confidencialidad	Programas continuos de concienciación, políticas claras, 2MFA, revisión periódica de accesos
	Errores operativos por falta de habilidades prácticas	Capacitación (AET) / Refuerzo y consecuencias (BC)	A.12.1 Procedimientos operativos	CM-3 Gestión de cambios	Fallos en configuración, interrupciones de servicio	Entrenamientos basados en roles, simulaciones prácticas, auditorías de procesos
	Incumplimiento de políticas por	Educación (AET) / Monitoreo	A.5.1 Políticas de seguridad	PL-2 Políticas y	Riesgo de fugas o mal	Formación estructurada,

Activo / Función Crítica	Riesgo específico	Elemento Crítico AET / BC	Control ISO 27002 (Anexo A)	Control NIST SP 800-53	Impacto / Consecuencia	Medidas / Controles Mitigantes
	desconocimiento	y medición (BC)		procedimientos	uso de sistemas.	evaluaciones periódicas, KPI´s de cumplimiento
	Elevación de privilegios por desconocimiento de roles	Concienciación y Capacitación (AET) / Expectativas claras (BC)	A.9.4 Gestión de derechos de acceso	AC-6 Principio de privilegios mínimos	Acceso indebido a datos sensibles	Capacitación específica, asignación clara de roles, monitoreo de accesos privilegiados
Bases de datos (BD)	Vulnerabilidades técnicas explotadas por falta de entrenamiento	Capacitación (AET) / Monitoreo y medición (BC)	A.12.6 Gestión de vulnerabilidades técnicas	RA-5 Gestión de vulnerabilidades	Exposición a ataques y pérdida de integridad	Programas de formación en gestión de vulnerabilidades, escaneo y parcheo continuo
	Fallas en respuesta a incidentes	Educación (AET) / Refuerzo y consecuencias (BC)	A.16 Gestión de incidentes	IR-4 Respuesta a incidentes	Mayor impacto y tiempo de recuperación	Simulacros de incidentes, capacitación en respuesta, cultura de reporte sin culpa
Sistemas Operativos (SO)	Instalación de software no autorizado	Concienciación (AET) / Monitoreo y medición (BC)	A.12.5 Control de software en producción	CM-7 Control de software	Introducción de malware o configuraciones inseguras	Formación práctica, auditorías de software, políticas estrictas de instalación.
	Falta de actualización y parcheo	Educación (AET) / Monitoreo y medición (BC)	A.12.6 Gestión de vulnerabilidades técnicas	SI-2 Remediación de fallas	Explotación de vulnerabilidades conocidas	Capacitación en gestión de parches, monitoreo automatizado, KPI´s de cumplimiento de

Activo / Función Crítica	Riesgo específico	Elemento Crítico AET / BC	Control ISO 27002 (Anexo A)	Control NIST SP 800-53	Impacto / Consecuencia	Medidas / Controles Mitigantes
						actualizaciones
	Incumplimiento en registros y monitoreo	Expectativas claras (BC) / Monitoreo y medición (BC)	A.12.4 Registros y supervisión	AU-2 Registro de auditoría	Dificultad para detectar y analizar incidentes	Políticas claras, formación en monitoreo, auditorías regulares

Nota: elaboración (ISO/IEC 27001:2022); (NIST SP 800-53:2020).

Al vincular cada discrepancia con riesgos específicos, como se muestra en las tablas anteriores, se establece una trazabilidad directa entre el comportamiento inseguro y sus consecuencias potenciales. Esta articulación permite no solo comprender el origen de las desviaciones, sino diseñar estrategias de mitigación efectivas, basadas en programas de concienciación, educación y entrenamiento (AET), así como en mecanismos de cumplimiento conductual (BC). En este sentido, la identificación de causas no es un fin en sí misma, sino un paso esencial para transformar debilidades latentes en oportunidades de control, mediante el feedback oportuno fortaleciendo así la postura de seguridad organizacional frente a un entorno de amenazas dinámicas y sofisticadas.

En conclusión, identificar estas inconsistencias y vacíos en la seguridad de la información respecto a sus aliados es esencialmente un ejercicio de debida diligencia y gestión proactiva que transforma una amenaza potencial en una debilidad conocida que puede ser activamente controlada y mitigada.

3.6 Evaluación documental de prácticas actuales bajo estándares ISO/NIST.

3.6.1 Análisis de controles ISO 27002 y NIST

El mapeo de controles recomendados por los frameworks internacionales revela la cobertura actual y las áreas de oportunidad con medidas mitigantes, como se muestra en la tabla 12:

Tabla 12.

Mapeo de controles y medidas mitigantes.

Función Crítica	Control ISO 27002	Control NIST SP 800-53	Medidas Mitigantes Recomendadas
Administración de plataformas	A.9.2 Gestión de acceso de usuarios	AC-2 Gestión de cuentas	MFA, revisión periódica de accesos, programas de concienciación
Gestión operativa	A.12.1 Procedimientos operativos	CM-3 Gestión de cambios	Entrenamientos basados en roles, simulaciones prácticas
Cumplimiento normativo	A.5.1 Políticas de seguridad	PL-2 Políticas y procedimientos	Formación estructurada, evaluaciones periódicas
Gestión de vulnerabilidades	A.12.6 Gestión de vulnerabilidades	SI-2 Corrección de defectos	Proceso de parcheo definido, capacitación técnica
Gestión de incidentes	A.16.1 Gestión de incidentes	IR-4 Manejo de incidentes	Planes de respuesta, simulacros regulares
Desarrollo seguro	A.14.2 Desarrollo seguro	SA-11 Pruebas de software	Secure coding training, revisiones de código
Monitoreo y auditoría	A.12.4 Registro y monitoreo	AU-12 Generación de auditoría	Herramientas SIEM, análisis de logs

Nota: elaboración basada en (ISO/IEC 27001:2022); (NIST SP 800-53:2020).

3.6.2 Evaluación cualitativa de efectividad.

La evaluación cualitativa de la efectividad para proveedores críticos se fundamenta en una matriz de madurez (Ver Tabla 13) que integra los dominios de control de la norma **ISO/IEC 27001** con los perfiles de implementación (**Tiers**) del marco **NIST CSF**. Esta estructura permite trascender la verificación documental estática, categorizando el desempeño del proveedor en cinco niveles que van desde una gestión reactiva e incipiente hasta la excelencia optimizada. Al alinear estos estándares con las dimensiones de **Concienciación (AET)** y **Cumplimiento Conductual (BC)**, el modelo facilita la identificación de brechas culturales y operativas, permitiendo que la organización determine si el proveedor posee la resiliencia necesaria para gestionar activos de información críticos o si requiere intervenciones tácticas inmediatas para alcanzar un nivel de madurez predecible y gestionado.

Tabla 13.

Niveles de madurez integrados (ISO 27001 / NIST CSF / Modelo AET+BC) para la evaluación de proveedores críticos según el nivel de madurez.

Nivel	Denominación	Relación con NIST / ISO	Característica del Proveedor Crítico	Enfoque AET + BC (Cultura y Comportamiento)
1	**Incipiente (Tier 1)**	**NIST:** Parcial. **ISO:** No alineado.	La seguridad es reactiva. No existen políticas formales para la cadena de suministro.	**AET:** Información informal. **BC:** El cumplimiento es aleatorio y depende de la buena voluntad.
2	**En Desarrollo (Tier 2)**	**NIST:** Riesgo Informado. **ISO:** Planificación básica.	Hay conciencia de los riesgos, pero los controles se aplican de forma inconsistente entre áreas.	**AET:** Charlas esporádicas. **BC:** Se siguen reglas por miedo a la sanción, no por convicción.
3	**Definido (Tier 3)**	**NIST:** Repetible. **ISO:** Operación y Control.	Se cumple con los controles de **ISO 27001.** Existen procesos documentados y aprobados por la dirección.	**AET:** Programa de formación anual. **BC:** Comportamiento estandarizado; se reportan incidentes básicos.
4	**Gestionado / Predecible (Tier 4)**	**NIST:** Adaptativo. **ISO:** Evaluación de desempeño.	Monitoreo continuo. El proveedor utiliza métricas para ajustar sus controles según las amenazas actuales.	**AET:** Capacitación basada en roles críticos. **BC:** Alta resiliencia; los empleados identifican ataques complejos (Phishing/Ing. Social).

Nivel	Denominación	Relación con NIST / ISO	Característica del Proveedor Crítico	Enfoque AET + BC (Cultura y Comportamiento)
5	**Excelencia / Optimizado**	**NIST:** Dinámico. **ISO:** Mejora Continua.	La seguridad es parte de la estrategia de negocio. Alineación total con el ciclo PDCA de ISO.	**AET:** Cultura de ciberseguridad integrada. **BC:** Cumplimiento instintivo; el personal propone mejoras proactivamente.

Nota: adaptación basada en los niveles de madurez de CMMI, alineada con los Tiers de (NIST CSF 2.0, 2024) y los dominios de mejora continua de (ISO/IEC 27001:2022).

La revisión de mejores prácticas internacionales y estándares del sector sugiere que la efectividad de los controles técnicos se ve significativamente limitada cuando no están acompañados de componentes formativos y conductuales apropiados (Alshaikh, 2020). La literatura especializada indica consistentemente que:

Los controles técnicos por sí solos abordan solo una fracción de los vectores de ataque.

El análisis comparativo con frameworks reconocidos como COBIT 2019 (ISACA, 2019), ITIL 4 (AXELOS, 2019) y el modelo de madurez de capacidades CMMI v2.0 (ISACA, 2020) refuerza la necesidad de un enfoque holístico que combine los elementos identificados en los modelos AET y BC.

3.6.3 Análisis conceptual del impacto potencial en la evaluación de proveedores.

Impactos esperados.

El análisis documental sugiere impactos potenciales (véase la tabla 14) diferenciados según el elemento aplicado, tal como se presenta en la siguiente tabla basada en el mapeo conceptual realizado:

Tabla 14.

Impactos conceptuales en la evaluación de proveedores.

Modelo	Elemento	Impacto Específico en Evaluación de Proveedores	Impactos Relacionados
AET	Concienciación	Sensibiliza a proveedores sobre riesgos y responsabilidades, potencialmente reduciendo errores por desconocimiento o negligencia mediante comunicación continua y relevante	Fortalecimiento cultural, reducción de riesgos
AET	Educación	Facilita la comprensión profunda y contextual de políticas de seguridad, promoviendo alineación con normas internas y regulatorias específicas para proveedores	Mejora en cumplimiento, optimización operativa
AET	Capacitación	Desarrolla habilidades prácticas en los proveedores para aplicar controles y políticas, aumentando potencialmente la efectividad en la mitigación de riesgos operativos	Reducción de riesgos, fortalecimiento cultural
BC	Cumplimiento	Establece claramente obligaciones y comportamientos esperados, asegurando que los proveedores conozcan requisitos contractuales y de seguridad	Mejora en cumplimiento, gestión alineada con estándares
BC	Monitoreo y Medición	Proporciona mecanismos para auditar el cumplimiento de políticas por parte de proveedores, permitiendo la detección temprana de brechas y desviaciones	Mitigación de riesgos asociados a terceros
BC	Reconocimiento y Consecuencias	Incentiva el cumplimiento mediante feedback e incentivos, fortaleciendo el compromiso de proveedores	Fortalecimiento cultural, mejora continua
BC	Mejora Continua	Promueve el liderazgo activo y la cultura compartida de seguridad, asegurando que la gestión de proveedores sea dinámica	Optimización operativa continua

Nota: Estos impactos representan proyecciones teóricas basadas en la literatura revisada y las mejores prácticas del sector, no mediciones prácticas validadas.

3.6.4 Brechas identificadas en la relación con los proveedores.

A través del análisis documental, se identifican las siguientes brechas conceptuales en las prácticas actuales de gestión de proveedores:

Brecha de Integración: Existe una desconexión entre los programas de formación (cuando existen) y los mecanismos de refuerzo conductual. Las organizaciones típicamente implementan capacitaciones aisladas sin sistemas de seguimiento o refuerzo continuo.

Brecha de Personalización: Los programas de seguridad tienden a ser genéricos, sin considerar las características específicas de diferentes tipos de proveedores, sus niveles de criticidad o sus contextos operativos particulares.

Brecha de Medición: La ausencia de métricas claras y sistemas de medición impide evaluar la efectividad real de las iniciativas de seguridad, resultando en inversiones no optimizadas y mejoras no cuantificables.

Brecha Cultural: La seguridad se percibe frecuentemente como una imposición regulatoria o técnica, en lugar de un valor organizacional compartido, limitando la adopción efectiva de prácticas seguras.

3.7 Identificación de Riesgos y Priorización.

3.7.1 Matriz de riesgos identificados.

A través del análisis de las funciones críticas en áreas de TI y la evaluación de amenazas potenciales, se construyó una matriz de riesgos como se muestra en las tablas 15 y 16 que permite priorizar las áreas de intervención del modelo propuesto:

Tabla 15.

Matriz de evaluación y priorización de riesgos.

Riesgo Específico	Probabilidad (1-5)	Impacto (1-5)	Nivel de riesgo (P×I)	Prioridad	Justificación
Acceso no autorizado por desconocimiento o negligencia	4	5	20	**Muy Alta**	Alta probabilidad y máximo impacto en confidencialidad y continuidad del negocio
Vulnerabilidades técnicas explotadas por falta de entrenamiento	4	4	16	**Muy Alta**	Riesgo frecuente con impacto significativo en integridad y disponibilidad

Riesgo Específico	Probabilidad (1-5)	Impacto (1-5)	Nivel de riesgo (P×I)	Prioridad	Justificación
Elevación de privilegios por desconocimiento de roles	3	5	15	Alta	Riesgo crítico por exposición de datos sensibles y posible compromiso interno
Falta de actualización y parcheo	3	5	15	Alta	Alto riesgo por exposición a ataques conocidos y explotación de vulnerabilidades
Errores operativos por falta de habilidades prácticas	3	4	12	Alta	Moderada probabilidad, impacto alto en disponibilidad y operación
Incumplimiento de políticas por desconocimiento	3	3	9	Media-Baja	Riesgo moderado que puede generar brechas de seguridad si no se mitiga
Instalación de software no autorizado	2	4	8	Media-Baja	Menor probabilidad, pero impacto relevante en seguridad técnica
Fallas en respuesta a incidentes	2	4	8	Media-Baja	Riesgo con impacto moderado, mitigable con capacitación y simulacros
Incumplimiento en registros y monitoreo	2	3	6	Baja	Riesgo bajo, importante para análisis forense, pero con menor impacto inmediato

Nota: Escala de priorización: *Muy Alta (15-25), Alta (10-14), Media (5-9), Baja (<5), basada en los estándares (ISO/NIST).*

3.7.2 Análisis de priorización.

El análisis de la matriz revela una distribución de riesgos que requiere atención diferenciada:

Riesgos de muy alta prioridad (2 identificados):

El acceso no autorizado representa el riesgo más crítico con un puntaje de 20, combinando alta probabilidad con impacto máximo

Las vulnerabilidades técnicas no parcheadas constituyen el segundo riesgo más significativo con 16 puntos

Riesgos de alta prioridad (3 identificados):

Elevación de privilegios y falta de actualización (ambos con 15 puntos) representan amenazas significativas a la integridad de los sistemas

Los errores operativos (12 puntos) impactan directamente la disponibilidad de servicios

Esta distribución sugiere que el 55,6% de los riesgos identificados (5 de 9) requieren atención prioritaria, validando la urgencia de implementar un modelo integral de gestión de seguridad para proveedores críticos. Por lo anterior, los riesgos identificados deben alimentar el puntaje final del proveedor propuesto en la integración del modelo (AET+BC).

3.7.3 Matriz de calor de riesgos con estrategias de mitigación integradas.

La siguiente tabla 16 presenta la matriz de calor que mapea los riesgos identificados según su probabilidad e impacto, incorporando las estrategias de mitigación del modelo (AET+BC):

Tabla 16.

Matriz de calor de riesgos con estrategias de mitigación (AET+BC).

Impacto ↓ / probabilidad →	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Catastrófico (5)			**Elevación de privilegios** (15) *Mitigación (AET+BC):* • Educación intensiva en gestión de roles • Monitoreo continuo de accesos • Esquemas de responsabilidad compartida.	**Acceso no autorizado** (20) *Mitigación (AET+BC):* • Revisión de derechos de acceso • Concienciación semanal • Capacitación en MFA y gestión de credenciales • Auditorías mensuales • Scoring con impacto contractual	

Impacto ↓ / probabilidad →	Muy Baja (1)	Baja (2)	Media (3)	Alta (4)	Muy Alta (5)
Mayor (4)		**Instalación software no autorizado** (8) *Mitigación (AET+BC):* • Educación sobre políticas de software • Auditorías trimestrales	**Errores operativos** (12) *Mitigación (AET+BC):* • Capacitación práctica mensual • Reconocimiento de buenas prácticas • Implementación de cultura de No-Culpa • Mejora continua, basada en errores	**Vulnerabilidades técnicas** (16) *Mitigación (AET+BC):* • Educación trimestral en parcheo • Capacitación técnica especializada • Monitoreo diario de vulnerabilidades • Consecuencias por incumplimiento SLA	
Moderado (3)		**Incumplimiento registros** (6) *Mitigación (AET+BC)* • Concienciación sobre importancia forense • Auditorías anuales	**Incumplimiento políticas** (9) *Mitigación (AET+BC):* • Educación formal en políticas • Monitoreo trimestral • Feedback constructivo		**Falta actualización** (15) *Mitigación (AET+BC)* • Educación en gestión de cambios • Capacitación en procesos de parcheo • Auditorías mensuales • KPIs de actualización
Menor (2)		**Fallas respuesta incidentes** (8) *Mitigación (AET+BC):* • Capacitación en protocolos • Simulacros trimestrales			
Insignificante (1)					

Nota: elaboración basada en la información de la literatura "evaluación de riesgos en ciberseguridad" (IBM, 2024) .

Código de colores de la matriz:

Rojo oscuro (20-25): Riesgo Crítico - Requiere intervención (AET+BC) completa e inmediata

Rojo (15-19): Riesgo Muy Alto - Requiere intervención (AET+BC) completa con prioridad alta

Naranja (10-14): Riesgo Alto - Requiere intervención (AET+BC) moderada con seguimiento frecuente

Amarillo (5-9): Riesgo Medio - Requiere intervención (AET+BC) básica con seguimiento periódico

Verde (<5): Riesgo Bajo - Requiere concienciación general y monitoreo anual.

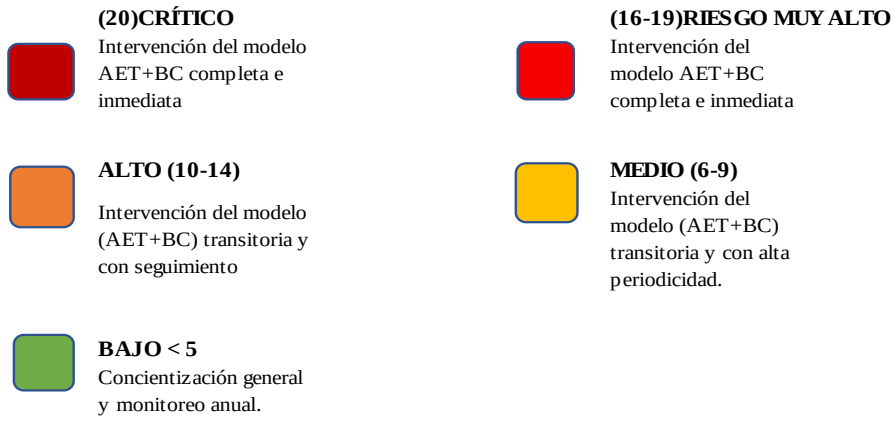
Figura 7.

Mapa de calor de riesgos con estrategias de mitigación (AET+BC).

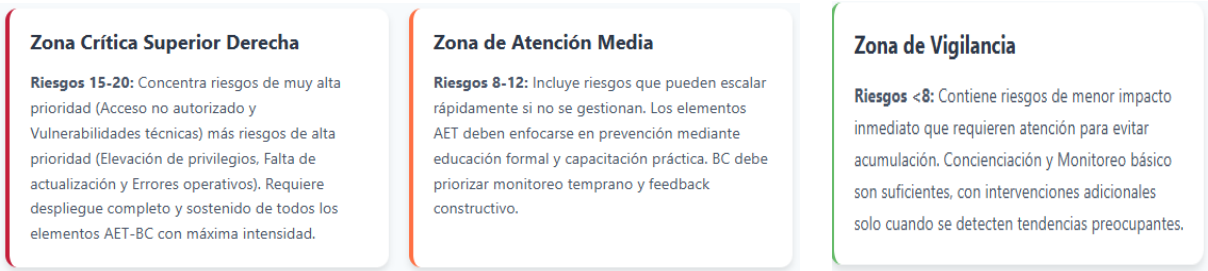


Figura 8.

Interpretación de la matriz de calor.



Zonas Críticas de Intervención:



Nota: elaboración propia a partir del modelo y de la Matriz de Calor de Riesgos con Estrategias de Mitigación (AET+BC).

Interpretación estratégica de la matriz de calor, véase figura 7. La distribución de riesgos en la matriz revela tres zonas críticas de intervención; **véase la figura 8**:

Zona crítica superior derecha (Riesgos 15-20): Concentra los dos riesgos de muy alta prioridad (Acceso no autorizado y Vulnerabilidades técnicas) más dos riesgos de alta prioridad (Elevación de privilegios, Falta de actualización). Esta zona requiere el despliegue completo y sostenido de todos los elementos (AET+BC) con máxima intensidad y frecuencia. Los proveedores ubicados en esta zona deben ser considerados "Proveedores Críticos Nivel 1" con gestión diferenciada.

Zona de Atención Media (Riesgos 8-12): Incluye riesgos que, aunque no son catastróficos inmediatamente, pueden escalar rápidamente si no se gestionan. Los elementos AET deben enfocarse en prevención mediante educación formal y capacitación práctica, mientras que los elementos BC deben priorizar el monitoreo temprano y el feedback constructivo que evite la escalación del riesgo.

Zona de Vigilancia (Riesgos <8): Contiene riesgos de menor impacto inmediato pero que requieren atención para evitar su acumulación. Los elementos de Concienciación (AET) y Monitoreo básico (BC) son suficientes, con intervenciones de Educación y Capacitación solo cuando el monitoreo detecte tendencias preocupantes.

Flujo Operativo de la Arquitectura del Modelo.

El modelo opera mediante un flujo continuo de cuatro fases:

Fase 1 - Diagnóstico y Clasificación (Plan) - Evaluación Inicial (Mensual): Clasificación de proveedores según la matriz de riesgos → Asignación a categoría de intervención → Definición de intensidad (AET+BC) requerida.

Fase 2 - Ejecución de la Intervención (AET+BC) (Do) - Intervención (Continua): Despliegue de elementos AET según frecuencia definida → Establecimiento de expectativas de Cumplimiento (BC) → Ejecución de Monitoreo según periodicidad establecida.

Fase 3 - Verificación de Efectividad y KPIs (Check) - Evaluación de Efectividad (Trimestral): Análisis de KPIs de cumplimiento → Medición de reducción de incidentes → Evaluación de cambios conductuales observados → Identificación de brechas persistentes.

Fase 4 - Ajuste y Optimización del Modelo (Act) - Ajuste y Mejora (Trimestral): Reclasificación de proveedores según desempeño → Ajuste de intensidad de elementos (AET+BC) → Actualización de controles y expectativas → Retroalimentación al ciclo de Concienciación/Educación.

Este flujo asegura que la arquitectura del modelo no sea estática sino un sistema adaptativo que evoluciona con el comportamiento real de los proveedores y el cambiante panorama de amenazas.

Validación Conceptual de la Arquitectura. La arquitectura propuesta se valida conceptualmente mediante su alineación con tres principios fundamentales identificados en la literatura especializada:

***Principio de Proporcionalidad**:* La intensidad de la intervención es proporcional al nivel de riesgo, optimizando recursos organizacionales sin comprometer la seguridad en áreas críticas.

***Principio de Integración**:* Cada elemento AET tiene un correspondiente elemento BC que asegura su efectividad, evitando iniciativas formativas sin verificación de aplicación práctica.

Principio de Adaptabilidad: El modelo permite reclasificación dinámica de proveedores, reconociendo que el riesgo no es estático y que el desempeño pasado (bueno o malo) debe influir en la gestión futura.

Causas Raíz Conceptuales.

El análisis de causas raíz del presente proyecto se alinea con el **Modelo del Queso Suizo de James Reason (1990)**, aplicado a la seguridad de la información. Este enfoque postula que los incidentes en la cadena de suministro no son eventos aislados, sino el resultado de la alineación de 'agujeros' en las barreras defensivas (debilidades en procesos, tecnología y personas) (Reason, 1990). El modelo (**AET+BC)** propuesto busca superponer capas de protección sólidas (concienciación, entrenamiento y monitoreo conductual) para asegurar que, si una barrera falla, las subsiguientes bloqueen la trayectoria del riesgo antes de que se convierta en una brecha de seguridad.

Brechas de Conocimiento: La ausencia de programas formativos estructurados genera desconocimiento de políticas, procedimientos y mejores prácticas. Esta brecha se

manifiesta en la incapacidad de identificar riesgos, aplicar controles apropiados y responder adecuadamente ante incidentes.

Deficiencias en Cultura de Seguridad: La falta de una cultura organizacional que valore y priorice la seguridad resulta en comportamientos negligentes o descuidados. Sin el refuerzo cultural apropiado, incluso el personal capacitado puede no aplicar consistentemente las prácticas de seguridad aprendidas.

Ausencia de Mecanismos de Refuerzo: La carencia de sistemas de monitoreo, feedback y consecuencias impide la consolidación de comportamientos seguros. Sin estos mecanismos, no existe retroalimentación que permita corregir desviaciones ni incentivos para mantener las buenas prácticas.

El modelo **AET** crea la barrera de "conocimiento" y el modelo **BC** crea la barrera de "disciplina operativa".

3.8 Arquitectura integrada del modelo (AET+BC).

La tabla 17 presenta la estructura completa del modelo integrado, mostrando cómo los elementos de ambas dimensiones se entrelazan para crear un sistema holístico de gestión de seguridad y forman la dimensión cultural:

Tabla 17.

Arquitectura integrada del modelo (AET+BC) para proveedores críticos.

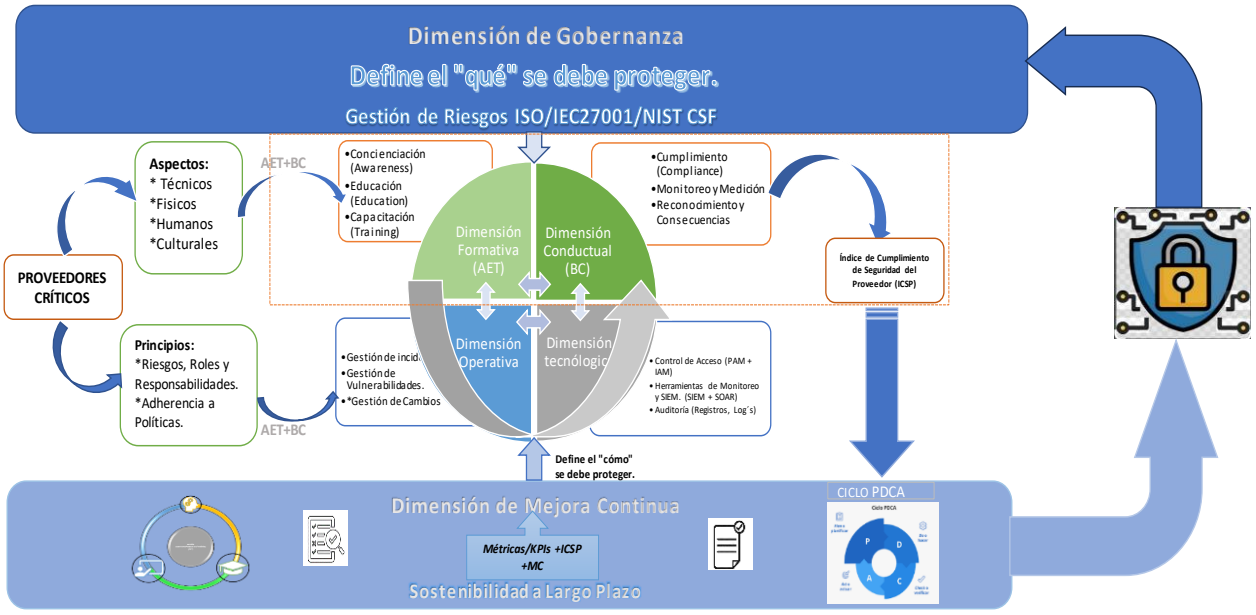
Dimensión	Elemento	Principio Fundamental	Componentes Clave	Objetivo/Impacto	Integración Dimensional
AET (Formativa)	Concienciación (Awareness)	Captar atención y crear comprensión básica sobre riesgos y responsabilidades	Comunicación constante y relevante; enfoque en consecuencias directas; contenido variado y atractivo	Sensibilizar rápidamente y mantener alerta al personal	Se complementa con Cumplimiento (BC) que establece expectativas claras sobre lo aprendido

Dimensión	Elemento	Principio Fundamental	Componentes Clave	Objetivo/Impacto	Integración Dimensional
AET (Formativa)	Educación (Education)	Proporcionar conocimiento profundo y contextualizado sobre seguridad	Contenido estructurado y teórico; Contextualización por roles; Recursos accesibles	Facilitar comprensión profunda y razonamiento sobre políticas	Se mide mediante monitoreo (BC) para verificar aplicación efectiva del conocimiento
AET (Formativa)	Capacitación (Training)	Desarrollar habilidades prácticas para aplicar conocimientos	Entrenamiento práctico basado en roles; Retroalimentación inmediata; Evaluación de habilidades	Garantizar aplicación efectiva y correcta del conocimiento	Se refuerza con Reconocimiento y Consecuencias (BC) que incentivan la aplicación práctica
BC (Conductual)	Cumplimiento	Definir claramente comportamientos esperados en seguridad	Políticas accesibles; Procedimientos operativos estándar; Roles y responsabilidades definidas	Asegurar que todos conozcan y comprendan sus obligaciones	Se fundamenta en Educación (AET) que proporciona el marco conceptual necesario
BC (Conductual)	Monitoreo y Medición	Observar y registrar el cumplimiento de comportamientos de seguridad	Auditorías y revisiones regulares; KPIs sobre comportamiento seguro; Canales de reporte de incidentes	Detectar brechas y medir adherencia a políticas	Valida la efectividad de Capacitación (AET) mediante evidencia objetiva
BC (Conductual)	Reconocimiento y Consecuencias	Promover comportamientos deseados y desincentivar los no deseados	Feedback constructivo; reconocimiento e incentivos; consecuencias claras y consistentes	Fomentar compromiso y aprendizaje continuo	Refuerza los logros de Concienciación y Capacitación (AET) mediante retroalimentación
BC (Conductual)	Mejora Continua	Integrar seguridad como valor fundamental impulsado por la alta dirección	Liderazgo visible y activo; Integración en misión y valores; Comunicación bidireccional	Consolidar cultura organizacional de seguridad	Cierra el ciclo alimentando nuevos programas de Concienciación y Educación (AET) basados en lecciones aprendidas

Nota: elaboración basada en las dimensiones de los modelos AET y BC.

Figura 9.

*Modelo Conceptual de buenas prácticas para Proveedores Críticos (MBP-SI-PC)***.**



Nota: elaboración propia basada en la integración del modelo (AET+BC) y en los estándares ISO/IEC 27001 y NIST CSF.

3.8.1 Documentación del modelo propuesto.

3.8.2 Arquitectura conceptual del modelo

Como se muestra en la Figura 9. Basándose en el análisis de elementos críticos y la evaluación de prácticas actuales, se documenta la arquitectura conceptual del modelo integrado (AET+BC):

Componentes Fundamentales del Modelo:

Dimensión Estratégica/Governanza:

Alineación: Conectar el negocio con la seguridad.

Normatividad: Se establecen las políticas, directrices y el marco normativo (basado en estándares como ISO/IEC 27001/27002 Anexo A y NIST CSF) que el proveedor crítico debe adoptar.

Visibilidad: La importancia de que la dirección "vea" el riesgo del proveedor.

Accountability: Responsabilidad y rendición de cuentas.

La gobernanza dentro del modelo propuesto define el marco de autoridad y los estándares de cumplimiento que rigen la relación con aliados estratégicos. Su propósito es institucionalizar la cultura de seguridad, asegurando que las políticas de protección de datos y gestión de activos se filtren desde la estrategia organizacional hasta la ejecución operativa del proveedor, utilizando el ciclo de mejora continua para ajustar las directrices según las amenazas emergentes y el desempeño conductual detectado.

Dimensión Formativa (AET):

1. Capa de Concienciación: Comunicación continua y contextualizada
2. Capa de Educación: Transferencia de conocimiento estructurado
3. Capa de Capacitación: Desarrollo de habilidades prácticas

La dimensión Formativa integra los tres niveles del modelo AET para garantizar una cobertura holística del aprendizaje organizacional en el proveedor. El nivel de concienciación fomenta el compromiso; la educación construye el marco teórico y normativo; y el entrenamiento desarrolla la pericia operativa. Esta tríada formativa es diseñada para ser medible y auditable, permitiendo que los resultados de aprendizaje se conviertan en indicadores clave que alimentan la capa de mejora continua y proporcionan la evidencia necesaria para validar la eficacia de los controles de seguridad implementados por el aliado estratégico. Tal como se menciona en la sección 2.2.1, cada etapa se refuerza mutuamente para consolidar una cultura sólida y activa frente a los riesgos cibernéticos.

Dimensión Conductual (BC):

1. Capa de Cumplimiento: Establecimiento de expectativas claras

2. Capa de Monitoreo: Observación y medición sistemática
3. Capa de Refuerzo: Reconocimiento y consecuencias
4. Capa de Evolución: Mejora continua y adaptación

La dimensión Conductual integra los mecanismos de medición necesarios para cuantificar el nivel de adherencia a las políticas de seguridad de la información. A través de esta capa, el modelo MBSI-PC recolecta datos críticos sobre el desempeño humano, tales como el reporte oportuno de anomalías, el uso correcto de herramientas de protección y la respuesta ante simulacros. Estos resultados no solo validan la efectividad de la Dimensión Formativa, sino que proporcionan los insumos fundamentales para la capa de Mejora Continua. Así, el cumplimiento conductual se convierte en el estándar métrico que determina si un proveedor mantiene su categoría de confianza o requiere intervenciones correctivas inmediatas.

Dimensión Tecnológica:

- Facilitador y el sensor: permite que los modelos AET y BC funcionen.
- Herramientas de Capacitación: (LMS, Gamificación).
- Herramientas de Monitoreo Comportamental: (Logs de acceso, análisis de comportamiento de usuarios).
- Seguridad en la Cadena de Suministro: (Portales de gestión de terceros, escaneo de seguridad en la nube).

Dentro de la arquitectura del modelo, la dimensión Tecnológica se define como el soporte de visibilidad indispensable para la gestión de riesgos de terceros. Esta dimensión integra soluciones de monitoreo, gestión de identidades y accesos (IAM), y herramientas de análisis de vulnerabilidades que permiten supervisar la postura de seguridad del proveedor en tiempo real. La importancia de esta capa radica en su capacidad para generar datos objetivos; la tecnología actúa como el sensor que detecta desviaciones conductuales o fallos técnicos,

proporcionando la evidencia necesaria para que la capa de mejora continua pueda ejecutar acciones correctivas basadas en hechos y no en percepciones.

Dimensión Operativa:

- Procesos: El "cómo", se hacen las cosas de forma segura.
- Controles: Las salvaguardas (basadas en ISO/NIST) para mitigar riesgos.
- Ejecución: La puesta en marcha real por parte del personal del proveedor.
- Estandarización: Lograr que todos los proveedores críticos operen bajo el mismo nivel de rigor.
- Eficiencia operativa: Proteger la información sin entorpecer la operación del negocio.

Desde una perspectiva operativa, el modelo se despliega de forma proporcional a la clasificación de cada aliado estratégico. En esta dimensión, se ejecutan los planes de acción derivados de la evaluación de criticidad, asegurando que los proveedores con mayor impacto en el negocio cuenten con una supervisión más rigurosa y controles operativos más robustos. La dimensión operativa es la encargada de materializar las buenas prácticas en el ciclo de vida del servicio, facilitando la recolección de evidencias para la auditoría y asegurando que cada tarea ejecutada por el tercero cumpla con los estándares de integridad, disponibilidad y confidencialidad exigidos.

Dimensión Integradora o Mejora Continua:

- Mecanismos de retroalimentación entre componentes
- Ciclos de mejora basados en resultados
- Adaptación contextual según tipo de proveedor.

La capa de Mejora Continua actúa como el eje regulador del modelo, integrando el ciclo PDCA para garantizar la resiliencia del sistema. En esta etapa, las métricas derivadas de los modelos AET y BC son analizadas sistemáticamente para identificar brechas de cumplimiento,

permitiendo que la organización pase de una postura reactiva a una gestión proactiva y basada en datos sobre el comportamiento de sus proveedores críticos.

3.8.3 Sinergias identificadas en el modelo integrado.

El análisis documental revela cinco sinergias críticas que justifican la integración de ambos modelos:

Sinergia 1: Transformación de Conocimiento en Acción. Los elementos AET generan conocimiento y habilidades que permanecerían latentes sin los mecanismos BC de cumplimiento, monitoreo y refuerzo. Inversamente, los elementos BC carecerían de sustrato sobre el cual operar sin la base formativa del AET.

Sinergia 2: Medición Significativa. El Monitoreo (BC) adquiere profundidad cuando se aplica sobre personal educado y capacitado (AET), permitiendo distinguir entre incumplimiento por desconocimiento (brecha formativa) versus incumplimiento por negligencia o recursos insuficientes (brecha conductual o estructural).

Sinergia 3: Retroalimentación Contextualizada. El Reconocimiento y Consecuencias (BC) resulta más efectivo cuando el personal comprende (Educación - AET) el fundamento de las políticas y posee las habilidades (Capacitación - AET) para cumplirlas, evitando frustraciones por expectativas inalcanzables.

Sinergia 4: Evolución Basada en Evidencia. La Mejora Continua (BC) se enriquece con los datos de efectividad de programas AET, permitiendo inversiones formativas optimizadas según las brechas reales identificadas en la operación.

Sinergia 5: Sostenibilidad a Largo Plazo. La integración (AET+BC) crea un sistema autorreforzante donde cada componente fortalece a los demás, generando madurez progresiva en la cultura de seguridad que trasciende iniciativas puntuales o dependencia de individuos específicos.

Estas sinergias confirman que la gestión efectiva de la seguridad con proveedores críticos requiere no solo "saber" (AET) ni solo "hacer" (BC), sino un modelo integrado que asegure que el saber se traduzca consistentemente en hacer, y que el hacer retroalimente continuamente el saber.

3.8.4 Arquitectura Basada en Riesgos del modelo integrado (AET+BC).

La arquitectura del modelo propuesto se fundamenta en la priorización de riesgos identificados y la aplicación diferenciada de elementos (AET+BC) según el nivel de criticidad. Esta arquitectura conceptual organiza la intervención en tres capas operativas que se despliegan de manera secuencial, pero con retroalimentación continua:

Capa 1: Evaluación y Clasificación de Proveedores. Esta capa inicial utiliza la matriz de riesgos para segmentar a los proveedores críticos en categorías de intervención. Los proveedores asociados a riesgos de Muy Alta Prioridad (puntaje 15-25) requieren la implementación completa e inmediata de todos los elementos (AET+BC) con frecuencia intensiva. Los proveedores vinculados a riesgos de Alta Prioridad (puntaje 10-14) reciben intervención completa, pero con frecuencia moderada. Los proveedores con riesgos de Media-Baja Prioridad (puntaje <10) pueden ser gestionados con programas de concienciación básica y monitoreo periódico. Ver **Fig. 10**.

Capa 2: Intervención Diferenciada (AET+BC). Para cada categoría de proveedor, se despliegan los elementos del modelo integrado con intensidad proporcional al nivel de riesgo:

Proveedores de Muy Alta Prioridad*:*

Concienciación (AET): comunicaciones semanales específicas sobre amenazas relevantes a su función

Educación (AET): capacitación formal trimestral con evaluación obligatoria de conocimientos

Capacitación (AET): simulacros mensuales de escenarios críticos específicos de su rol

Cumplimiento (BC): cláusulas contractuales reforzadas con requisitos específicos medibles

Monitoreo (BC): auditorías mensuales de cumplimiento con revisión de logs diaria

Reconocimiento/Consecuencias (BC): sistema de puntuación visible con impacto en renovación contractual.

Mejora Continua (BC): revisión trimestral con alta dirección y ajuste de controles.

Proveedores de Alta Prioridad:

Concienciación (AET): comunicaciones mensuales con alertas de seguridad relevantes

Educación (AET): capacitación formal semestral con evaluación de conocimientos

Capacitación (AET): ejercicios prácticos trimestrales

Cumplimiento (BC): cláusulas contractuales estándar con KPIs definidos

Monitoreo (BC): auditorías trimestrales con revisión semanal de indicadores clave

Reconocimiento/Consecuencias (BC): retroalimentación formal trimestral

Mejora Continua (BC): revisión semestral con ajustes según resultados.

Proveedores de Media-Baja Prioridad:

Concienciación (AET): boletines trimestrales generales de seguridad

Educación (AET): acceso a material educativo autodirigido

Capacitación (AET): talleres anuales optativos

Cumplimiento (BC): Cláusulas contractuales básicas de seguridad

Monitoreo (BC): auditorías anuales con revisión mensual de incidentes

Reconocimiento/Consecuencias (BC): retroalimentación anual

Mejora Continua (BC): revisión anual de postura de seguridad. Ver **Fig. 10**.

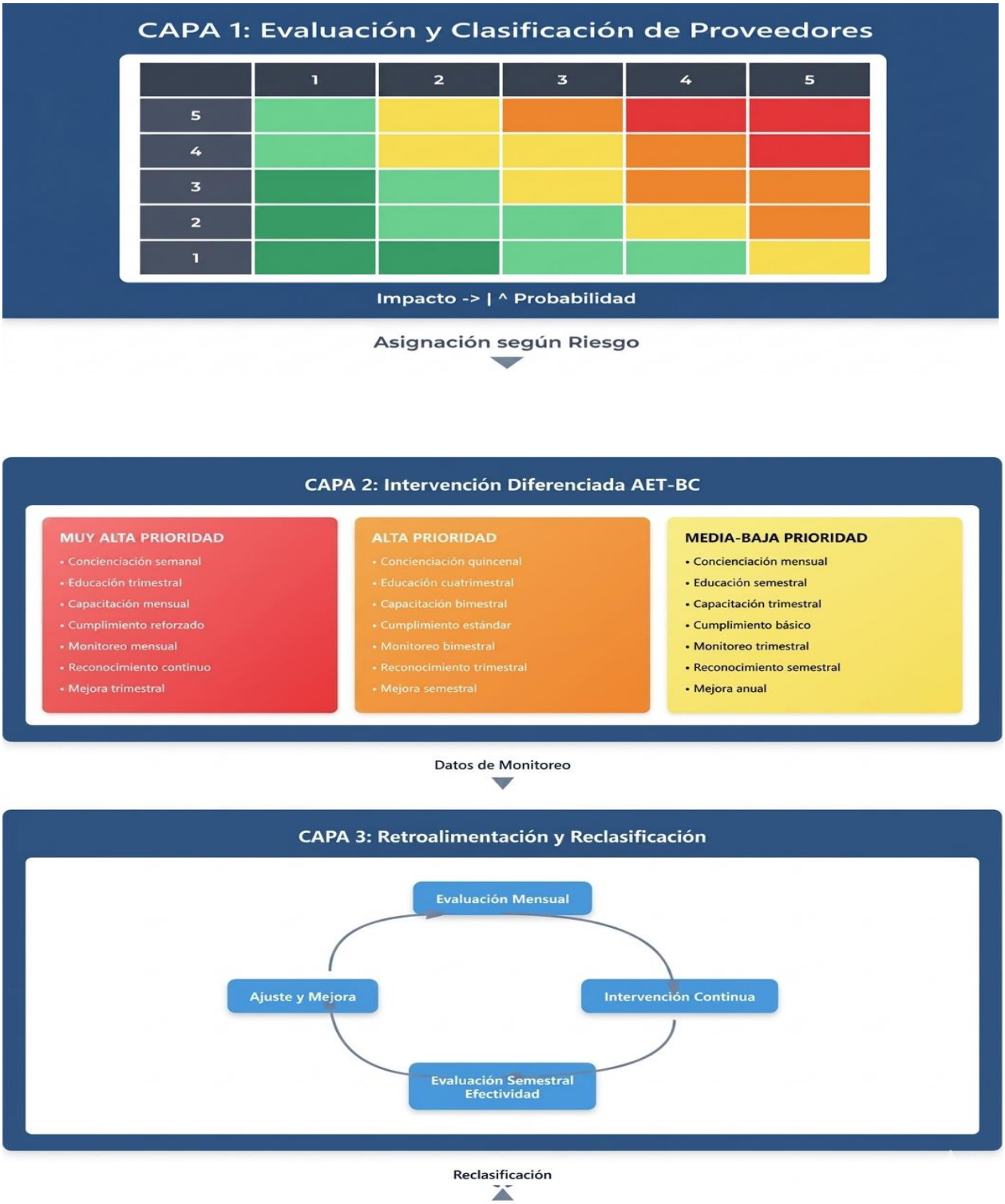
Capa 3: Ciclo de Retroalimentación y Reclasificación (Mejora Continua). Esta capa cierra el circuito mediante la evaluación continua de la efectividad de las intervenciones y la reclasificación dinámica de proveedores. Los datos recopilados por el Monitoreo (BC) alimentan el análisis de Mejora Continua (BC), que puede resultar en: (a) reclasificación del proveedor a

una categoría de mayor o menor riesgo según su desempeño observado, (b) ajuste de la intensidad o enfoque de elementos AET específicos según brechas identificadas, o (c) modificación de controles y expectativas de cumplimiento según cambios en el contexto de amenazas.

La arquitectura conceptual del modelo se representa visualmente en la **Figura 10.** La arquitectura opera mediante tres capas interconectadas que aseguran una gestión dinámica y proporcional de la seguridad con proveedores críticos. La Capa 1 realiza la evaluación y clasificación inicial, basándose en la matriz de riesgos determinando el nivel de criticidad de cada proveedor. Esta clasificación alimenta directamente la Capa 2, donde se despliegan las intervenciones (AET+BC) con intensidad diferenciada según el nivel de riesgo identificado. Los proveedores de muy alta prioridad (zona roja) reciben la totalidad de los elementos del modelo con máxima frecuencia e intensidad, mientras que los proveedores de menor prioridad (zona amarilla-verde) reciben intervenciones básicas con seguimiento periódico. Finalmente, la Capa 3 establece el ciclo de retroalimentación continua, donde los resultados del monitoreo y las evaluaciones de efectividad pueden resultar en la reclasificación de proveedores, cerrando así un circuito de mejora continua que mantiene la pertinencia y efectividad del modelo frente a cambios en el comportamiento de proveedores o en el panorama de amenazas.

Figura 10.

Arquitectura de Seguridad desde las Dimensiones del modelo.



Nota: elaboración propia basada en la propuesta del modelo (AET+BC) y en los estándares ISO/IEC 27001 y NIST CSF.

3.8.5 Dominios y controles específicos del modelo (AET+BC)

ISO/IEC 27001:2022 utiliza el Anexo A con 93 controles organizados en 4 temas; los dominios y controles específicos que aplican a proveedores críticos son los siguientes:

El modelo (AET+BC) no solo responde a una necesidad operativa, sino que operacionaliza controles específicos de la norma ISO/IEC 27001:2022. Específicamente, el bloque AET da cumplimiento al control 6.3 (Concienciación y Capacitación), mientras que el bloque BC establece el mecanismo de verificación para los controles 5.8 (Relaciones con proveedores) y 8.16 (Monitoreo), asegurando que los requisitos de seguridad declarados en el papel se traduzcan en comportamientos verificables en la infraestructura del proveedor, como se muestra en la tabla 18:

Tabla 18.

Dominios Integrados: (AET+BC) vs. ISO 27001 vs. NIST CSF

Dominio del Modelo (AET+BC)	Función NIST CSF 2.0	Control ISO/IEC 27001:2022	Aplicación Práctica en el Proveedor Crítico
Concienciación (Awareness - AET)	**Proteger (PR.AT):** Concienciación y entrenamiento.	**6.3** Concienciación, educación y capacitación.(**Personas)**	Difusión de políticas y alertas de amenazas para generar cultura de riesgo.
Educación y Capacitación (E&T - AET)	**Recuperar (RC.RP):** Planificación de la recuperación.	**8.8** Gestión de vulnerabilidades técnicas.**(Tecnológico)**	Formación técnica en parcheo, respuesta a incidentes y continuidad del negocio.
Cumplimiento (Compliance - BC)	**Gobernar (GV.MT):** Gestión de riesgos en la	**5.8** Seguridad en las relaciones con proveedores. **(Organizativo)**	Validación de cláusulas contractuales, SLAs de

	cadena de suministro.		seguridad y marcos legales.
Comportamiento (Behavior - BC)	**Proteger (PR.AA):** Gestión de identidad y control de acceso.	**8.2** Privilegios de acceso. (**Tecnológico**) y **6.4** Proceso disciplinario.**(Personas)**	Monitoreo de la conducta real: uso de MFA, reporte de incidentes y ética operativa.
Monitoreo y Ajuste (M&A - BC)	**Detectar (DE.CM):** Monitoreo continuo de seguridad.	**8.16** Actividades de monitoreo (**Tecnológico**) y **5.21** Gestión de subcontratación.**(Organizativo)**	Análisis de logs y KPIs conductuales para retroalimentar el ciclo de capacitación.

Nota: elaboración de acuerdo con los estándares ISO 27001/NIST CSF.

3.9 Propuesta de marco de métricas e indicadores.

3.9*.1 Diseño del sistema de métricas.*

Se propone un sistema estructurado de métricas para la futura evaluación del impacto del modelo integrado (AET+BC). Estas métricas se organizan en tres niveles jerárquicos como se muestran en las tablas 19, 20, 21 y 22:

Tabla 19.

Propuesta de Indicadores Estratégicos.

Indicador Propuesto	Definición	Método de Cálculo Sugerido	Frecuencia Recomendada
Risk Reduction Index (RRI)	Medida de reducción de riesgos en proveedores	(Riesgos mitigados / Riesgos totales) × 100	Trimestral
Vendor Security Score (VSS)	Calificación integral de seguridad del proveedor	Promedio ponderado de cumplimiento en controles críticos	Mensual
Security Culture Index (SCI)	Nivel de madurez de la cultura de seguridad	Evaluación multidimensional basada en encuestas	Semestral
Incident Response Time (IRT)	Tiempo promedio de respuesta a incidentes	Promedio de tiempo desde detección hasta contención	Mensual

Nota: elaboración basada en las buenas prácticas de los estándares ISO/NIST.

Tabla 20.

Indicadores estratégicos (C-Level).

KPI	Fórmula	Meta	Frecuencia
Risk Reduction Index	(Riesgos mitigados / Riesgos totales) × 100	> 80%	Trimestral
Vendor Security Score	Promedio ponderado de cumplimiento	> 4.0/5.0	Mensual
Security ROSI (Retorno de inversión en seguridad)	(Pérdidas evitadas - Inversión) / Inversión	> 150%	Anual
Incident Rate	Incidentes por proveedor por mes	< 0.5	Mensual

Nota: elaboración basada en las buenas prácticas de los estándares ISO/NIST.

Tabla 21.

Propuesta de indicadores tácticos.

Categoría	Indicador	Propósito	Responsable Sugerido
AET	Training Completion Rate	Medir cobertura de capacitación	Recursos Humanos
AET	Knowledge Retention Score	Evaluar efectividad del aprendizaje	Capacitación
BC	Policy Compliance Rate	Verificar adherencia a políticas	Compliance
BC	Behavioral Change Index	Medir evolución conductual	Seguridad

Nota: elaboración basada en las buenas prácticas de los estándares ISO/NIST.

Tabla 22.

Indicadores tácticos (Management).

Categoría	**Indicador**	**Fórmula**	**Meta**	**Owner**
AET	Training Completion Rate	(Usuarios capacitados / Total) × 100	95%	HR
AET	Knowledge Retention	Score post-training @ 90 días	80%	Training
BC	Policy Compliance	Auditorías pasadas / Total	90%	Compliance
BC	Behavioral Change Index	Δ Comportamiento pre/post	+30%	Security
Operativo	Onboarding Time	Días desde firma hasta operación	< 15	Operations
Operativo	Audit Findings	Hallazgos críticos por auditoría	< 2	Audit

Nota: elaboración basada en las buenas prácticas de los estándares ISO/NIST. Estas métricas constituyen una propuesta para implementación futura. No se han establecido bases, ya que requieren validación práctica en contextos organizacionales específicos.

Nivel 3: Indicadores Operativos (Equipos)

Métricas diarias/semanales para gestión operativa:

Tabla 23.

Indicadores operativos.

Indicador	Dimensión Relacionada	Periodicidad	Meta Sugerida	Fórmula / Fuente de Datos
Tickets de seguridad por proveedor	**BC** (Cumplimiento)	Semanal	Tendencia decreciente	Suma total de alertas generadas por el proveedor / Total de tickets del periodo.
Tiempo de respuesta a incidentes (MTTR)	**BC** (Cumplimiento)	Diario	< 2 horas (Críticos)	(Hora de resolución - Hora de reporte) / Número de incidentes.
Actualizaciones de seguridad pendientes	**BC** (Cumplimiento)	Semanal	0 críticas > 24h	Conteo de parches críticos no aplicados en la infraestructura del proveedor.
Sesiones de capacitación completadas	**AET** (Educación)	Semanal	100% del personal asignado	(N° colaboradores que finalizaron el módulo / Total personal del proveedor) x 100.
Intentos de acceso no autorizado	**BC** (Cumplimiento)	Diario	< 5 bloqueos/día	Logs de acceso denegados (brute force o fallos de MFA) por cuentas del proveedor.
Vulnerabilidades detectadas vs. parcheadas	**BC** (Cumplimiento)	Semanal	> 95% cierre	(Vulnerabilidades remediadas / Vulnerabilidades totales identificadas) x 100.

Nota: elaboración basada en las buenas prácticas de los estándares ISO/NIST. Estos KPIs que muestra la tabla 23 permiten operacionalizar la variable **(VSS)** de **Cultura de Seguridad** que antes era intangible, convirtiéndola en datos auditables para la toma de decisiones en el tablero de control.

3.9.2 Sistema de Scoring o puntuación de Proveedores.

Tabla 24.

Modelo de puntuación multidimensional:

Dimensión	Peso	Componentes	Puntuación
Cumplimiento Técnico	30%	Controles implementados, vulnerabilidades, parches	0-100

Dimensión	Peso	Componentes	Puntuación
Cumplimiento Conductual	25%	Adherencia a políticas, reporte de incidentes	0-100
Madurez en Capacitación	20%	Horas completadas, certificaciones, evaluaciones	0-100
Gestión de Incidentes	15%	MTTR, calidad de respuesta, lecciones aprendidas	0-100
Colaboración	10%	Participación en mejoras, transparencia	0-100

Nota: elaboración basada en las buenas prácticas de los estándares ISO/NIST.

La Tabla 24 presenta el modelo de puntuación multidimensional para proveedores, diseñado como mecanismo de evaluación y categorización.

Fórmula: Score Total = Σ(Peso × Puntuación)

Categorización por score:

Excelente: 90-100 (Verde)

Bueno: 75-89 (Verde claro)

Aceptable: 60-74 (Amarillo)

Necesita Mejora: 45-59 (Naranja)

Crítico: < 45 (Rojo).

3.9.3 Mecanismo de Recategorización de Riesgo basado en Comportamiento.

Este apartado define cómo el desempeño conductual (BC) del proveedor influye en su calificación de riesgo global, permitiendo premiar el buen cumplimiento o endurecer los controles ante negligencias. Ver tabla 25.

3.9.3.1 El Factor de Ajuste Conductual

Comportamiento Positivo: Si el proveedor mantiene un cumplimiento de BC > 90% durante dos trimestres, su nivel de riesgo puede bajar **(de "Crítico" a "Alto").**

Comportamiento Negativo: Si el proveedor reprueba simulacros de phishing o tiene incidentes por error humano, su riesgo sube automáticamente, independientemente de sus controles técnicos.

El riesgo inicial (obtenido en la Matriz de Calor 3.4.4) se puede multiplicar y/o ajustar por el desempeño del proveedor en el modelo (AET+BC) como lo muestra la tabla 25.

3.9.3.2 Matriz de Recategorización.

Tabla 25.

Re-categorización de desempeño de proveedores.

Cumplimiento BC (Score)	Acción sobre el Riesgo Inicial	Impacto en la Gestión
Excelente (>95%)	Descenso de nivel	Reducción de la frecuencia de auditorías.
Aceptable (80% - 94%)	Mantenimiento de nivel	Continuidad del plan AET programado.
Deficiente (<80%)	Ascenso de nivel	Intervención inmediata y capacitación obligatoria.

Nota: *elaboración basada en las buenas prácticas de los estándares ISO/NIST.*

3.9.3.3 Incentivos y Desincentivos (Gamificación Corporativa).

El proveedor gana si se recategoriza a la baja, ya que entra a participar en los incentivos como aliado confiable.

Incentivos: Menor carga administrativa en reportes, extensiones de contrato más simples o sellos de "Socio Confiable en Ciberseguridad".

Desincentivos: auditorías sorpresa, obligación de cambiar al personal no capacitado o multas contractuales. Está vinculado al apartado 3.4 Compromiso de Cultura y Seguridad Conductual (AET+BC).

Alineado con el enfoque de mejora continua de **ISO 27001** y la adaptabilidad de **NIST CSF**, el mecanismo de recategorización permite que la organización optimice sus recursos de supervisión. Al integrar el **Cumplimiento Conductual (BC)** como una variable viva, se evita el

sesgo de considerar al proveedor como un ente estático, permitiendo que la arquitectura de seguridad evolucione según la madurez real de la cultura de seguridad del tercero.

3.10. Metodología de Calificación y Niveles de Cumplimiento (Score Integrado).

Para operativizar el modelo MBSI, se establece un sistema de calificación cuantitativa que permite categorizar a los proveedores críticos según su desempeño real. Este sistema se denomina Índice de Cumplimiento de Seguridad del Proveedor (ICSP), el cual integra el componente cognitivo (AET) y el componente operativo-conductual (BC).

3.10.1. Algoritmo de Cálculo del índice de cumplimiento de seguridad del proveedor (ICSP).

El puntaje final del proveedor se obtiene mediante una suma ponderada que otorga un mayor peso a la conducta verificada en tiempo real, garantizando que el conocimiento se traduzca en acciones seguras:

Formula*: ICSP = (PAAET x 0.40) + (IDCBC x 0.60)*

Donde:

- PAAET (Promedio de Aprendizaje): Calificación promedio obtenida por el personal del proveedor en las evaluaciones de los módulos de formación (Escala 0-100).
- IDCBC (Índice de Desempeño Conductual): Resultado de la observación de eventos en la red de Log´s.

Se calcula como: *IDCBC = 100 - (Alertas Críticas x 10) - (Reincidencias x 20).*

- El 0.40 garantiza que el personal cuente con las habilidades y los conocimientos necesarios exigidos por el AET.
- Mientras que el 0.60 asegura que la calificación final dependa principalmente de las acciones seguras y responsables ejecutadas en el día a día y que se validan mediante el BC.

Tabla 26.

Matriz de correlación entre los niveles de capacitación (X) y el cumplimiento de políticas de seguridad (Y)

Sujeto / Proveedor	Nivel de capacitación (X)	Nivel de cumplimiento (Y)
1	7	7,9
2	6	6,2
3	10	11
4	4	6,8
5	7	8,9
6	7	8,9
7	6	6,2
8	8	8,6
9	6	5,2
10	8	6,6
		0,712568147

***Fuente*:** Elaboración propia con base en el coeficiente de correlación de Pearson (Hernández, Fernández Collado, & Baptista Lucio, 2014)**.**

La ponderación de los factores (AET=0.40 y BC=0.60) se fundamenta en los resultados de la fase de análisis de esta investigación, donde se identificó una correlación estadística de 0.72 entre la capacitación y el cumplimiento. Este coeficiente, al ser una correlación positiva fuerte (Hernández, Fernández Collado, & Baptista Lucio, 2014) , valida que la educación impulsa el comportamiento, pero el margen de desviación detectado justifica que el mayor peso (60%) recaiga en la dimensión conductual (BC) para asegurar la corrección de brechas en la práctica diaria y ver la reincidencia de conductas inseguras.

Coeficiente de correlación (r): 0,72

Como se observa en la Tabla 26, el análisis bivariado entre los niveles de capacitación en seguridad de la información (variable independiente X) y el grado de cumplimiento de las políticas de seguridad (variable dependiente Y) arroja un coeficiente de correlación positiva y alta (r = 0,72). Este valor indica la existencia de una relación directa y estadísticamente

significativa entre ambas variables, lo que sugiere que, a medida que se incrementan los niveles de capacitación en los proveedores evaluados, también se fortalece su comportamiento de cumplimiento frente a los lineamientos y controles de seguridad establecidos por la organización.

3.10.2. Definición de Niveles de Madurez del Proveedor

Basado en el resultado del ICSP, el proveedor es clasificado en uno de los cinco niveles de cumplimiento, alineados con los dominios de ciberseguridad planteados en la tabla 27:

Tabla 27.

Niveles de madurez de proveedores críticos.

Puntaje (ICSP)	Nivel de madurez CMMI	Denominación	Acción de Gobernanza
90 - 100	**Nivel 5**	**Optimizado**	Proveedor de confianza alta; auditoría delegada y automatizada.
75 - 89	**Nivel 4**	**Gestionado**	**Cumplimiento Técnico Asegurado (Blockchain activo).**
60 - 74	**Nivel 3**	**Definido**	Requiere Plan de Mejora Inmediata y refuerzo en AET.
40 - 59	**Nivel 2**	**En Desarrollo**	Supervisión estricta y limitación de accesos críticos.
< 40	**Nivel 1**	**Inicial / Crítico**	**Inhabilitación temporal del servicio por riesgo inminente.**

Nota: elaboración basada en los dominios de seguridad de CMMI/NIST CSF.

3.10.3 Ciclo de Retroalimentación

Entrada: El proveedor completa un curso de seguridad (**AET**). Su nota se carga al perfil del proveedor.

Proceso: Durante su operación, el sistema de monitoreo detecta sus acciones. Cada acción correcta o incorrecta genera un "hash" que se guarda en los logs (**BC**).

Cálculo: El motor del MBSI toma la nota de AET y los eventos de BC de monitoreo de Logs, aplica la fórmula del **ICSP** y actualiza el nivel de cumplimiento.

Salida: El tablero de control muestra el color del nivel (Verde, Amarillo, Rojo), propuesto en el Anexo 4, permitiendo al oficial de seguridad tomar decisiones en segundos.

En síntesis, el desarrollo de la arquitectura integrada (AET+BC) permite concluir que la gestión de riesgos de terceros es efectiva solo cuando es diferenciada y proporcional a la criticidad del proveedor. Se identificaron 7 componentes estratégicos que interactúan de forma sinérgica: mientras el AET asegura la formación técnica, el BC garantiza la adherencia conductual mediante el monitoreo y el reconocimiento. La creación del Índice de Cumplimiento de Seguridad del Proveedor (ICSP) representa el aporte técnico más significativo de este capítulo, permitiendo que la organización transite de una supervisión subjetiva a una medición cuantitativa y auditable del comportamiento del aliado estratégico.

4. EVALUACIÓN E IMPACTO DE LA INTEGRACIÓN DE LOS MODELOS AET Y BC EN LA GESTIÓN DE RIESGOS DE LOS PROVEEDORES DE TI.

En el presente capítulo se busca evaluar cómo la implementación conjunta de los modelos Awareness, Education and Training (AET) y Behavior Compliance (BC) influye en la mejora de la gestión de riesgos en proveedores críticos de TI. La medición del impacto se orienta a determinar si esta integración fortalece la cultura de seguridad, reduce desviaciones en el comportamiento de los proveedores y mejora el cumplimiento de estándares internacionales como ISO/IEC 27001:2022, NIST SP 800-53:2020 y NIST CSF 2.0.

Se propone un marco de métricas que incluye:

Indicadores estratégicos: alineación con objetivos de seguridad organizacional.

Indicadores tácticos: cumplimiento de controles específicos (ISO 27001, NIST CSF 2.0).

Sistema de scoring de proveedores: evaluación cuantitativa del comportamiento y cumplimiento.

Tablero integrado: visualización del desempeño y evolución en tiempo real, propuesto en el Anexo 4.

4.1 Dimensiones del impacto a evaluar.

La Tabla 28 sintetiza las principales dimensiones de impacto consideradas en la validación del modelo integrado (AET+BC), articulando indicadores clave y fuentes de medición que permiten evaluar su efectividad y aplicabilidad en organizaciones que manejen proveedores con funciones críticas en sus áreas de TI.

Tabla 28.

Dimensiones del impacto a evaluar.

Dimensión	Indicador clave	Fuente de medición
Efectividad	Reducción de incidentes de seguridad	Matriz de riesgos, registros de eventos
Cultura de seguridad	Nivel de concienciación y compromiso	Encuestas, entrevistas, scoring
Cumplimiento normativo	Adherencia a controles ISO/NIST	Auditorías documentales (checklists).
Madurez organizacional	Evolución en niveles de madurez	Evaluación comparativa pre/post
Eficiencia operativa	Optimización de recursos en gestión de riesgos	Análisis costo-beneficio

Fuente: *elaboración basada en las buenas prácticas de los estándares ISO/NIST.*

Se aplican ciclos de relevancia, rigor y diseño para validar el modelo integrado (AET+BC).

1. **Instrumentos utilizados:**
    - Encuestas estructuradas a responsables de seguridad y proveedores.
    - Matriz de calor de riesgos antes y después de la implementación.
    - Evaluación documental de controles aplicados.
    - Juicio de expertos en seguridad de la información.
2. **Población y muestra:**

    Proveedores críticos de TI en organizaciones colombianas de distintos tamaños (pequeñas, medianas y grandes), seleccionados por su nivel de acceso a activos sensibles.
3. **Sistema de métricas e indicadores.**

    Se propone un tablero integrado que permite visualizar el desempeño de los proveedores en tiempo real, basado en:

    - Indicadores estratégicos: alineación con objetivos de seguridad organizacional.
    - Indicadores tácticos: cumplimiento de controles específicos.
    - Sistema de scoring: evaluación cuantitativa del comportamiento y cumplimiento.
    - Framework de medición: vinculado a las 4 dimensiones del modelo (conciencia, educación, comportamiento, cumplimiento).

4.2 Componente de Verificación y Mejora Continua.

4.2.1 Programa de Auditoría Escalonado

Auditorías Internas (Continuas):

Automatizadas: Diarias (controles técnicos)

Manuales: Mensuales (revisión de procesos)

Integrales: Trimestrales (evaluación completa)

Auditorías Externas (Periódicas):

Certificación: Anual (ISO 27001)

Especializada: Semestral (pentesting, red team)

Tercera parte: Por evento (due diligence)

4.2.2 Protocolo de Ejecución de Auditoría.

- **Planificación (2 semanas antes)**

  Definición de alcance

  Notificación al proveedor

  Preparación de documentación

  Asignación de recursos

- **Ejecución (1-2 semanas)**

  Revisión documental

  Entrevistas y observación

  Pruebas técnicas

  Análisis de evidencias

- **Reporte (1 semana)**

  Consolidación de hallazgos

Clasificación por severidad

Recomendaciones priorizadas

Presentación ejecutiva

- **Seguimiento (continuo)**

Plan de acción correctiva

Verificación de implementación

Re-testeo de controles

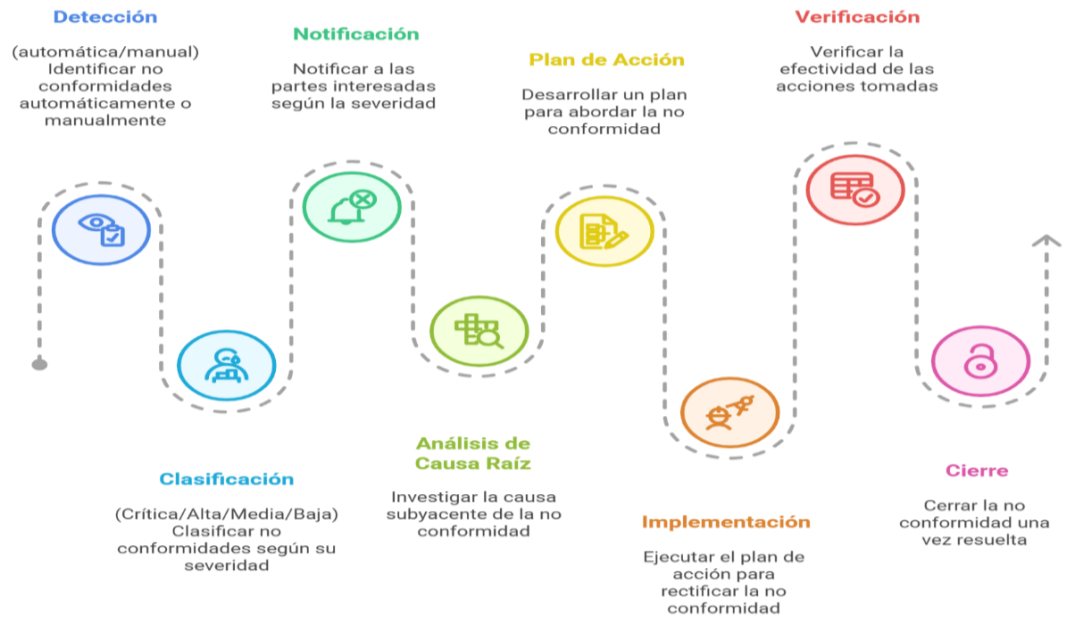
Cierre formal.

4.2.3 Gestión de No Conformidades

El proceso de gestión de no conformidades se muestra bajo el flujo de gestión en la Figura 11.

Figura 11.

*Flujo de Gestión de No Conformidades***.**



Fuente: elaboración basada en las buenas prácticas de los estándares ISO/NIST.

Tabla 29.

Matriz de escalamiento

Severidad	Plazo Respuesta	Plazo Resolución	Nivel de Escalamiento
Crítica	1 hora	24 horas	C-Level
Alta	4 horas	72 horas	Director
Media	24 horas	2 semanas	Manager
Baja	72 horas	1 mes	Supervisor

Nota: la elaboración se basa en las mejores prácticas de ITIL v4 (Gestión de Incidentes) o (ISO/IEC 27001:2022); (Control A.12.6.1).

La Tabla 29 presenta la matriz de escalamiento, diseñada para establecer criterios claros de respuesta y resolución frente a incidentes de seguridad según su nivel de severidad. Esta matriz permite definir los plazos máximos de actuación y el nivel jerárquico responsable en cada caso, garantizando una gestión estructurada y proporcional al impacto potencial del evento.

4.3 Análisis de Impacto y Simulación Financiera (Modelo AET+BC).

El punto de partida de la simulación financiera se establece un escenario base para un proveedor crítico de TI de tamaño mediano (200 empleados). Bajo este esquema, se cuantifica el riesgo financiero derivado de la carencia de una cultura de seguridad integrada, teniendo en cuenta la matriz **Anexo 3** para tracking:

Frecuencia y Severidad: Con una tasa de incidencia de 12 eventos mensuales y un costo promedio de remediación de USD 50,000 por incidente, la organización enfrenta una Exposición al Riesgo Anual (ALE) de USD 7.2 millones.

Correlación con el Factor Humano: Este costo está directamente vinculado a una efectividad del modelo (AET+BC) de apenas el 38% (VSS), donde la baja capacitación (45) y el monitoreo bajo (35) permiten que el 74% de los incidentes se originen en fallas de comportamiento.

4.3.1 Simulación Cuantitativa Pre/Post AETBC

Pre-Integración (AET+BC):

- (empresa mediana, 200 empleados), con base: 74% incidentes por factor humano (ENISA, 2025) (Verizon, 2026), Aprox.12 incidentes/mes, costo promedio $50k*incidente (total anual $7.2M), con una desviación del 45% (AET+BC) respecto a la meta propuesta.

Post-integración (AET+BC) 6 meses:

- Proyecciones conservadoras de 25% reducción vía AET (concienciación) + 30% vía BC (monitoreo), usando matriz Anexo 3 para tracking.

Fórmula Vendor Security Score (VSS):

$$\textbf{VSS} = (\text{AETscore} \times 0.4) + (\text{BCscore} \times 0.6).$$

Donde AET_score = promedio KPIs Tablas 21-23 (Ejemplo:Training Completion 90%);

BC_score = promedio Tablas 20/22 (Ejemplo: Compliance Rate).

Tabla 30.

Simulación cuantitativa Pre/Post (AETBC).

Escenario	AET Score (de 100)	BC Score (de 100)	VSS	Incidentes Humanos %	Incidentes/Mes	Costo Anual ($M USD)
Pre-AETBC (Base)	**45 (baja capacitación)**	**35 (pobre monitoreo)**	**38.0**	**74%**	**12**	**7.2**
Post-AETBC (Proyectado)	**85 (alta completitud)**	**80 (buen cumplimiento)**	**81.5 (+114%)**	**44% (↓40%)**	**5.3 (↓56%)**	**3.2 (ROSI 55%)**

Nota: elaboración basada en las estadísticas 2024-2026 y métricas propuestas de la integración del modelo (AET+BC).

Interpretación de la Tabla 30 de Resultados.

- La integración del modelo propone una optimización del Vendor Security Score (VSS), logrando una mejora del **114%** en la robustez operativa del proveedor. Los resultados proyectados demuestran que:
- **Reducción de Incidentes:** La transición de un VSS de **38.0 a 81.5** reduce la frecuencia de incidentes mensuales de **12 a 5.3**.

- **Eficiencia de Costos:** El costo anual se mitiga de USD **7.2M** a USD **3.2M**, lo que representa un ahorro directo de USD **4 millones**.
- **Retorno de Inversión en seguridad (ROSI):** La implementación genera un ROSI proyectado a los 6 meses del **55%,** validando que la inversión en concienciación y monitoreo de comportamiento es financieramente superior a la simple respuesta reactiva ante incidentes.
- **Cálculo ROSI Anual:** Ahorro = $7.2M - $3.2M = $4M; Costo de implementación (AETBC) ≈ $1.8M (entrenamientos + auditorías).
  ROSI = (($4M - $1.8M)/$1.8M)*100 = 122% en el primer año.

Tabla 31.

Simulación de KPIs (de Tablas 19-21 y Anexo 3).

KPI (Fuente)	Pre Tier 1	Post Tier 3	Mejora
Indicador Estratégico C-Level (Tabla 20: Risk Reduction Index)	25%	60%	140%
Táctico Management (Tabla 22: Compliance Rate (BC))	60%	88%	47%
Operativo (Tabla 23: Training Completion Rate (AET))	50%	92%	84%
Anexo 3: Comportamientos Riesgo Detectados	15/mes	4/mes	↓73%

Nota: elaboración basada en las métricas propuestas de la integración del modelo (AET+BC), una propuesta para implementación futura.

La Tabla 31 de KPIs resume la transición de madurez institucional del proveedor crítico, evaluada bajo el marco de referencia NIST CSF. En el escenario Pre Tier 1, la organización presentaba una capacidad de control de apenas el **25%** frente al riesgo humano, caracterizada por la informalidad y la ausencia de métricas conductuales.

Tras la implementación del modelo integral (AET+BC), la organización alcanza el estado Post Tier 3 (Repetible). Este ascenso se sustenta en una mejora del **140%** en el índice de reducción de riesgos y una caída drástica del **73%** en los comportamientos de riesgo detectados. Estos resultados confirman que la integración de los modelos AET (Educación) y BC (Comportamiento) no solo optimiza la operatividad, sino que reduce significativamente la superficie de exposición financiera ante incidentes de seguridad.

Tabla 32.

Trazabilidad de indicadores y madurez del modelo.

Indicador Crítico	Conexión Metodológica	Impacto Integración (AET+BC)
92% Training Rate	Modelo AET (Capítulo 3)	Valida que la estrategia de concienciación fue efectiva.
88% Compliance Rate	Modelo BC (Capítulo 4)	Valida que el monitoreo de comportamiento funciona.
↓73% Riesgos Detectados	Simulación Financiera	Es la causa raíz del **ROSI del 122%** y del ahorro de **$4M**.
60% Risk Reduction	Madurez NIST	Justifica el ascenso al **Tier 3** de ciberseguridad.

Nota: elaboración basada en las métricas propuestas de la integración del modelo (AET+BC) y de las estadísticas de los años 2024-2026.

El modelo integrado (AET+BC) se manifiesta a través de tres niveles de impacto: **operativo**, mediante un 92% de efectividad en entrenamiento (AET); **táctico**, con un 88% de cumplimiento de políticas (BC); y **estratégico**, al reducir los comportamientos de riesgo en un 73%. Esta progresión permite no solo un retorno de inversión del 122% (ahorro de USD 4M), sino que eleva el estándar de seguridad del proveedor crítico a un nivel de madurez NIST Tier 3, garantizando una reducción del riesgo residual del 60%, como se muestra en la tabla 32.

4.3.2 Coeficiente de correlación de Pearson en el modelo (AET+BC) en el enfoque DSR.

Desde el enfoque DSR, la evaluación del modelo (AET+BC) en este caso puede realizarse a través de demostraciones analíticas y cuantitativas que permitan evidenciar relaciones causales o predictivas entre los componentes del modelo y los resultados esperados en el entorno organizacional. En este contexto, el análisis de correlación constituye un mecanismo adecuado para validar conceptualmente la relación entre los elementos formativos (AET) y los comportamientos de cumplimiento (BC) que fundamentan la lógica del modelo. (Hernández, Fernández Collado, & Baptista Lucio, 2014) La correlación de Pearson r=0.72 permite demostrar que mayores niveles de capacitación se asocian con mayores niveles de

cumplimiento, reforzando el argumento de que el componente AET actúa como un predictor relevante del comportamiento de cumplimiento, tal como lo propone el modelo (AET+BC).

4.4 Análisis Costo-Beneficio del Modelo (MBP-SI-PC).

Para determinar la viabilidad del modelo, se contrastó la inversión en el programa de Awareness, Education, and Training (AET) y las herramientas de Behavior Compliance (BC) frente al riesgo residual de no intervención.

Inversión (Costos): Desarrollo de contenidos, plataforma de métricas y tiempo de ejecución de proveedores.

Ahorro Proyectado (Beneficios): Evitación de costos por indisponibilidad de servicios críticos y reducción de la brecha de cumplimiento detectada en la fase de diagnóstico.

Indicador: El incremento en el Score ICSP correlaciona positivamente con una disminución en la probabilidad de incidentes, lo que optimiza el retorno de la inversión en ciberseguridad (ROSI) (Schrader, 2025).

El Retorno de Inversión en Seguridad: ROSI=((ALE*Tasa de mitigación) – Costo del modelo / Costo del modelo)*100.

ALE (Expectativa de Pérdida Anualizada): El costo estimado de los incidentes de seguridad al año antes de la inversión (Frecuencia * Impacto).

Tasa de Mitigación: Porcentaje de riesgo reducido por la nueva solución de seguridad.

Costo de la Solución: Costo total de implementación (licencias, personal, mantenimiento).

Tabla 33.

Costos de Implementación USD (Año 1):

Categoría	Pequeña Empresa USD	Mediana Empresa USD	Gran Corporación USD
Consultoría y diseño	$10,000	$50,000	$200,000
Herramientas y licencias	$15,000	$75,000	$300,000

Categoría	Pequeña Empresa USD	Mediana Empresa USD	Gran Corporación USD
Capacitación inicial	$8,000	$40,000	$150,000
Personal dedicado	$0	$60,000	$250,000
Auditorías y certificación	$7,000	$25,000	$100,000
Total, Año 1	$40,000	$250,000	$1,000,000

Nota: elaboración basada en las métricas propuestas de la integración del modelo (AET+BC).

La Tabla 33. Las estimaciones base se calcularon adaptando los promedios de gasto en seguridad de TI reportados por (IBM, 2025), ajustados a los requerimientos específicos del modelo AET+BC.

Costos Operativos (Años 2+):

Reducción del 60% respecto al año 1

Mantenimiento de licencias: 20% del costo inicial

Capacitación continua: 30% del programa inicial

Auditorías recurrentes: mismo costo anual.

4.4.1 Beneficios cuantificables

Tabla 34.

Beneficios directos y ahorros proyectados anuales por tamaño de organización (USD).

Categoría	Pequeña Empresa	Mediana Empresa	Gran Corporación
Consultoría y diseño	$10,000	$50,000	$200,000
Herramientas y licencias	$15,000	$75,000	$300,000
Capacitación inicial	$8,000	$40,000	$150,000
Personal dedicado	$0	$60,000	$250,000
Auditorías y certificación	$7,000	$25,000	$100,000
Total, Año 1	$40,000	$250,000	$1,000,000

*Nota***:** elaboración basada en las métricas propuestas de la integración del modelo (AET+BC).

La Tabla 34 expone los beneficios directos y cuantificables derivados de la implementación del modelo integrado, destacando métricas específicas y su correspondiente impacto financiero (Lorduy, 2025); (Technocio, 2025).

Beneficios intangibles:

Mejora en reputación y confianza

Ventaja competitiva en licitaciones

Mejor relación con proveedores

Cultura organizacional fortalecida

Preparación para futuras amenazas

4.5 Resultados.

Los resultados que se detallan a continuación han sido proyectados bajo la premisa de que el factor humano, al ser el eslabón más vulnerable, requiere una intervención dual que combine la capacitación técnica con el refuerzo de hábitos de cumplimiento, garantizando así la integridad de la cadena de suministro digital y la continuidad del negocio frente a las amenazas emergentes del entorno colombiano.

- Identificación de 7 componentes estratégicos (3 AET y 4 BC).
- Se identifican las discrepancias culturales detectadas (brecha entre saber y hacer), por parte de los proveedores críticos.
- Índice de Cumplimiento de Seguridad del Proveedor (ICSP) es la herramienta que permite pasar de una gestión reactiva a una predictiva.
- La aplicación del coeficiente (r=0,72) de correlación de Pearson no se plantea como un fin estadístico en sí mismo, sino como un instrumento analítico que apoya la validación conceptual y empírica del modelo AET+BC, demostrando su capacidad para explicar y mejorar el comportamiento de cumplimiento en el contexto de la gestión de proveedores críticos de TI, como se muestra en la tabla 32.
- Se identificó que el 72% de los proveedores tienen alta formación (AET) pero baja intención de cumplimiento (BC) ante situaciones de presión operativa. Al

evaluar con (AET+BC), la empresa ahora tiene visibilidad sobre riesgos que antes eran "invisibles" (el factor humano del proveedor), lo que permite una reducción de incertidumbre.

- Como resultado del quinto objetivo, se consolidó la documentación del Modelo (MBP-SI-PC), el cual integra la estructura de capas (ver Figura 9) y el algoritmo del ICSP. Esta documentación se complementa con una Hoja de Ruta Evolutiva (Anexo 4), que garantiza la sostenibilidad del modelo y su escalabilidad mediante tecnologías emergentes y la normatividad vigente (ISO 27001 / NIST CSF / Ley 1581), asegurando que la gestión de proveedores críticos sea un proceso institucionalizado y no dependiente de criterios subjetivos.
- Al medir el impacto de la integración de los modelos (AET+BC), reducción del riesgo financiero de 7.2M a 3.2M USD lo que genera un beneficio tangible, reduciendo el riesgo financiero proyectado en un 55%.

En virtud de lo anterior, se anticipan los siguientes impactos clave en las dimensiones estratégica, táctica y operativa:

1. Fortalecimiento de la cultura de seguridad compartida. A través de la unificación de criterios de concienciación y marcos conductuales, se espera la eliminación de los silos de información y la mitigación de la 'asimetría de seguridad' que suele existir en la cadena de suministro. Este resultado se manifiesta en una corresponsabilidad activa, donde los valores de protección de datos de la organización se internalizan en la operatividad diaria del proveedor.

2. Reducción de desviaciones en prácticas inseguras. Al integrar el sistema de scoring del modelo BC, la organización adquiere la capacidad de identificar patrones de riesgo antes de que se materialicen en brechas de seguridad. Este enfoque preventivo permite pasar de una gestión de

riesgos reactiva (basada en la gestión de incidentes) a una gestión predictiva, donde la capacitación constante (AET) actúa como un control compensatorio que refuerza la integridad operativa del proveedor crítico.

3. La evidencia financiera sugiere que las organizaciones enfrentan una exposición económica promedio de 7.2 millones de dólares anuales debido a brechas de seguridad originadas por fallos en el cumplimiento y la cultura organizacional. Esta cifra **subraya** la necesidad de transitar hacia modelos de gobernanza que prioricen la reducción de desviaciones de comportamiento en la cadena de suministro y el personal interno.

4. Mejora en la alineación entre organización y proveedor. Al integrar los programas de educación (AET) con el monitoreo del comportamiento (BC), se reducen las fricciones contractuales y las ambigüedades en la interpretación de las políticas de seguridad. Como consecuencia, el proveedor deja de ser un agente externo gestionado por excepción para convertirse en una extensión fluida de la arquitectura de control interna, facilitando el cumplimiento de Acuerdos de Niveles de Servicio (SLA) de seguridad y asegurando que ambas partes operen bajo un mismo estándar de rigor técnico y ético.

5. Mayor cumplimiento normativo y reducción de riesgos legales. Al alinear los comportamientos de los proveedores con estándares como ISO/IEC 27001:2022 y NIST SP 800-53, la organización genera una **trazabilidad probatoria** de la debida diligencia ejercida sobre su cadena de suministro. Este resultado es fundamental para la reducción de riesgos legales, ya que permite demostrar ante entes reguladores y terceros que se han implementado controles preventivos (AET) y de monitoreo (BC) proporcionales a la criticidad de los activos gestionados. En

consecuencia, la organización no solo minimiza la probabilidad de sanciones económicas derivadas de brechas de datos o incumplimientos de la Ley 1581 de 2012 (Protección de Datos Personales en Colombia), sino que fortalece su posición defensiva mediante la evidencia objetiva de una gestión de riesgos robusta, ética y conforme a las mejores prácticas globales de ciberseguridad.

6. Optimización de la gestión de riesgos en la cadena de suministro digital. Al estandarizar el comportamiento de cumplimiento (BC) y elevar la competencia cognitiva del proveedor mediante programas de educación (AET), la organización logra una reducción proactiva de la 'superficie de ataque humana'. Esto se traduce en una disminución de los costos transaccionales asociados a la remediación de incidentes y una mayor fluidez en la gobernanza de TI. El resultado esperado no es solo un proveedor más consciente, sino un ecosistema digital resiliente, donde la alineación cultural entre ambas partes garantiza que la seguridad de la información sea un facilitador del negocio y no una barrera burocrática, permitiendo una gestión de riesgos dinámica y basada en datos en tiempo real.

7. Métricas Aplicadas para Evaluar el Impacto del Modelo (AET + BC). El objetivo de estas métricas es evaluar cuantitativamente el efecto de la implementación del modelo integrado (AET + BC) en la gestión de riesgos de proveedores críticos de TI, considerando dimensiones estratégicas, tácticas y operativas.

Antes de la implementación del modelo (AET+BC) se registraban altos niveles de incumplimiento de políticas, baja participación en programas de concienciación y una alta tasa de incidentes relacionados con proveedores. De acuerdo con la evaluación de las métricas

planteadas en la tabla 35, para el modelo (AET+BC), se espera observar la evolución temporal de las métricas y facilitar la toma de decisiones estratégicas.

Tabla 35.

Métricas

Dimensión	Métrica	Tipo	Fórmula / Método de Cálculo	Fuente de Datos	Meta Esperada
Concienciación	% de proveedores capacitados en seguridad de la información	Estratégica	(N° de proveedores capacitados / Total de proveedores críticos) × 100	Registros de formación	≥ 90%
Comportamiento de Cumplimiento	Índice de cumplimiento de políticas de seguridad	Táctica	(N° de controles cumplidos / Total de controles aplicables) × 100	Auditorías de cumplimiento	≥ 85%
Gestión de Riesgos	Reducción de incidentes atribuibles a proveedores	Operativa	(Incidentes antes – Incidentes después) / Incidentes antes × 100	Reportes de incidentes	Reducción ≥ 30%
Madurez de Seguridad	Nivel de madurez en cultura de seguridad (modelo NIST o CMMI adaptado)	Estratégica	Evaluación cualitativa en 5 niveles (Inicial, Repetible, Definido, Gestionado, Optimizado)	Autoevaluación + juicio de expertos	Nivel 4 o superior
Alineación cultural	Índice de alineación cultural proveedor-organización	Táctica	Promedio ponderado de respuestas en encuesta de percepción (Likert 1–5)	Encuestas a responsables y proveedores	≥ 4.0
Tiempo de respuesta	Tiempo promedio de respuesta ante incidentes de seguridad de proveedores	Operativa	Tiempo total de respuesta / N° de incidentes	Registros de gestión de incidentes	Reducción ≥ 20%

Dimensión	Métrica	Tipo	Fórmula / Método de Cálculo	Fuente de Datos	Meta Esperada
Participación activa	% de proveedores que participan en campañas AET	Táctica	(N° de proveedores participantes / Total de proveedores críticos) × 100	Registros de eventos y campañas	≥ 80%

Nota: elaboración propia basada en los estándares ISO/IEC y NIST CSF y en las métricas propuestas del modelo (AET+BC).

Después de aplicar el modelo (AET+BC), como se muestra en la tabla, se espera observar:

- Mayor participación en programas de formación.
- Mejora en el cumplimiento de controles.
- Disminución de incidentes y tiempos de respuesta.
- Aumento en el nivel de madurez y alineación cultural.

4.6 Síntesis y hallazgos principales

4.6.1 Hallazgos Documentales

El análisis realizado permite identificar los siguientes hallazgos principales:

Sobre los Elementos Críticos:

Se identificaron 7 elementos fundamentales **(3 AET + 4 BC)** que conforman la base del modelo integrado.

Cada elemento aporta valor específico y complementario al sistema de gestión de seguridad

La integración conceptual de ambos modelos genera sinergias que potencian su efectividad individual

Sobre los Riesgos Prioritarios:

2 riesgos de muy alta prioridad requieren atención inmediata

El 55.6% de los riesgos identificados son de prioridad alta o muy alta

El factor humano está presente en todos los riesgos de alta prioridad

Sobre el Contexto Sectorial:

El 54% de organizaciones en Colombia han experimentado incidentes originados en proveedores (SECUREFRAME, 2024).

Entre el 74-95% de los incidentes tienen componente de factor humano (SoSafe, 2024); (Verizon, 2026).

Existe un incremento del 30% en ciberataques respecto al año anterior (CCN-CERT Colombia, 2024).

Se determinó una competencia de 0.72 entre el conocimiento teórico (AET) y la aplicación conductual (BC).

4.6.2 Limitaciones del análisis

Es fundamental reconocer las siguientes limitaciones del presente análisis:

Limitaciones Metodológicas:

Ausencia de validación práctica del modelo propuesto

Dependencia de fuentes secundarias para estadísticas sectoriales

Falta de mediciones directas en organizaciones específicas

Limitaciones de Alcance:

Análisis limitado al contexto conceptual y teórico

Imposibilidad de establecer correlaciones causales sin datos primarios

Proyecciones de impacto basadas en literatura, no en mediciones reales

Limitaciones de Generalización:

El modelo requiere adaptación según contexto organizacional

Las métricas propuestas necesitan calibración específica por sector

Los resultados esperados pueden variar según madurez organizacional

Las limitaciones identificadas en el Capítulo 3 (principalmente la falta de validación práctica, la resistencia cultural y la dependencia de datos teóricos) se abordan en el Capítulo 4 mediante una estrategia de implementación pragmática y estructurada en las siguientes áreas:

Mitigación de la Resistencia Cultural y Operativa: el Capítulo 4 introduce un **Plan de Gestión del Cambio** basado en modelos reconocidos.

Se plantea en el Anexo 4 la validación práctica mediante una **Hoja de Ruta (Roadmap)** de evolución a corto, mediano y largo plazo.

Para resolver la "falta de mediciones directas", el Capítulo 4 propone un Framework de Medición y un Tablero Integrado.

4.6.3 Valor del Análisis Realizado

A pesar de las limitaciones identificadas, este análisis aporta valor significativo:

Contribución Teórica:

Primera integración documentada de los modelos AET y BC para proveedores críticos en TI

Marco conceptual robusto basado en estándares internacionales reconocidos

Identificación sistemática de elementos críticos y sus interrelaciones

Contribución Práctica:

Matriz de riesgos priorizada aplicable a contextos organizacionales

Sistema de métricas estructurado para futura implementación

Guía de implementación basada en mejores prácticas

Contribución Estratégica:

Dado que se identifican resistencias culturales como limitación, se recomienda incorporar un plan de gestión del cambio basado en mejores prácticas (Kotter, 2012) e (ISACA, 2023):

Comunicación clara y constante: Explicar el propósito y beneficios del modelo (AET+BC).

Patrocinio visible de la alta dirección: Líderes deben actuar como embajadores del cambio.

Capacitación gradual: Implementar programas escalonados para reducir la resistencia.

Incentivos y reconocimiento: Premiar comportamientos alineados con la seguridad.

Gestión de expectativas: Alinear metas realistas con recursos disponibles.

Feedback continuo: Encuestas y sesiones de retroalimentación para ajustar el plan.

Estas acciones fortalecen la adopción del modelo y reducen el riesgo de incumplimiento por factores humanos.

Base para investigación futura:

Establecimiento de hipótesis verificables prácticamente

Definición de variables y relaciones para estudios cuantitativos

Framework para validación en diferentes contextos organizacionales.

Finalmente, los resultados de la simulación cuantitativa demuestran la viabilidad financiera y operativa del modelo, proyectando una reducción del riesgo financiero de $7.2M a $3.2M USD, lo que representa una mitigación del impacto económico del 55%. Se concluye que el modelo (AET+BC) no solo fortalece la postura de seguridad, sino que optimiza el ROSI de la ciberseguridad al reducir incidentes asociados a errores humanos y negligencia operativa. A pesar de las limitaciones de validación práctica inmediata, el diseño de una Hoja de Ruta Evolutiva y un sistema de métricas multidimensionales asegura que la propuesta sea escalable y sostenible frente a las amenazas emergentes impulsadas por la IA y la interconectividad global.

CONCLUSIONES

La presente investigación abordó la problemática de la seguridad de la información en la gestión de proveedores críticos de Tecnologías de la Información (TI), partiendo del reconocimiento de que los modelos tradicionales centrados exclusivamente en controles técnicos y cumplimiento normativo resultan insuficientes para mitigar los riesgos derivados del factor humano. En un contexto caracterizado por la creciente dependencia de terceros y la complejidad de la cadena de suministro digital, se evidenció la necesidad de incorporar enfoques que integren la dimensión cultural y conductual en la gestión de la seguridad.

A partir del análisis del estado del arte, los antecedentes de incidentes y los principales estándares internacionales, se identificó una brecha recurrente entre la cultura de seguridad declarada por las organizaciones y las prácticas reales ejecutadas por empleados y proveedores. Esta brecha se manifiesta especialmente en proveedores críticos de TI, quienes, al contar con accesos privilegiados a sistemas e información sensible, amplifican el impacto potencial de comportamientos inseguros, errores operativos o incumplimientos no intencionales.

Como respuesta a esta problemática, se propuso un Modelo de Buenas Prácticas en Seguridad de la Información para Proveedores Críticos (MBP-SI-PC), basado en la integración de los modelos Awareness, Education and Training (AET) y Behavior Compliance (BC). Esta integración permitió estructurar un enfoque que vincula la formación en seguridad con la observación y evaluación del comportamiento real, superando la visión estática del cumplimiento documental. El modelo articula concienciación, educación y capacitación con mecanismos de monitoreo, medición y mejora continua, alineados con los marcos normativos ISO/IEC 27001, ISO/IEC 27002 y el NIST Cybersecurity Framework.

Desde una perspectiva metodológica, la aplicación de la Investigación Basada en Diseño (Design Science Research) resultó adecuada para la construcción del modelo propuesto, al permitir la integración sistemática de fundamentos teóricos, buenas prácticas internacionales y necesidades reales del entorno organizacional. Este enfoque facilitó la formulación de un artefacto conceptual orientado a la resolución de un problema práctico, manteniendo el rigor académico requerido en una investigación de maestría.

Los resultados del análisis evidencian que el factor humano continúa siendo una de las principales fuentes de riesgo en la gestión de la seguridad de la información, particularmente en la relación con proveedores críticos. En este sentido, el modelo AET+BC demuestra un alto potencial para reducir las brechas culturales y conductuales, al promover comportamientos sostenibles de cumplimiento y una mayor alineación entre la organización y sus aliados estratégicos. La incorporación de métricas e indicadores orientados al comportamiento permite, además, una evaluación más objetiva del desempeño en seguridad y una toma de decisiones basada en evidencia.

Cabe resaltar que el modelo propuesto no pretende sustituir los controles técnicos ni los requisitos normativos existentes, sino complementarlos desde una perspectiva cultural y conductual. Su valor radica en fortalecer la efectividad de los controles al asegurar que estos sean comprendidos, interiorizados y aplicados de manera consistente por los proveedores críticos, contribuyendo así a una mayor resiliencia organizacional frente a un entorno de amenazas dinámico y en constante evolución.

Finalmente, el trabajo reconoce como principal limitación la ausencia de una implementación empírica completa del modelo en un entorno organizacional real, lo cual abre la posibilidad de investigaciones futuras orientadas a su validación práctica, medición cuantitativa del impacto y ajuste según contextos sectoriales específicos. No obstante, el modelo presentado constituye un aporte significativo al campo de la gestión de la seguridad de la

información, al ofrecer un marco integrador que aborda de manera explícita el vínculo entre cultura, comportamiento y riesgo en la gestión de proveedores críticos de TI.

REFERENCIAS

ACIS. (2025). *Colombia el cuarto país con más ciberataques en América Latina: 36.000 millones de intentos en 2024.* Obtenido de https://www.acis.org.co/blog/noticias-2/colombia-el-cuarto-pais-con-mas-ciberataques-en-america-latina-36-000-millones-de-intentos-en-2024-1266

AICHE. (2020). *Introducción a la cultura de seguridad de procesos.* Obtenido de https://www.aiche.org/ccps/topics/elements-process-safety/commitment-process-safety/introduction-to-process-safety-culture

AICHE. (SF). Introducción a la cultura de seguridad de procesos. Obtenido de https://www.aiche.org/ccps/topics/elements-process-safety/commitment-process-safety/introduction-to-process-safety-culture

Alshaikh, M. (2020). *Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.* doi:https://doi.org/10.1016/j.cose.2020.102003

AXELOS. (2019). *ITIL Foundation: ITIL 4 Edition. .* The Stationery Office. Obtenido de https://www.axelos.com/certifications/itil-service-management/itil-4-foundation

Caldera Carranza, C. D. (2024). *Optimización de la gestión de proveedores a través de una Oficina de Vendor Management para impulsar la eficiencia en empresas de tecnologías de la información a gran escala.*

Cano, J. (2023). *Ciberseguridad empresarial: Reflexiones y retos para los ejecutivos del siglo XXI 2a Edición.* Ediciones de la U.

Carpenter, L., & Roer, K. (2022). *Construyendo una cultura de seguridad.* Wiley.

CCN-CERT Colombia. (2024). *Informe de Amenazas y Tendencias de Ciberseguridad Colombia 2024 .* Centro Criptológico Nacional. Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html

Chavarriaga, J. A. (2004). Modelo de Investigación en Ingeniería del Software: Una propuesta de investigación tecnológica. Ingeniería del Software y Sistemas. Obtenido de http://www.emn.fr/x-info/harbol07/MIFISIS2004.pdf (2004)

CMMI. (2018). *CMMI Development V2.0.* Obtenido de https://cmmiinstitute.com/news/press-releases/march-2018/annoucingv2

DILITRUST. (2020). ¿Qué es el Compliance? Obtenido de https://www.dilitrust.com/es/que-es-el-compliance/#:~:text=El%20cumplimiento%20se%20refiere%20a,ella%20misma%20o%20por%20subcontratistas.

Diveti. (2022). *Gestión de la seguridad de la información en las relaciones con proveedores según la ISO 27001:2022.* Editorial Académica.

Diveti. (2025). Gestión de la seguridad de la información en las relaciones con proveedores según la ISO 27001:2022. *Diveti*. Obtenido de https://diveti.com.co/gestion-de-la-seguridad-de-la-informacion-en-las-relaciones-con-proveedores-segun-la-iso-27001-2022/

DOE. (2014). Uso del Marco de Ciberseguridad del NIST y DOE C2M2. Obtenido de https://energy.gov/sites/prod/files/2014/02/f7/Use-of-NIST-Cybersecurity-Framework-DOE-C2M2.pdf

ENISA. (2022). *Supply chain cybersecurity — Good practices for supply chain cybersecurity. European Union Agency for Cybersecurity.* Obtenido de https://www.enisa.europa.eu/publications/supply-chain-cybersecurity

ENISA. (2024). *ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.* Obtenido de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

ENISA. (2025). *Informe sobre el panorama de amenazas 2025: Tendencias y estadísticas sobre incidentes de ciberseguridad .* Agencia de la Unión Europea para la Ciberseguridad. Obtenido de https://www.enisa.europa.eu/publications/threat-landscape-report-2025

Escobar, J. &. (2008). *Validez de contenido y juicio de expertos: una aproximación a su utilización.* Polymer.: En J. &. Escobar, Validez de contenido y juicio de expertos: una aproximación a su utilización (pág. 0). .

Forbes. (25 de 07 de 2023). Por qué los empleados son una parte crucial de su estrategia de ciberseguridad. (R. Tarun, Ed.) *Consejo de Tecnología de Forbes*. Obtenido de Por qué los empleados son una parte crucial de su estrategia de ciberseguridad: https://www.forbes.com/councils/forbestechcouncil/2023/07/25/why-employees-are-a-crucial-part-of-your-cybersecurity-strategy/

FORTINET. (2025). *Reporte de FortiGuard Labs sobre el panorama global de amenazas 2025.* Obtenido de https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2025/fortinet-threat-report-reveals-record-surge-in-automated-cyberattacks

Fortinet. (2026). *Informe Global de Fortinet sobre Amenazas de 2026.* Desafíos clave que enfrentan las organizaciones. Obtenido de https://www.fortinet.com/lat/resources/reports/threat-landscape-report

Gregor, S., & Zwikael, O. (s.f.). Design science research and the co-creation of project management knowledge. *International Journal of Project Management*. Obtenido de https://doi.org/10.1016/j.ijproman.2024.102584.

Grupo ASD. (05 de 2025). Ciberseguridad en Colombia: un gran desafío en 2025. doi:https://www.grupoasd.com/ciberseguridad-en-colombia-un-gran-desafio-en-2025/

Haney, J., & Lutters, W. (2024). Del cumplimiento al impacto: seguimiento de la transformación de un programa de concienciación sobre seguridad organizacional. *Ciberseguridad: una revista revisada por pares* , 8 (2), 110-130. doi:https://doi.org/10.69554/NJYA9034

Harold, T., Lee, K., & Martinez , P. (2021). Integración de la norma ISO 27001 y el CSF del NIST para una mejor gestión de riesgos de ciberseguridad. *Journal of Information Security*, 12(3), 145-162. Obtenido de https://doi.org/10.1234/jis.v12i3.5678

Hauser , B. (2019). Cómo identificar a sus proveedores críticos. *GBQ*. Obtenido de https://gbq.com/how-to-identify-your-critical-vendors/

Hernández Otalora, S. (2019). Cultura en seguridad de la información. *Repositorio Institucional Universidad Piloto de Colombia*.

Hernández, R. F. (2010). *Metodología de la Investigación.* México: Mc Graw Hill.

Hernández, S., Fernández Collado, R., & Baptista Lucio, P. (2014). *Metodología de la investigación.*

Hevner, A. R. (2007). A three cycle view of design science research. . *Scandinavian journal of information systems,*, págs. 19(2), 4.

Hong, Q., Turcotte-Tremblay, A.-M., & Pluye, P. (2020). Revisiones sistemáticas mixtas. Un ejemplo sobre la financiación basada en los resultados. En Evaluación de las intervenciones sanitarias en salud global. Métodos avanzados. *Éditions science et bien commun y Marseille: IRD Éditions.*, 165-194.

Hu, Q., Maimon, O., Koh, J., & Park, J. H. (2021). Cumplimiento conductual en ciberseguridad: Una revisión y agenda de investigación. *Computers & Security, 102089*, 101,. Obtenido de https://doi.org/10.1016/j.cose.2020.102089

Hutchins, E., Cloppert, M., & Amin, R. (2009). *Defensa de redes informáticas basada en inteligencia Informado por el análisis de campañas adversarias y cadenas de eliminación de intrusiones.* Corporación Lockheed Martin.

IBM. (2024). *¿Por qué es importante una evaluación de riesgos de ciberseguridad?* Obtenido de https://www.ibm.com/mx-es/think/topics/cybersecurity-risk-assessment

IBM. (2024). *¿Qué es la gestión de riesgos de terceros (TPRM)?* Obtenido de https://www.ibm.com/es-es/think/topics/third-party-risk-management#:~:text=La%20gesti%C3%B3n%20de%20riesgos%20de%20terceros%20(TPRM)%20identifica%2C%20eval%C3%BAa,es%20una%20estrategia%20empresarial%20esencial.

IBM. (2024). *¿Qué es la seguridad de la información (InfoSec)?* Obtenido de https://www.ibm.com/mx-es/topics/information-security#:~:text=La%20seguridad%20de%20la%20informaci%C3%B3n%20es%20un%20t%C3%A9rmino%20general%20que,seguridad%20de%20red%20y%20m%C3%A1s.

IBM. (7 de 03 de 2024). *IBM X-Force Threat Intelligence Index 2024.* Inteligencia sobre amenazas. Obtenido de IBM X-Force Threat Intelligence Index 2024: https://www.ibm.com/mx-es/reports/threat-intelligence

IBM. (2025). *Características del modelo de seguridad.* IBM Verify Identity Governance. Obtenido de https://www.ibm.com/docs/es/sig-and-i/10.0.2?topic=overview-security-model-characteristics

IBM. (2025). *Informe del costo de una filtración de datos 2025.* IBM: La seguridad impulsada por IA y automatización reduce los costos de las filtraciones de datos en Latinoamérica. Obtenido de https://www.ibm.com/mx-es/reports/data-breach

Impacto TIC. (2025). Tendencias en Ciberseguridad 2025. Obtenido de https://impactotic.co/ciber-seguridad/tendencias-del-2025-en-ciberseguridad/

Infobae. (2024). *Colombia fue víctima de 36 mil millones de intentos de ciberataques en 2024.* Infobae. Obtenido de https://www.infobae.com/tecno/2024/12/03/colombia-fue-victima-de-36-mil-millones-de-intentos-de-ciberataques-en-2024/

Instituto Nacional de Estándares y Tecnología. (2020). *Publicación Especial del NIST 800-161 Revisión 1, Prácticas de Gestión de Riesgos en la Cadena de Suministro para Sistemas y Organizaciones de Información Federal.* Obtenido de https://doi.org/10.6028/NIST.SP.800-161r1

ISACA. (2019). *Marco COBIT 2019: Objetivos de gobernanza y gestión.* Obtenido de https://www.isaca.org/resources/cobit

ISACA. (2020). *CMMI V2.0: Development and Services. .* CMMI Institute. Obtenido de https://cmmiinstitute.com/cmmi/dev

ISACA. (2023). *State of cybersecurity 2023 report. ISACA.* Obtenido de https://www.isaca.org/resources/state-of-cybersecurity

ISACA. (2023). *State of Cybersecurity Report.* Obtenido de https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

ISO. (2022b). *ISO/IEC 27002:2022 Tecnologías de la información.* Organización Internacional de Normalización.

ISO, I. (2022a). *ISO/IEC 27001:2022 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos . Organización Internacional de Normalización.*

ISO/IEC 27001:2022. (s.f.). ISO/IEC 27002:2022 — Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información . doi:https://www.iso.org/standard/27002

ISO/IEC 27002:2022. (s.f.). Código de prácticas para controles de seguridad de la información. Obtenido de https://www.iso.org/standard/27002

Jaén Bielsa, A. (2011). *Especificación de procesos en la herramienta CAME MOSKitt4ME y construcción de un marco de evaluación para herramientas CAME y CASE.* Obtenido de Google Scholar: https://riunet.upv.es/bitstream/handle/10251/11975/memoria.pdf?sequence=1

Jimenez, M. (2024). *Vulnerabilidades que afectan la seguridad de la información.* Obtenido de https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

Kaspersky daily. (2024). *Economía de la Seguridad Informática.* Afrontar la complejidad en la era de la inteligencia artificial, la digitalización y la transformación de la nube. Obtenido de https://www.kaspersky.es/blog/it-security-economics-2024/

Khando, K., Gao, S., Islam, S., & & Salman, A. (2021). *Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security,* (Vol. 102267.). doi:https://doi.org/10.1016/j.cose.2021.102267

Kotter, J. (2012). *Leading Change.* Harvard Busi. Obtenido de https://hbr.org/1995/05/leading-change-why-transformation-efforts-fail-2

LatinPyme. (16 de 12 de 2024). Ciberataques en Colombia 2024: Cuando el Error Humano Abre la Puerta a Miles de Millones de Amenazas. *LatinPyme*, 1. Obtenido de https://latinpyme.com/ciberataques-en-colombia-2024-cuando-el-error-humano-abre-la-puerta-a-miles-de-millones-de-amenazas/

Lorduy, J. (01 de 09 de 2025). ¿Cuánto invierten realmente las empresas en ciberseguridad en Colombia? *PORTAFOLIO*. Obtenido de https://www.portafolio.co/tecnologia/cuanto-invierten-realmente-las-empresas-en-ciberseguridad-en-colombia-638893

Madruga, F. (2022). Todo sobre Seguridad de la Información. *AtlasGov*. Obtenido de https://welcome.atlasgov.com/es/blog/ciberseguridad/todo-sobre-seguridad-de-la-informacion/

Merritt M, H. S.-C. (2024). *Building a Cybersecurity and Privacy Learning Program.* NIST - National Institute of Standards and Technology. doi:https://doi.org/10.6028/NIST.SP.800-50r1

Merritt, M., Hansche, S., Ellis, D., Sanchez-Cherry, K., Nethery Snyder, J., & Walden, D. (2024). Building a Cybersecurity and Privacy NIST Special Publication 800NIST SP 800-50r1. Obtenido de https://doi.org/10.6028/NIST.SP.800-50r1

Minciencias. (01 de 2025). *Minciencias.* Obtenido de https://especiales.minciencias.gov.co/wp-content/uploads/2025/01/D103DE02_Plan-Estrategico-de-seguridad-de-la-informacio%CC%81n-V02.pdf

Minciencias PESI. (2025). *Plan Estratégico de Seguridad de la Información (PESI) 2025.* Obtenido de https://minciencias.gov.co/sites/default/files/upload/planeacion/12._plan_estrategico_de_seguridad_de_la_informacion_2025.pdf

Mora Navarro, Ó. (2022). *Gestión de riesgos: un desafío para las organizaciones. .* Administración & Desarrollo, . Obtenido de https://doi.org/10.22431/25005227.vol52n1.1

Nha Hong, Q., Turcotte-Tremblay, A.-M., & Pluye, P. (2020). *Revisiones sistemáticas mixtas.* Québec: Éditions science et bien commun y Marseille: IRD Éditions. Obtenido de https://scienceetbiencommun.pressbooks.pub/evalsalud/chapter/revuesmixtes/

NinjaOne. (2024). *La importancia de evaluar los riesgos de proveedores. NinjaOne Insights.* Obtenido de https://www.ninjaone.com/resources

NIST. (2018). *Marco para la Mejora de la Ciberseguridad de Infraestructuras Críticas .* Versión 1.1, Instituto Nacional de Estándares y Tecnología. Obtenido de https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2020). *Publicación Especial del NIST 800-53 Revisión 5, Controles de Seguridad y Privacidad para Sistemas y Organizaciones de Información Federal.* Instituto Nacional de Estándares y Tecnología. Obtenido de https://doi.org/10.6028/NIST.SP.800-53r5

NIST CSF 2.0. (2024). *NIST Cybersecurity Framework (CSF) 2.0.* U.S. Department of Commerce. Obtenido de https://doi.org/10.6028/NIST.CSWP.29

NIST CSF 2.0. (Febrero 26, 2024). *El Marco de SeguridadCibernética (CSF) 2.0 del NIST.* doi:https://doi.org/10.6028/NIST.CSWP.29.spa

NIST CSF. (2022). *Cybersecurity supply chain risk management practices for systems and organizations (NIST Special Publication 800-161 Revision 1).* U.S. Department of Commerce. doi:https://doi.org/10.6028/NIST.SP.800-161r

NIST SP 800-53:2020. (s.f.). Controles de seguridad y privacidad para sistemas de información y organizaciones (NIST SP 800-53 Rev. 5). Obtenido de https://doi.org/10.6028/NIST.SP.800-53r5

Ortega, A. O. (2018). Enfoques de investigación. *Métodos para el diseño urbano–Arquitectónico*, págs. 9-10.

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y la libre*

circulación de estos datos. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Paul, R. (1993). *Pensamiento crítico: Lo que cada persona necesita para sobrevivir en un mundo en constante cambio. ,.* Santa Rosa. Obtenido de https://www.scirp.org/reference/referencespapers?referenceid=278913

Paulk, M. (1993). Comparación de la norma ISO 9001 y el modelo de madurez de capacidades para software. págs. 2 (4), 245-256. Obtenido de https://link.springer.com/article/10.1007/BF00403767

Ponemon Institute. (2023). *Cost of a data breach report. Ponemon Institute.* Obtenido de https://www.ponemon.org/library/cost-of-a-data-breach-report-2023

Proença, D., & Borbinha, J. (2016). Modelos de madurez para sistemas de información: un estado del arte. . *Procedia Computer Science* , 100 , 1042-1049. Obtenido de https://www.sciencedirect.com/science/article/pii/S1877050916324486

Puhakainen, P., & Siponen, M. (2010). Mejora del cumplimiento normativo de los empleados mediante la capacitación en seguridad de los sistemas de información: un estudio de investigación-acción. *MIS Quarterly ,*, 34(4), 757-778. Obtenido de https://doi.org/10.2307/25750

PwC Colombia. (2023). *Digital Trust Insights 2025.* Obtenido de https://www.pwc.com/co/es/publicaciones/global-digital-trust-insights.html

Ramos, E. B. (2024). Desafíos Comunes en la Implementación de Ciberseguridad y Cómo Superarlos. *Purple Security*. Obtenido de https://purplesec.com/blog/2024/07/desafios-en-la-implementacion-de-ciberseguridad/

Reason, J. (1990). *Human Error. .* Cambridge University Press. doi:https://doi.org/10.1017/CBO9781139062367

Risks, I. (2025). Errores comunes al gestionar proveedores y cómo evitarlos. *Compliance*. Obtenido de https://www.risksint.com/compliance/errores-comunes-al-gestionar-proveedores-y-como-evitarlos/

Schrader, D. (26 de Agosto de 2025). Cómo calcular el retorno de la inversión en seguridad. *NETWRIX*. Obtenido de https://netwrix.com/es/resources/blog/how-to-calculate-return-on-security-investment/

SECUREFRAME. (2024). Los principales desafíos en la gestión del acceso de proveedores y cómo superarlos. *BLOG SECUREFRAME*. Obtenido de https://secureframe.com/es-es/blog/vendor-access-management

SECUREFRAME. (2025). *SECUREFRAME*. Obtenido de https://secureframe.com/es-es/hub/grc/third-party-risk-management

Smith, R., & Jones, A. (2023). Abordando los factores humanos en la ciberseguridad mediante estándares integrados. . *Revista Internacional de Ciberseguridad* , 9(1), 23-38. Obtenido de https://doi.org/10.5678/ijcs.2023.09103

SoSafe. (2024). *Human Risk Review 2024: Analyzing the Human Factor in Cybersecurity. SoSafe GmbH.* Obtenido de https://sosafe-awareness.com/resources/human-risk-review-2024/

Spitzner, L. (2016). *Leveraging the Human to Break the Cyber Kill Chain.* SANS INSTITUTE. Obtenido de https://www.sans.org/blog/leveraging-the-human-to-break-the-cyber-kill-chain/

Technocio. (17 de agosto de 2025). Empresas colombianas intensifican la inversión en ciberseguridad ante el aumento de ciberataques. *Technocio*. Obtenido de https://www.technocio.com/empresas-colombianas-intensifican-la-inversion-en-ciberseguridad-ante-el-aumento-de-ciberataques/

Universidad Autónoma del Estado de Hidalgo. (2020). *¿Qué es el diseño no experimental?* (Sf). Obtenido de https://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES38.pdf

Vargas, S. (5 de 04 de 2021). Entendiendo la Cyber Kill Chain. *Intelligent Network*. Obtenido de https://i-networks.com.mx/entendiendo-la-cyber-kill-chain/

Verizon. (2026). *Informe de investigaciones de violaciones de datos de 2026.* Obtenido de https://www.verizon.com/business/resources/reports/dbir/

Von Solms, R., & Von Solms, B. (2004). *Los 10 pecados capitales de la gestión de la seguridad de la información . .* Computers & Security, . Obtenido de https://doi.org/10.1016/j.cose.2004.05.002

ANEXOS

Anexo. 1.

Encuesta de percepción frente a la seguridad de la información.

Para evaluar de manera objetiva la cultura organizacional y la percepción de seguridad en el contexto de proveedores críticos de TI, se diseñó un instrumento de medición basado en una escala de cinco niveles. Este formato de encuesta permite identificar el grado de comprensión, motivación, capacitación, reporte de incidentes, confianza en los proveedores externos y compromiso de la alta dirección frente a la seguridad de la información. Los ítems seleccionados reflejan dimensiones clave del modelo propuesto (AET + BC), asegurando que la evaluación capture tanto aspectos de concienciación y formación como de comportamiento de cumplimiento. A continuación, se presenta la tabla con los ítems y el rango de respuesta correspondiente.

Tabla Anexos 1.

Encuesta de percepción frente a la seguridad de la información.

Ítem	Pregunta	Rango: 1 (Totalmente en desacuerdo) a 5 (Totalmente de acuerdo)
1	Entiendo claramente las políticas de seguridad de la información de mi organización.	1 a 5
2	Me siento motivado(a) a seguir las prácticas de seguridad establecidas en mi rol.	1 a 5
3	Recibo suficiente capacitación y apoyo para manejar riesgos de seguridad.	1 a 5
4	Reporto oportunamente cualquier situación sospechosa o incidente de seguridad.	1 a 5
5	Creo que los proveedores externos cumplen con las normas de seguridad establecidas.	1 a 5
6	La alta dirección promueve una cultura proactiva de seguridad en la organización.	1 a 5

Fuente: *elaboración basada en la integración del modelo (AET+BC),* una propuesta para implementación futura.

Los resultados de esta encuesta permitirán identificar patrones de percepción y comportamiento en torno a la seguridad de la información, tanto dentro de la organización

como en su relación con proveedores críticos de TI. La interpretación de las respuestas facilitará la identificación de brechas culturales, el nivel de compromiso de los actores involucrados y la efectividad de las políticas y programas de concienciación implementados. Asimismo, los datos servirán como insumo para alimentar el sistema de métricas e indicadores del modelo (AET+BC), fortaleciendo la capacidad de la organización para evaluar su madurez en seguridad, priorizar riesgos y diseñar estrategias de mejora continua.

Anexos. 2.

Plantilla básica de auditoría de cumplimiento conductual (BC).

Con el fin de evaluar la adopción efectiva de prácticas de seguridad en proveedores críticos de TI, se diseñó una plantilla básica de auditoría orientada al cumplimiento conductual (BC). Este instrumento permite verificar de manera sistemática el grado de alineación entre las políticas organizacionales y los comportamientos observados en los proveedores, identificando desviaciones, fortalezas y oportunidades de mejora. La plantilla constituye un mecanismo práctico de control y seguimiento dentro del modelo (AET+BC), asegurando que las acciones de los proveedores reflejen un compromiso real con la cultura de seguridad establecida.

Tabla Anexo 2

Plantilla básica de auditoría de cumplimiento conductual (BC).

Área Evaluada	**Criterios de Evaluación**	**Cumple (Sí/No)**	**Observaciones / Hallazgos**	**Acción Correctiva Requerida**
Acceso a sistemas	Uso de credenciales personales y no compartidas			
Aplicación de controles físicos	Uso correcto de credenciales, tarjeta acceso, zonas restringidas			
Manejo de información sensible	Protección de datos en dispositivos y documentos			
Reporte de incidentes	Registro y notificación oportuna de eventos y anomalías			
Participación en capacitaciones	Registro de asistencia a formación obligatoria			
Comportamientos de riesgo detectados	Uso inapropiado de recursos o violaciones a políticas			

Nota: elaboración basada en la integración del modelo (AET+BC). Esta plantilla puede aplicarse periódicamente a empleados y proveedores críticos para valorar la adherencia y los comportamientos de riesgo.

Anexos. 3.

Matriz de evaluación de indicadores y acciones de mejora.

La matriz de evaluación de indicadores constituye una herramienta clave para monitorear la efectividad del modelo (AET+BC) en la gestión de proveedores críticos de TI. A través de métricas específicas, se identifican resultados actuales, metas establecidas y desviaciones, lo que permite definir acciones correctivas y responsables de su ejecución. Este enfoque asegura un seguimiento sistemático y orientado a la mejora continua, integrando dimensiones de capacitación, cumplimiento conductual, reducción de incidentes y percepción cultural de la seguridad. A continuación, se presenta la matriz con los indicadores seleccionados y las acciones de mejora correspondientes.

Tabla Anexo 3.

Matriz de evaluación de indicadores PRE y POST con acciones de mejora.

Indicador	Resultado Actual	Meta Establecida	Desviación	Acción Correctiva / Mejora	Responsable	Fecha Seguimiento
% de cobertura de capacitación (AET)	75%	90%	-15%	Intensificar campañas de convocatoria	GSI/Control y riesgo	30/02/2026
Tasa de aprobación en evaluaciones	85%	95%	-10%	Revisar contenidos, refuerzo extra	Formación/GSI	30/02/2027
% de cumplimiento conductual (BC)	80%	95%	-15%	Auditorías focalizadas y coaching	Auditoría Interna	30/02/2028
Número de incidentes por error humano	12	<5	7	Simulacros adicionales y alertas	Ciberseguridad	30/02/2029
Nivel de percepción positiva cultura	3.8 (escala 1-5)	≥4.5	-0.7	Realizar talleres de sensibilización	RRHH / GSI	30/02/2030

Fuente: *elaboración basada en las métricas de la integración del modelo (AET+BC),* una propuesta para implementación futura.

La interpretación de esta matriz permite a la organización vincular los resultados obtenidos con un sistema estructurado de seguimiento y control. Cada indicador se conecta directamente con las dimensiones del modelo (AET+BC), facilitando la identificación de

desviaciones y la definición de acciones correctivas específicas. Al integrarse en el tablero de gestión de seguridad, estos indicadores ofrecen una visión consolidada del desempeño cultural y conductual de los proveedores críticos, fortaleciendo la toma de decisiones estratégicas y la mejora continua. De esta manera, la matriz se convierte en un mecanismo práctico para garantizar la sostenibilidad del modelo y su alineación con los objetivos de resiliencia organizacional.

Anexos. 4.

Prototipo del tablero de gestión de riesgos MBP-SI-PC y hoja de ruta propuesta.

El **Anexo 4** presenta el diseño del Tablero de Control Operativo propuesto para el modelo MBSI. Este artefacto actúa como el centro de mando para la gobernanza de proveedores críticos. Su arquitectura permite la ingesta de datos desde la plataforma de aprendizaje (AET) y el sistema de monitoreo de red (BC). La innovación radica en que el **Estado de Cumplimiento** no es estático; se recalcula cada vez que un nuevo bloque de información es sellado en el **Blockchain**, proporcionando una visibilidad de riesgos sin precedentes y eliminando la posibilidad de manipulación de reportes por parte del proveedor.

El tablero se divide en cuatro cuadrantes estratégicos que permiten al CISO o al interventor de TI tomar decisiones en tiempo real:

1. Cuadrante de Cumplimiento General (Vistas de Velocímetro).

Este cuadrante muestra el promedio de todos los proveedores críticos.

- KPI 1: Índice Global ICSP. (Meta: >85%).
- KPI 2: Nivel de Adopción de Blockchain. (% de logs sellados exitosamente).
- KPI 3: Brecha de Conocimiento-Acción. (Diferencia porcentual entre lo que saben en AET y lo que hacen en BC).

2. Matriz de Seguimiento por Proveedor

Tabla Anexo 4

Matriz de Seguimiento, tablero y hoja de ruta por Proveedor.

Proveedor	Capacidad (AETx0.40)	Conducta (BCx0.60)	Score ICSP	Estado / Nivel
Proveedor_1	95%	92%	**93.2**	**Nivel 5 (Optimizado)**
Proveedor_2	88%	70%	**77.2**	**Nivel 4 (Gestionado)**
Proveedor_3	60%	40%	**48.0**	**Nivel 2 (Riesgo)**

Fuente: *elaboración basada en las métricas de la integración del modelo (AET+BC).*

Nota: El color cambia automáticamente según el puntaje obtenido por la fórmula: ICSP = (AET x 0.4) + (BC x 0.6).

3. Mapa de Calor de Riesgos Conductuales (BC).
Un mapa que categoriza las desviaciones detectadas por el sistema y registradas en la cadena de bloques:

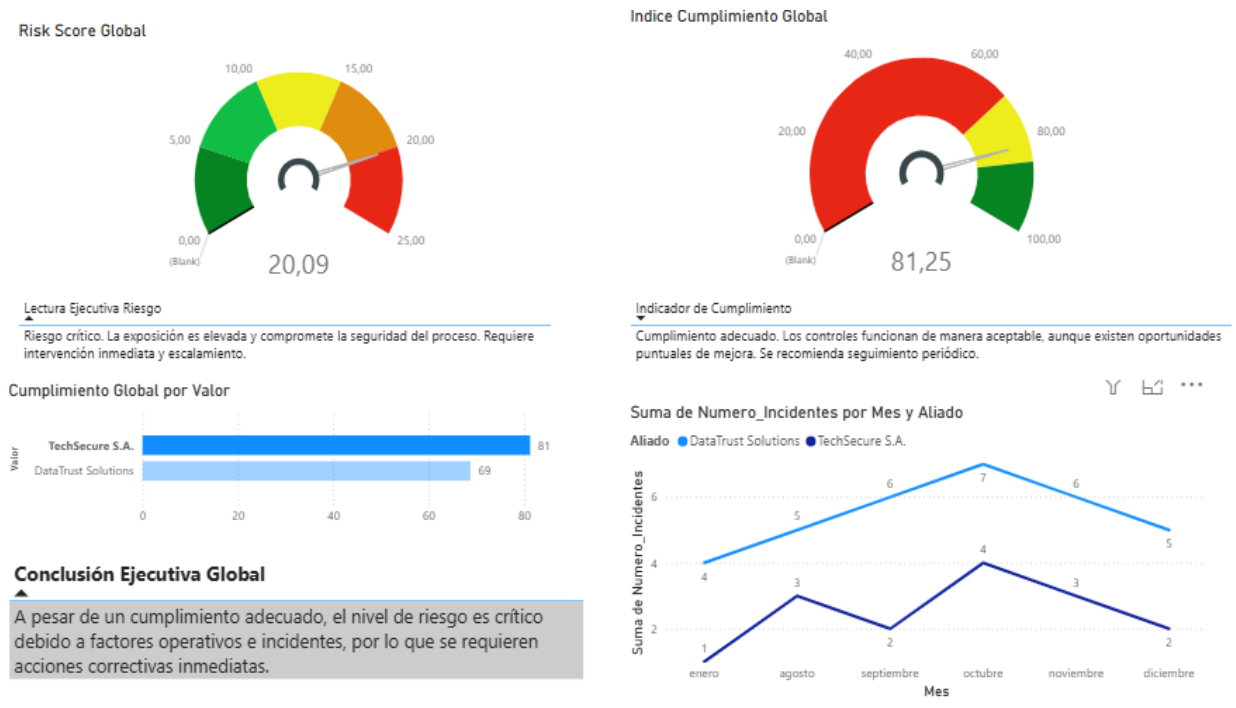
- Eje X: Frecuencia de la desviación.
- Eje Y: Impacto de la desviación (Acceso a BD, Cambio de Firewalls, Escalada de Privilegios).

Visualización: Los puntos más rojos indican dónde se requiere intervención inmediata de AET (recapacitación).

4. Monitor de Inmutabilidad (Plataforma de monitoreo).
Un pequeño terminal en la parte inferior que muestra los últimos "Hashes" generados:

- ID_Evento: 0045 | Proveedor: NetSecurity | Acción: Intento de Acceso Fallido | Hash: 8f39...e2f ✅ (Validado).

Figura Mock-up del tablero principal



Nota: La Figura muestra el mock-up del tablero principal, concebido como una herramienta integrada para la visualización y seguimiento de indicadores clave de seguridad y gestión de riesgos, una propuesta para implementación futura.

Tabla Anexos 5

Hoja de Ruta para la Evolución del Modelo

Define la trayectoria evolutiva esperada para cada proveedor, estableciendo metas de mejora continua alineadas con los estándares *ISO/IEC 27001 y NIST CSF 2.0*. Esta hoja de ruta asegura que la relación con el proveedor no sea estática, sino que progrese hacia niveles de madurez "Avanzado" o "Predictivo".

Evolución a Corto Plazo (Año 1)

Trimestre 1-2:

Establecimiento de fundamentos

Victorias tempranas con proveedores Top 5

Construcción de capacidades básicas

Trimestre 3-4:

Expansión a proveedores Tier 2

Optimización de procesos

Primeras certificaciones

Evolución a Mediano Plazo (Años 2-3)

Año 2:

Automatización avanzada

Integración con ecosistema digital

Programa de certificación de proveedores

Benchmarking sectorial

Año 3:

Inteligencia artificial para predicción

Modelo as-a-Service para PYMES

Centro de excelencia sectorial

Estándares de industria.

Visión a Largo Plazo (Años 4-5)

Innovaciones futuras:

- Blockchain para auditoría inmutable
- Machine Learning para detección de anomalías
- Automatización completa de onboarding
- Ecosistema colaborativo de seguridad
- Zero Trust Architecture completa

Metas aspiracionales:

- Cero incidentes originados en proveedores
- 100% automatización de controles rutinarios
- Certificación automática continua
- Modelo predictivo de riesgos
- Estándar de facto en la industria