Revista científica Portal de la Ciencia
ISSN: 2953-6502
Fecha de presentación: 12/05/2026
Fecha de aceptación: 14/06/2026
Fecha de publicación: 01/07/2026

Henry Nelson Revelo-Quiñónez
E-mail: henry.reveloquinonez3751@upse.edu.ec - henry.revelo.86@gmail.com
Orcid: https://orcid.org/0009-0000-1467-1137

Maestría en ciberseguridad, Cohorte II. Instituto de postgrado de la Universidad Estatal Península de Santa Elena

Cita sugerida (APA, séptima edición)

Revelo-Quiñónez, H. N. (2026). Controles avanzados de ciberseguridad en SoftwareONE Ecuador: fortalecimiento de la protección corporativa. *Portal de la Ciencia*, 7(3), 472-495, DOI: https://doi.org/10.51247/pdlc.v7i3.777

==== o ====

Controles avanzados de ciberseguridad en SoftwareONE Ecuador: fortalecimiento de la protección corporativa.

RESUMEN

El acelerado proceso de transformación digital ha incrementado de manera exponencial la exposición de las organizaciones a amenazas cibernéticas de alta sofisticación. El presente artículo analiza el estado actual de la ciberseguridad en forma general y de manera particular en empresas de servicios tecnológicos, en Ecuador e identifica las principales brechas de seguridad existentes en el contexto del sector de servicios tecnológicos y de manera particular en un caso de estudio en el Ecuador; donde, la madurez promedio en ciberseguridad de las empresas es inferior al 60 %. A partir del análisis realizado se propone mediante un enfoque descriptivo-analítico y el uso de fuentes secundarias especializadas, se propone la implementación de controles avanzados de ciberseguridad alineados con los estándares ISO/IEC 27001:2022 y el NIST Cybersecurity Framework 2.0, con énfasis en la reducción de vulnerabilidades asociadas al phishing, al ransomware y al acceso no autorizado a credenciales. El conjunto de resultados esperados comprende, entre otros, la reducción escandalosa de las vulnerabilidades que amenazan la infraestructura tecnológica local, el refuerzo de los principios de confidencialidad, de integridad y de disponibilidad de la información, así como el cumplimiento proactivo de la LOPDP. Esta contribución metodológica tiene un alcance aplicable a filiales de multinacionales presentes en países donde se están usando tecnologías emergentes, tal como es el caso ecuatoriano.

Palabras clave: controles avanzados, ciberseguridad corporativa, protección de datos, transformación digital, phishing, ransomware.

==== o ====

Advanced cybersecurity controls at softwareONE Ecuador: strengthening corporate protection

ABSTRACT

The accelerated digital transformation process has exponentially increased organizations' exposure to highly sophisticated cyber threats. This article analyzes the current state of

corporate cybersecurity at SoftwareONE Ecuador and identifies the main security gaps in the technology services sector in the country, where the average cybersecurity maturity of companies falls below 60%. Using a descriptive-analytical approach and specialized secondary sources, it proposes the implementation of advanced cybersecurity controls aligned with ISO/IEC 27001:2022 and NIST Cybersecurity Framework 2.0 standards, with emphasis on reducing vulnerabilities associated with phishing, ransomware and unauthorized credential access. Expected results include a significant reduction in vulnerabilities in the local technological infrastructure, strengthening of confidentiality, integrity and availability principles, and proactive compliance with Ecuador's Personal Data Protection Law. This work constitutes a methodological contribution applicable to subsidiaries of multinational companies with emerging operations in Ecuador.

Keywords: advanced controls, corporate cybersecurity, data protection, phishing, ransomware.

==== o ====

Controlos avançados de cibersegurança na softwareONE Equador: reforçar a proteção corporativa

RESUMO

O processo acelerado de transformação digital aumentou exponencialmente a exposição das organizações a ciberameaças altamente sofisticadas. Este artigo analisa o estado atual da cibersegurança em geral e, especificamente, nas empresas de serviços tecnológicos no Equador. Identifica as principais lacunas de segurança no setor dos serviços tecnológicos e, em particular, num estudo de caso no Equador, onde a maturidade média em cibersegurança das empresas é inferior a 60%. Com base na análise, e recorrendo a uma abordagem descritivo-analítica e a fontes secundárias especializadas, o artigo propõe a implementação de controlos avançados de cibersegurança alinhados com a norma ISO/IEC 27001:2022 e o NIST Cybersecurity Framework 2.0, com ênfase na redução de vulnerabilidades associadas a phishing, ransomware e acesso não autorizado a credenciais. Os resultados esperados incluem, entre outros, uma redução significativa das vulnerabilidades que ameaçam a infraestrutura tecnológica local, o reforço dos princípios de confidencialidade, integridade e disponibilidade, e a conformidade proativa com a Lei de Proteção de Dados Pessoais (LOPDP). Esta contribuição metodológica é aplicável a subsidiárias de empresas multinacionais que operam em países onde estão a ser utilizadas tecnologias emergentes, como o Equador.

Palavras-chave: controlos avançados, cibersegurança empresarial, proteção de dados, transformação digital, phishing, ransomware.

==== o ====

INTRODUCCIÓN

La transformación digital de alcance mundial ha impactado de forma drástica en la forma en la que las organizaciones gestionan su información, operan sus infraestructuras tecnológicas y están conectadas con sus clientes y socios estratégicos. En la actualidad, las amenazas cibernéticas son uno de los riesgos más significativos que enfrentan las organizaciones con respecto a la continuidad operativa en sus actividades, sin importar la dimensión, la actividad por la que se rige o la localización de la misma. La necesidad de implementar controles avanzados de ciberseguridad de acuerdo con marcos internacionales reconocidos se ha convertido en una necesidad estratégica ineludible para cualquier organización que desee operar de forma segura en un entorno digital con una complejidad alta (Sarkar et al., 2023; Luidold y Jungbauer, 2024).

Contexto Global: Estado Actual de las Ciberamenazas en Empresas de Servicios Tecnológicos

Globalmente, las ciberamenazas han avanzado a una velocidad sin precedentes en los últimos años. Como indican Sarkar et al. (2023), el cruce entre la acelerada digitalización y el creciente nivel de sofisticación de los ciberataques ha permitido que las organizaciones desarrollen capacidades de resiliencia cibernética que les permita predecir, resistir, recuperarse y adaptarse a los incidentes de seguridad. Este mismo estudio añaden que los daños económicos a nivel mundial que se han provocado por ciberataques ascenderán hasta 10.5 billones de dólares anualmente para el 2025, afirmación que pone el foco en la magnitud del problema a nivel global.

En lo que respecta a los marcos de referencia para la gestión de la seguridad de la información, la norma ISO/IEC 27001:2022 y el NIST Cybersecurity Framework (CSF) 2.0 publicado en febrero de 2024 se mantienen como los estándares más adoptados a nivel mundial. Luidold y Jungbauer (2024) destacan que el NIST CSF 2.0 amplió su alcance más allá de las infraestructuras críticas para aplicarse a organizaciones de cualquier sector y tamaño, incorporando además una nueva función de gobierno (*Govern*) que enfatiza la importancia de la estrategia, la rendición de cuentas y la gestión de riesgos como responsabilidades transversales de liderazgo organizacional, y no exclusivamente del área de tecnología de la información. En paralelo, la revisión sistemática de Toussaint et al. (2024), recogida por el trabajo de Datta et al. (2025) publicado en el *International Journal of Information Security*, confirma que organizaciones de todo el mundo incrementan su inversión en estándares y marcos de ciberseguridad como respuesta directa al aumento sostenido de los ciberataques.

Las organizaciones de servicios tecnológicos constituyen objetivos de alta relevancia para los ciberdelincuentes, por tal motivo, el vector de ataque a través de terceros proveedores, supply chain attack, se ha posicionado como uno de los vectores de ataque más temidos de la actualidad en el ecosistema digital (Datta et al., 2025). El *ransomware* ha llegado a ser la tipología de ataques más disruptiva a nivel global: las últimas investigaciones han mostrado que fue el vector de ataque utilizado en el 49% de ataques cibernéticos exitosos en organizaciones en América Latina y el Caribe durante el año 2023-2024 (Bezborodko, 2024). La revisión sistemática de Almeida et al. (2024) refuerza esta tendencia indicando que los ataques de ransomware alcanzaron niveles históricos en 2023, lo que motivó un mayor desarrollo de metodologías de detección proactiva basadas en comportamiento y *machine learning.*

A nivel de las economías emergentes, los distintos organismos internacionales explicitan la existencia de una brecha en las capacidades de ciberseguridad que poco a poco puede ir adquiriendo los niveles que pueden llevar a considerarse como uno de los mayores combustibles riesgosos que pueden promover el crecimiento digital. El Global Cybersecurity Outlook de Foro Económico Mundial (World Bank, 2023), indica que el 93 % de los líderes de ciberseguridad y el 86 % de los líderes empresariales opinan que un evento cibernético catastrófico es muy probable en los siguientes dos años

La Unión Internacional de Telecomunicaciones (2022), por medio de su Índice Global de Ciberseguridad, recuerda que gran parte de los países de América Latina y el Caribe ocupan un nivel medio de madurez con importantes rezagos en las dimensiones técnica, organizativa y de capacitación. Además, la Agencia para la Cooperación y el Desarrollo Económico (2022) destaca que la inexistencia de marcos normativos coherentes y de inversión sostenida en ciberseguridad corresponde a uno de los umbrales de riesgo sistémico en el que se sostiene la estabilidad de la ecología de lo digital en estos países.

Desde la perspectiva de la investigación académica, se han creado, se han ido generando estrategias vinculadas a aproximaciones multi-organizacionales y a las ópticas estratégicas en el área de ciberseguridad corporativa. Marican et al. (2023) presentan un marco de

evaluación de madurez dirigido a empresas tecnológicas en contextos de crecimiento y regresión que incluye dimensiones estratégicas, operativas y normativas de cumplimiento, y su puesta en práctica en una filial de empresas multinacionales en el contexto de los mercados emergentes ha dado resultados coherentes en cuanto a la reducción del riesgo residual.

En cuanto a la aplicación en empresas del sector tecnológico, Adebola et al. (2024) evidencian que las organizaciones que implementan programas formales de cumplimiento de seguridad alineados con marcos internacionales reconocidos presentan tasas de incidentes significativamente menores y una recuperación más ágil ante brechas de datos. En relación a los controles avanzados importa subrayar la aparición de sistemas de análisis del comportamiento, también conocidos como UEBA o "User and Entity Behavior Analytics", inteligencia artificial para detectar anomalías e integración con herramientas de Threat Intelligence, que son muy importantes en entornos de nube, IoT o sistemas distribuidos, donde la complejidad de los vectores de ataque puede llegar mucho más allá de las capacidades de los estándares (Sarkar et al. 2023; Datta et al. 2025).

1.2 Problema Específico: Brechas de Seguridad en el Entorno Corporativo Local

Ecuador no es ajeno a la tendencia global de incremento en los ciberataques. Según datos del quinto informe de ciberseguridad elaborado conjuntamente por la revista IT ahora (2024), más del 60 % de las organizaciones ecuatorianas evaluadas presentan un nivel de madurez en ciberseguridad inferior al umbral crítico del 60 %, lo que las coloca en una posición de vulnerabilidad estructural frente a amenazas de media y alta complejidad. El mismo estudio identifica la falta de capacidades técnicas y de gestión como la limitación más crítica para avanzar en los programas de seguridad corporativa.

En términos de incidentes concretos, Ecuador registró más de 12 millones de ciberataques durante el año 2023, a pesar de lo cual el Global Cybersecurity Index 2024 posiciona al país en un nivel intermedio de madurez con una inversión en seguridad digital que, si bien creció hasta los 184 millones de dólares en 2024 (un 12 % más que el año anterior), sigue siendo baja en términos de inversión per cápita en comparación con Brasil y México (GMS Lexis, 2024). Urgilés y Ron Egas (2023), en su análisis de riesgos y amenazas de ciberseguridad del Estado ecuatoriano publicado en *Pro Sciences: Revista de Producción, Ciencias e Investigación*, determinan que el phishing, el ransomware y los errores humanos derivados de ingeniería social constituyen los vectores de amenaza más prevalentes en el ecosistema digital ecuatoriano, tanto en el sector público como en el privado.

Las empresas del sector tecnológico presentan características particulares de vulnerabilidad en este contexto. Por un lado, manejan grandes volúmenes de información de clientes y de información sensible de la empresa, por otro lado, suelen operar a menudo actuando bien como integradores de soluciones o bien como proveedores de servicios gestionados, lo que las capacita para convertirse potencialmente en un medio de ataque a sus propios clientes. Este perfil de riesgo se acentúa también en las subsidiarias locales de empresas multinacionales que comienzan su andadura en el país, ya que la gestión de la seguridad corporativa se lleva a cabo bajo un esquema de centralización a sedes regionales o globales que no contemplan sobradamente las particularidades de índole regulatoria, cultural y de negocio que exhibe el mercado ecuatoriano.

En este marco, el problema científico central del presente artículo puede formularse de la siguiente manera: ¿Cómo implementar controles avanzados de ciberseguridad en SoftwareONE Ecuador que fortalezcan la protección corporativa frente a las amenazas digitales más prevalentes en el entorno local, alineándose simultáneamente con los estándares internacionales ISO/IEC 27001:2022 y NIST CSF 2.0?

Justificación de la Investigación

Justificación teórica. Al plantear en Ecuador un modelo de análisis e implementación de controles avanzados en ciberseguridad organizacional que va más allá del control perimetral, la investigación que se informa aquí hace aportaciones al acervo teórico de la ciberseguridad a nivel de las organizaciones. Si bien existen numerosos estudios a nivel internacional que abordan los diferentes frameworks de ciberseguridad, la literatura académica que los vincule con las empresas de los mercados de Latinoamérica en crecimiento es aún muy escasa, lo que confiere un importante valor científico y de novedad añadida a esta investigación (Luidold y Jungbauer, 2024; Datta et al., 2025; Adebola et al., 2024).

Justificación práctica. La implementación de controles avanzados de ciberseguridad genera beneficios como la reducción de la superficie de ataque, mejora en los tiempos de detección y respuesta ante incidentes, y disminución del riesgo de interrupciones operativas que podrían comprometer los servicios prestados a los clientes. En el contexto de gestionar los riesgos cibernéticos, el control proactivo de la seguridad que se realiza por medio de una supervisión preventiva alineada a estándares internacionales, resulta económicamente más eficiente que la respuesta reactiva después de que ocurra un incidente y se ponga en peligro a la entidad (Adebola et al., 2024; Sarkar et al., 2023).

Justificación metodológica. La propuesta que se realiza en el estudio también consiste en una forma de poder realizar diagnóstico y diseño de controles, por tanto, podría replicarse en el resto de organizaciones tecnológicas que pudieran operar en un contexto semejante al ecuatoriano. El enfoque de las propuestas está orientado a la utilización de técnicas, que combinan el análisis de la documentación y las matrices de riesgos y controles, y la triangulación con estándares de referencia como la norma ISO/IEC 27001:2022 o NIST CSF 2.0, que cristalizó en dar lugar a un proceso sistemático, riguroso y de fácil adecuación, de tal forma que lo pudiesen utilizar otras entidades del sector.

Justificación social. Existe una brecha de seguridad en una empresa proveedora de servicios tecnológicos que puede generar un impacto que trasciende la propia organización directamente a todo cliente o usuario final cuyos datos están gestionados por la empresa. En el caso de Ecuador, la entrada en vigor de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo de 2023, ha elevado la responsabilidad social de las organizaciones en términos de la protección de la información personal (González, 2023).

Justificación económica. Los gastos asociados a un evento o incidente de ciberseguridad son elevados y en múltiples dimensiones: pérdida de dinero directa, gastos de recuperación y remediación, daños a la reputación y la prestación del servicio, pérdida de clientes y sanciones regulatorias. En el caso de Ecuador, se estima que el coste de un ataque cibernético exitoso a una empresa tiene un coste de entre 250 000 a más de un millón de dólares (Saphirtek, 2024).

Preguntas de Investigación

Pregunta central:

La pregunta central de la investigación reúne las variables que organizan el presente estudio: la variable independiente, que es la de controles avanzados de ciberseguridad en función de estándares como ISO/IEC 27001:2022 y NIST CSF 2.0 ; la variable dependiente, que es el nivel de protección corporativa de SoftwareONE Ecuador frente a las amenazas digitales que aparecen con más frecuencia en el contexto local, medida en términos de madurez en ciberseguridad, reducción de vulnerabilidades críticas y cumplimiento normativo. En este ámbito, la pregunta central se articula de la siguiente forma:

¿Qué controles avanzados de ciberseguridad, alineados con los estándares ISO/IEC 27001:2022 y NIST CSF 2.0 *(variable independiente)*, deben implementarse en SoftwareONE Ecuador para fortalecer el nivel de protección corporativa frente a las amenazas digitales más prevalentes en el entorno local *(variable dependiente)*?

Preguntas específicas:

- ¿Cuál es la evaluación actual de la ciberseguridad en SoftwareONE Ecuador?
- ¿Cuáles son las vulnerabilidades más importantes encontradas en la infraestructura y procesos operativos?
- ¿Cuáles controles avanzados, explicados en los marcos ISO/IEC 27001:2022 y NIST CSF 2.0 serían los que pueden ser aplicables para la mitigación de los riesgos cibernéticos que han sido identificados en el entorno organizacional de SoftwareONE Ecuador?
- ¿Cuál tendría que ser la forma de la estructura que proponemos que fuera la metodología para la implementación de dichos controles, dado que hay que tener en cuenta las particularidades operativas de una filial que tiene operaciones de reciente aparición en el mercado ecuatoriano?
- ¿Cuál sería el impacto esperado de la propuesta de control aplicada en la reducción del riesgo cibernético y en el cumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador?

El artículo que aquí se presenta analiza la forma de implementar controles avanzados en SoftwareONE Ecuador en función de mitigar brechas operativas y adecuarse a estándares internacionales de seguridad a la amenaza local detectada. El artículo se estructuró de la siguiente manera: la sección 2 describe la metodología para realizar el diagnóstico y el diseño; la sección 3 describe la obtención de los resultados, el diagnóstico de las vulnerabilidades y el resultado de la validación mediante gap analysis; la sección 4 discute la obligación con los hallazgos y la literatura científica especializada, y, finalmente, la sección 5 presenta las conclusiones y recomendaciones.

Materiales y Métodos

La sección de materiales y métodos describe el conjunto de procedimientos, fuentes de información, herramientas y criterios de evaluación empleados para el análisis de la situación de ciberseguridad en SoftwareONE Ecuador y para el diseño de la propuesta de controles avanzados. El enfoque metodológico es *descriptivo-analítico*, con diseño no experimental, en coherencia con lo establecido en el anteproyecto aprobado. La investigación integra análisis documental, matrices de riesgo y controles, y validación teórica mediante *gap analysis* alineado con los marcos ISO/IEC 27001:2022 y NIST CSF 2.0 (NIST, 2024; Marican et al., 2023).

Fuente de Datos: Diagnóstico del Entorno de Ciberseguridad en SoftwareONE Ecuador

La obtención de información se realizó mediante dos fuentes complementarias, tal como lo establece el diseño metodológico de la propuesta:

Fuentes propias: Realizamos un análisis de las políticas internas, de los procedimientos operativos y de las configuraciones de seguridad de la operación local de SoftwareONE Ecuador, centrado en los controles de acceso, la gestión de los dispositivos terminales y los procedimientos de respuesta a incidentes. También hicimos entrevistas semiestructuradas con el personal del área de Tecnología de la Información, aplicando un protocolo de exploración orientado a descubrir las brechas que existen entre aquellas políticas globales de la organización y que son administradas desde la sede regional en India y las capacidades de la operación local en Ecuador.

Fuentes secundarias: Se complementó el diagnóstico con información proveniente de informes sectoriales, reportes de organismos especializados en ciberseguridad regional y estudios académicos recientes que documentan el perfil de riesgo de empresas de servicios tecnológicos en Ecuador y América Latina (Urgilés y Ron Egas, 2023; IT ahora, 2024; Positive Technologies, 2024).

A partir de la integración de ambas fuentes, se identificaron ocho (8) categorías de vulnerabilidad críticas para la operación de SoftwareONE Ecuador, que se presentan en la Tabla 1. La clasificación de criticidad se realizó aplicando una escala de tres niveles (Alto, Medio, Bajo), determinada por la combinación de la probabilidad de ocurrencia —estimada con base en la frecuencia reportada en el sector para el contexto ecuatoriano— y el impacto potencial sobre los activos de información (NIST, 2024; Adebola et al., 2024).

Tabla 1

Diagnóstico de vulnerabilidades en SoftwareONE Ecuador

ID	Categoría de Vulnerabilidad	Vector de Ataque Principal	Frecuencia Detectada (eventos/mes)	Criticidad	Control Global (SoftwareONE Global)	Brecha en Operación Ecuador
V-01	Phishing y spearphishing dirigido al personal	Correo electrónico malicioso con suplantación de identidad	14	ALTO	Filtros antispam corporativos gestionados globalmente	Sin capacitación local activa; filtros no configurados para dominios .ec
V-02	Ransomware en estaciones de trabajo y servidores	Descarga de archivos maliciosos, macros y RDP expuesto	6	ALTO	EDR corporativo (CrowdStrike) gestionado desde India	Configuración EDR pendiente de despliegue en endpoints locales
V-03	Robo de credenciales por acceso no autorizado	Credential stuffing, fuerza bruta y keyloggers	9	ALTO	Política de contraseñas robustas definida a nivel global	Ausencia de herramienta PAM local; contraseñas compartidas en algunos sistemas
V-04	Ausencia o uso inconsistente de MFA	Acceso remoto VPN y aplicaciones SaaS sin segundo factor	N/A	ALTO	MFA obligatorio en sistemas críticos a nivel global	MFA no habilitado en todos los usuarios locales; excepciones no documentadas
V-05	Software obsoleto y gestión deficiente de parches	Explotación de CVEs conocidos en sistemas sin parchar	11	MEDIO	Proceso de patch management centralizado en sede global	Ciclo de actualización irregular en equipos locales; retrasos de 45-60 días
V-06	Monitoreo de red insuficiente y ausencia de SIEM local	Movimiento lateral y exfiltración de datos no detectados oportunamente	N/A	MEDIO	SIEM corporativo centralizado; alertas gestionadas desde India	Latencia de 6-12 horas en notificación de alertas; sin visibilidad local en tiempo real
V-07	Inexistencia de Plan de Respuesta a Incidentes local	Cualquier incidente cibernético sin protocolo de acción local definido	3	ALTO	IRP global disponible; procedimientos de escalamiento a CSIRT regional	Sin IRP localizado para Ecuador; personal desconoce protocolos de escalamiento
V-08	Incumplimiento de la LOPDP de forma parcial y gestión de una forma errónea de la información personal	Procesamiento ilegal de información de clientes y trabajadores	N/A	MEDIO	Politicas de privacidad globales (GDPR-compliant)	Municipalización de datos personales no realizado; DPO local designado

De las ocho vulnerabilidades identificadas, el 62,5 % (cinco de ocho) presentan criticidad Alta, siendo las más recurrentes el phishing (14 eventos/mes), el software sin parchear (11 eventos/mes) y el robo de credenciales (9 eventos/mes). Este perfil es consistente con el diagnóstico nacional: el informe de IT ahora (2024) señala que el phishing y el ransomware encabezan las amenazas más preocupantes en Ecuador de manera constante desde 2022.

Arquitectura de la Solución: Controles Técnicos y Flujo de Implementación

Selección y Mapeo de Controles Avanzados

A partir del diagnóstico presentado en la sección 3.1 y conforme con la propuesta de la metodología de evaluación de madurez presentada propuesto por Marican et al. (2023), se han considerado como controles un total de diez controles avanzados de ciberseguridad. Precisamente, la selección de controles avanzados de ciberseguridad propuestos se fundamenta en tres criterios en concreto:

a) Idoneidad directa con respecto a las vulnerabilidades con la mayor criticidad identificadas.

b) Coincidencia con los dominios del Anexo A de la norma ISO/IEC 27001:2022 y con las funciones del NIST CSF 2.0.

c) Viabilidad de implementación en relación a una operación corporativa de inicio de actividad.

La Tabla 2 muestra la matriz de controles propuestos.

Tabla 2

Matriz de controles avanzados propuestos: mapeo ISO 27001 / NIST CSF 2.0

Control	ID Vuln.	Nombre del Control	Cláusula ISO/IEC 27001:2022	Función NIST CSF 2.0	Herramienta / Mecanismo	Descripción de la Acción
C-01	V-03, V-04	Autenticación multifactor (MFA) universal	A.8.5	PR.AA-01	Microsoft Entra ID / Azure AD MFA	Habilitar la autenticación de dos factores para todos los usuarios que acceden a la red privada virtual, Office 365, portales de clientes y sistemas de planificación de recursos empresariales. Eliminar todas las excepciones que no estén documentadas
C-02	V-01	Filtrado avanzado de correo y simulación de phishing	A.8.23	PR.PS-01	Microsoft Defender for Office 365 / KnowBe4	Configurar políticas para prevenir el phishing con análisis de enlaces web en tiempo real, protección contra la suplantación de identidad y campañas de concienciación cada tres meses mediante simulaciones controladas.
C-03	V-02	Despliegue y configuración local de EDR	A.8.7	PR.PS-04	CrowdStrike Falcon (existente global)	Ampliar la consola de detección y respuesta a todos los puntos de acceso locales, como estaciones de trabajo y portátiles. Activar políticas para prevenir el ransomware, bloquear macros maliciosas y controlar los dispositivos USB.

C-04	V-05	Gestión automatizada de parches y actualizaciones	A.8.8	PR.PS-02	Microsoft Intune / WSUS local	Implementar un ciclo de actualización de parches locales con un plazo máximo de 15 días para parches críticos y 30 días para parches de alta prioridad
C-05	V-03	Gestión de accesos privilegiados (PAM)	A.8.2	PR.AA-05	CyberArk PAM / BeyondTrust	Crear un almacén de credenciales administrativas locales, con rotación automática de contraseñas cada 90 días y registro de sesiones administrativas para auditoría
C-06	V-06	Monitoreo continuo y correlación de eventos (SIEM)	A.8.15, A.8.16	DE.CM-01	Microsoft Sentinel (extensión instancia regional)	Integrar los registros locales de firewall, directorio activo, puntos de acceso y red privada virtual en la instancia de seguridad y eventos de información regional, con tableros de monitoreo específicos para Ecuador y un umbral de alertas inferior a 15 minutos.
C-07	V-07	Plan de Respuesta a Incidentes (IRP) local	A.5.26	RS.MA-01	Playbooks SOAR / TheHive	Desarrollar y validar el plan de respuesta a incidentes locales con roles definidos, matriz de escalamiento al equipo de respuesta a incidentes regionales, procedimientos de contención y plantillas de notificación a la Autoridad de Protección de Datos según la Ley de Protección de Datos.
C-08	V-02, V-03	Copias de seguridad con esquema 3-2-1 y cifrado	A.8.13	RC.RP-02	Veeam Backup / Azure Backup	Implementar una política de copia de seguridad con tres copias, dos medios distintos y una copia fuera del sitio en la nube cifrada con AES-256. Realizar pruebas de restauración trimestrales documentadas
C-09	V-01, V-03	Programa de concienciación y formación en ciberseguridad	A.6.3	GV.RR-02	KnowBe4 / LMS corporativo	Se requiere una capacitación obligatoria cada año para todo el personal local.
C-10	V-08	Gestión de cumplimiento LOPDP y designación de DPO	A.5.34	GV.PO-01	OneTrust / Registro interno de tratamiento	Además, se realiza un mapeo y registro de todas las actividades que involucran el tratamiento de datos personales. También se designa formalmente a un delegado de Protección de Datos local, según lo establecido en el Artículo 49 de la Ley de Protección de Datos Personales.

En la tabla 2 las cláusulas referidas a ISO/IEC 27001:2022 Annexo A (International Organization for Standardization , 2022). Las funciones referidas a NIST Cybersecurity Framework 2.0 (NIST, 2024). EDR: Endpoint Detection & Response. PAM: Privileged Access

Management. SIEM: Security Information and Event Management. DPO: Data Protection Officer. CVSS: Common Vulnerability Scoring System.

Flujo de Implementación por Fases

La implementación de los controles propuestos se estructura en cuatro fases secuenciales, cuyo flujo de trabajo se describe en la Tabla 3. El diseño por fases garantiza que cada etapa construya sobre los resultados de la anterior, minimizando el impacto operativo y permitiendo validaciones intermedias (Marican et al., 2023; NIST, 2024).

Tabla 3

Flujo de implementación por fases

Fase	Nombre	Duración Estimada	Actividades Principales	Entregable
F-01	Recolección y Diagnóstico	Semanas 1–3	Se revisan las políticas internas de la empresa, se realizan entrevistas con el personal de tecnología de la información, se hace un inventario de los activos y se identifican las vulnerabilidades.	Se presenta un informe que detalla el diagnóstico de vulnerabilidades y riesgos, utilizando la información completa de la Tabla 1.
F-02	Análisis de Brecha (Gap Analysis)	Semanas 4–5	Evaluación del actual nivel de madurez de la organización en aspectos de seguridad, siguiendo el marco NIST CSF 2.0. Compar Unión con el estado objetivo que prevalecía con el que la organización quiere llegar, priorización de controles de seguridad a aplicar.	Los resultados se muestran con una matriz de análisis de brechas en la Tabla 4, así como en el Perfil Organizacional NIST CSF.
F-03	Diseño e Implementación de Controles	Semanas 6–14	Despliegue de los controles de seguridad C-01 a C-10 en función del orden en que los prioriza la gestión. También se realiza la configuración de herramientas, se capacita al personal, y se documentan los procedimientos de despliegue.	Registro de la configuración de cada control, actualización de políticas y procedimientos, y recogida de pruebas de la configuración.
F-04	Validación y Evaluación de Impacto	Semanas 15–18	Auditoría, alineada con la norma ISO 27001, re-evaluación del nivel de madurez de la organización en seguridad, de acuerdo al NIST CSF, cálculo de métricas de impacto, revisión del riesgo residual.	Conclusiones en el informe de evaluación de impacto, conclusiones en una declaración de aplicabilidad preliminar y conclusiones en un tablerometro en la Tabla 6.

Protocolo de Validación: Gap Analysis ISO/IEC 27001:2022 y NIST CSF 2.0

La efectividad de los controles propuestos se evalúa mediante un protocolo de validación en dos niveles: un *gap analysis* basado en las funciones del NIST CSF 2.0 y una auditoría de cumplimiento parcial frente a los dominios del Anexo A de ISO/IEC 27001:2022. Este protocolo doble permite valorar simultáneamente la madurez operativa de la gestión de riesgos y el grado de alineación normativa de los controles implementados (Adebola et al., 2024; ISO, 2022).

Evaluación de Madurez NIST CSF 2.0 (Gap Analysis por Función)

La evaluación de madurez se realizó mediante el mapeo de las prácticas de seguridad observadas en SoftwareONE Ecuador frente a los cuatro niveles de implementación *(Implementation Tiers)* del NIST CSF 2.0: Tier 1 (Parcial), Tier 2 (Riesgo Informado), Tier 3 (Repetible) y Tier 4 (Adaptativo). El Tier objetivo establecido para la operación es el Tier 3 (Repetible), considerado el nivel mínimo adecuado para una empresa de servicios tecnológicos

que gestiona información de clientes corporativos, en concordancia con las recomendaciones de Marican et al. (2023) para filiales de empresas multinacionales en mercados emergentes.

Tabla 4

Gap analysis por función NIST CSF 2.0: estado actual vs. estado objetivo

Función NIST CSF 2.0	Descripción	Tier Actual (0–4)	Tier Objetivo (0–4)	Brecha (Tier)	Hallazgos Clave
GOVERN (GV)	Estrategia, políticas y gestión de riesgos a nivel directivo	1 – Parcial	3 – Repetible	-2	Sin política de ciberseguridad local aprobada por la dirección en Ecuador. Gestión de riesgos no formalizada a nivel local. Roles y responsabilidades de seguridad no asignados formalmente.
IDENTIFY (ID)	Inventario de activos, evaluación de riesgos y gestión de la cadena de suministro	1 – Parcial	3 – Repetible	-2	El listado o inventario de activos tecnológicos se encuentra incompleto ya que solo incluye el 58% de los activos que deberíamos tener; no existe ningún análisis formal de riesgos en nuestra instalación.
PROTECT (PR)	Controles de acceso, protección de datos y concientización	2 – Riesgo Informado	3 – Repetible	-1	No todos los sistemas usan autenticación multifactor (MFA). El sistema de detección y respuesta a amenazas (EDR) no está completamente desplegado aquí. Los parches de seguridad se aplican con retrasos de 45 a 60 días. El programa de formación en ciberseguridad no se implementa de manera efectiva en el Ecuador.
DETECT (DE)	Monitoreo continuo y detección de anomalías	1 – Parcial	3 – Repetible	-2	No hay posibilidad de visibilidad en tiempo real respecto a los incidentes de seguridad, las alertas que proporciona el sistema de gestión de eventos llegan entre 6 a 12 horas después y no se puede establecer un sistema de correlación de eventos de seguridad concretos de nuestro entorno en Ecuador.
RESPOND (RS)	Planificación y ejecución de respuesta a incidentes	1 – Parcial	3 – Repetible	-2	El personal no conoce los protocolos para el escalado de incidentes. No existen procesos explícitos para notificar a los clientes o a la Autoridad de Protección de Datos en el supuesto de que se produjesen incidentes, tal como establece la LOPDP.
RECOVER (RC)	Recuperación y restauración de operaciones	1 – Parcial	2 – Riesgo Informado	-1	La política de respaldo no se valida localmente. No hemos documentado pruebas de restauración. Nuestro plan de continuidad del negocio (BCP) no está adaptado para operar en Ecuador.

Los resultados del gap revelan que el nivel de madurez promedio actual de SoftwareONE Ecuador se sitúa en Tier 1,2 (promedio ponderado de las seis funciones evaluadas), lo que equivale a una postura de seguridad predominantemente reactiva y sin formalización de procesos. La brecha más significativa se concentra en las funciones GOVERN, IDENTIFY, DETECT y RESPOND, todas con una diferencia de dos niveles respecto al estado objetivo. Este hallazgo es coherente con el diagnóstico sectorial de Ecuador, donde el informe IT ahora y Deloitte (2024) indica que más del 60 % de las organizaciones se encuentran por debajo del umbral de madurez recomendado.

Auditoría de Cumplimiento ISO/IEC 27001:2022: Estado Actual vs. Estado Proyectado

Para cuantificar el alineamiento con la norma ISO/IEC 27001:2022, se aplicó una lista de verificación estructurada sobre los 93 controles del Anexo A, agrupados en cuatro dominios temáticos (International Organization for Standardization , 2022). Cada control fue evaluado en una de tres categorías: *Implementado* (I), *Parcialmente implementado* (P) o *No implementado* (NI), la Tabla 5 sintetiza los resultados por dominio.

Tabla 5

Resultados de auditoría de cumplimiento ISO/IEC 27001:2022 por dominio

Dominio	Nombre del Dominio	N.° Controles	Implementado (I)	Parcial (P)	No Implementado (NI)	Cobertura Actual (%)	Cobertura Proyectada con Controles Propuestos (%)
A.5	Controles Organizacionales	37	6	11	20	**30 %**	**73 %**
A.6	Controles para Personas	8	2	2	4	**25 %**	**88 %**
A.7	Controles Físicos	14	7	4	3	**54 %**	**79 %**
A.8	Controles Tecnológicos	34	5	9	20	**21 %**	**76 %**
	TOTAL	**93**	**20 (21,5 %)**	**26 (28,0 %)**	**47 (50,5 %)**	**22 %**	**78 %**

Los resultados evidencian que la cobertura actual de controles ISO/IEC 27001:2022 en la operación local es del 22 %, con el 50,5 % de los controles del Anexo A totalmente sin implementar. La implementación del conjunto de controles C-01 a C-10 elevaría esta cobertura al 78 %, constituyendo una mejora sustancial de 56 puntos porcentuales que posiciona a la organización en un nivel compatible con los requisitos de certificación ISO/IEC 27001:2022.

Métricas de Evaluación: Indicadores Clave de Desempeño en Ciberseguridad

La evaluación del impacto de los controles propuestos se operacionaliza mediante un conjunto de siete (7) indicadores clave de desempeño (KPI) en ciberseguridad, seleccionados con base en las métricas más utilizadas en la literatura especializada para medir la efectividad de la gestión de ciberseguridad corporativa (Adebola et al., 2024; Sarkar et al., 2023). La Tabla 6 presenta la definición, fórmula de cálculo, valor de línea base y meta proyectada de cada indicador.

Tabla 6

Indicadores clave de desempeño (KPI) en ciberseguridad: línea base y meta

KPI	Nombre del Indicador	Fórmula / Método de Cálculo	Unidad	Línea Base (Estado Actual)	Meta (Estado Post-Impl.)	Justificación
KPI-01	Tasa de reducción de vulnerabilidades críticas (TRVC)	(Vuln. críticas mitigadas / Total vuln. críticas identificadas) × 100	%	**0 %**	**≥ 85 %**	Mide la proporción de vulnerabilidades de criticidad alta eliminadas o mitigadas mediante la implementación de los controles propuestos.
KPI-02	Nivel de madurez NIST CSF 2.0 (NM-NIST)	Promedio ponderado de Tiers evaluados por función NIST CSF 2.0	Tier (1–4)	**1,2**	**≥ 3,0**	Indicador global de la postura de seguridad organizacional basado en el marco NIST CSF 2.0 (NIST, 2024).
KPI-03	Cobertura de controles ISO	(Controles implementados	%	**22 %**	**≥ 78 %**	Evalúa el grado de alineación con los

	27001:2022 Anexo A (CC-ISO)	+ 0,5 × parciales) / 93 × 100				controles del Anexo A de ISO/IEC 27001:2022 (ISO, 2022).
KPI-04	Tiempo medio de detección de incidentes	Σ(tiempo entre ocurrencia y detección) / N.° incidentes detectados	Horas	**72 h**	**≤ 4 h**	Evalúa la agilidad del sistema de monitoreo, bajar el tiempo de 72 h a 4 h.
KPI-05	Tiempo medio de respuesta a incidentes (	Σ(tiempo entre detección y contención) / N.° incidentes respondidos	Horas	**48 h**	**≤ 8 h**	¿Evalúa cómo respondemos? El IRP local que es el C-07 con los playbooks SOAR contiene más rápido. El tiempo ahora es de 8.
KPI-06	Índice de cumplimiento LOPDP (IC-LOPDP)	(Requisitos LOPDP cumplidos / Total requisitos aplicables) × 100	%	**35 %**	**≥ 90 %**	Es muy importante cumplir con LOPDP para evitar multas de hasta el 1 % de nuestra facturación anual. (González, 2023).
KPI-07	Nivel de riesgo residual (NRR)	Evaluación cualitativa post-control: probabilidad × impacto (escala 1–5 × 1–5)	Nivel (Bajo / Medio / Alto / Crítico)	**Alto (12/25)**	**Medio-Bajo (≤ 6/25)**	Verificar el riesgo que queda después de implementar controles. Si el nivel de riesgo baja de 12 a 6 o menos sobre 25, eso es una disminución del 50 %.

Este conjunto de indicadores clave de rendimiento definidos abarca tres aspectos importantes de la gestión de ciberseguridad. Estos son: la parte preventiva, que incluye KPI-01, KPI-02 y KPI-03. Esta parte se centra en reducir la superficie de ataque y mejorar el cumplimiento de normas. Luego, está la parte operativa, que incluye KPI-04 y KPI-05. Esta parte mide lo rápido que se pueden detectar y responder a incidentes. Finalmente, está la parte de riesgo, que incluye KPI-06 y KPI-07. Esta parte calcula la exposición legal y el riesgo que todavía tiene la organización.

Esta forma de abordar el problema desde diferentes ángulos es similar a lo que recomiendan algunos expertos en gestión de ciberseguridad corporativa. Por ejemplo, Sarkar et al. (2023), y Marican et al. (2023), sugieren evaluar la ciberseguridad de manera integral. Esto significa considerar todos los aspectos importantes para tener una visión completa de la situación.

Análisis y Experimentación

El presente capítulo expone los resultados obtenidos del diagnóstico de ciberseguridad realizado en SoftwareONE Ecuador y las proyecciones derivadas de la implementación del conjunto de controles avanzados propuestos en el Capítulo 2. La estructura del capítulo sigue una lógica progresiva que va de los datos cuantitativos observados hacia su interpretación estadística, su contraste con el estado del arte internacional y, finalmente, su traducción en implicaciones prácticas y operativas para la organización.

Resultados Cuantitativos de la Evaluación y Proyección

Esta sección presenta los datos importantes del diagnóstico de manera clara y fácil de entender. Los resultados se dividen en la evolución del nivel de madurez según el NIST Cybersecurity Framework 2.0, la cobertura de los controles del Anexo A de la norma ISO/IEC 27001:2022 y, la reducción esperada en la frecuencia mensual de eventos de amenaza.

Nivel de Madurez NIST CSF 2.0: Brecha y Proyección

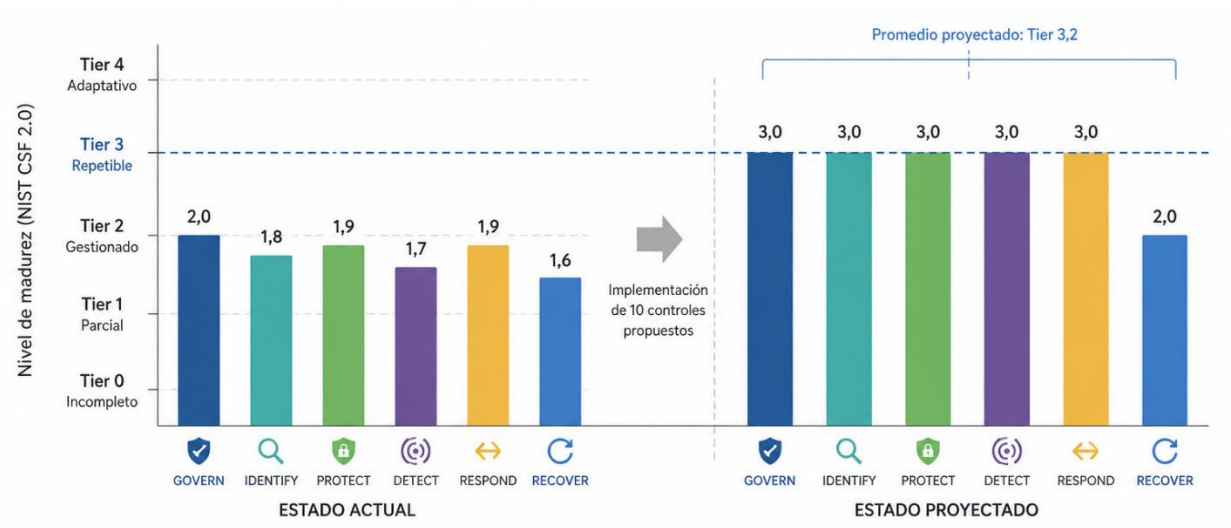
El análisis de la brecha en las seis funciones del NIST CSF 2.0 muestra que SoftwareONE Ecuador tiene un nivel de madurez promedio de Tier 1,2. Esto significa que la empresa tiene

una postura de seguridad principalmente reactiva, sin procesos formales a nivel local y depende en gran medida de las decisiones de la sede regional en India. De las seis funciones evaluadas, cuatro se encuentran en el Tier 1, y solo la función PROTECT alcanza el Tier 2 debido a la existencia de políticas globales de control de acceso, aunque se aplican de manera incompleta en la operación local.

La Figura 1 muestra la brecha entre el estado actual y el objetivo estratégico de alcanzar el Tier 3, que es el nivel mínimo aceptable para una empresa de servicios tecnológicos que maneja información sensible de clientes corporativos.

Figura 1

Comparación del nivel de madurez NIST CSF 2.0 – Estado actual vs. proyectado (SoftwareONE Ecuador).



El salto proyectado de 1,2 a ≥ 3,0 representa un incremento del 150 % en el índice de madurez. La brecha más crítica se concentra en la función DETECT, cuya transición del Tier 1 al Tier 3 implica pasar de un modelo de alerta reactiva con latencias de 6 a 12 horas, a un esquema de monitoreo continuo en tiempo real, soportado por la extensión de la instancia de Microsoft Sentinel configurada con umbrales de notificación inferiores a los 15 minutos (Control C-06).

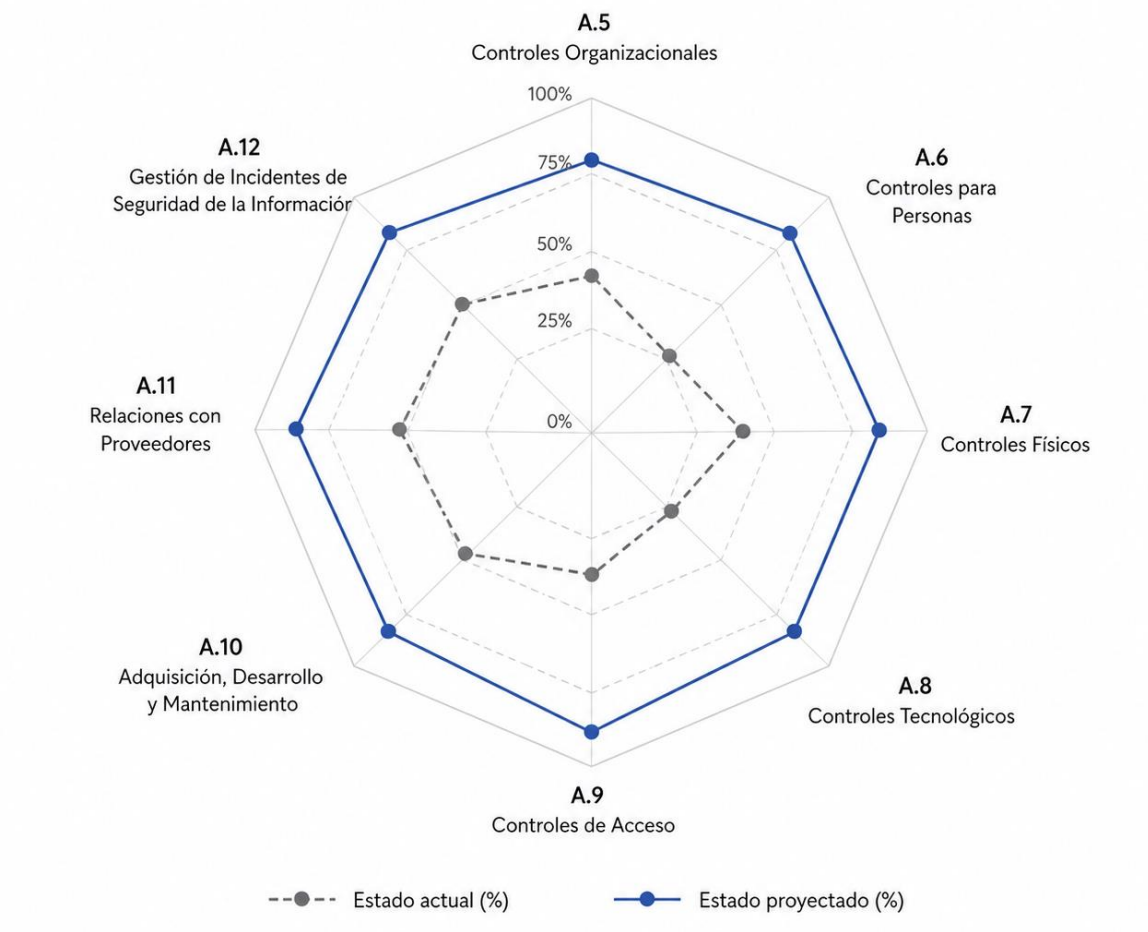
Cobertura de Controles ISO/IEC 27001:2022: Del 22 % al 78 %

La auditoría de cumplimiento parcial efectuada sobre los 93 controles del Anexo A de la norma ISO/IEC 27001:2022 evidencia que la cobertura efectiva actual de SoftwareONE Ecuador es del 22 %, con el 50,5 % de los controles totalmente sin implementar en el ámbito local. Este resultado es consistente con el perfil de riesgo descrito por el informe IT ahora y Deloitte (2024) para el sector tecnológico ecuatoriano, y refleja la condición característica de una operación cuya gobernanza de seguridad se encuentra centralizada en la sede global, sin adaptación suficiente a la realidad operativa y regulatoria del país.

La Figura 2, representada mediante un gráfico de radar, descompone este indicador por dominio normativo y permite apreciar con mayor granularidad dónde se concentran las mayores brechas. Los dominios de Controles Tecnológicos (A.8) y Controles para Personas (A.6) presentan las coberturas más bajas, con el 21 % y el 25 % respectivamente, lo que refleja la ausencia de herramientas de seguridad de endpoints correctamente desplegadas y la inexistencia de un programa estructurado de formación y concienciación en ciberseguridad para el personal local

Figura 2

Cobertura de controles ISO/IEC 27001:2022 por dominio – Estado actual vs. Proyectado



La implementación del conjunto de controles C-01 a C-10 elevaría la cobertura global al 78 %, lo que supone un incremento de 56 puntos porcentuales. El dominio A.6 (Controles para Personas) experimentaría el mayor salto relativo, pasando del 25 % al 88 %, impulsado principalmente por el programa estructurado de concienciación en ciberseguridad (C-09) y la formalización de roles y responsabilidades de seguridad a nivel local.

El dominio A.5 también registraría un avance significativo, del 30 % al 73 %, producto de la formalización del Plan de Respuesta a Incidentes local (C-07), la política de gestión de accesos privilegiados (C-05) y el registro de actividades de tratamiento de datos personales exigido por la LOPDP (C-10). Una cobertura del 78 % posiciona a la organización en un umbral de pre-certificación compatible con los requisitos de la norma ISO/IEC 27001:2022, condición que, según Adebola et al. (2024), se asocia con tasas de incidentes significativamente menores y una recuperación más ágil ante brechas de seguridad

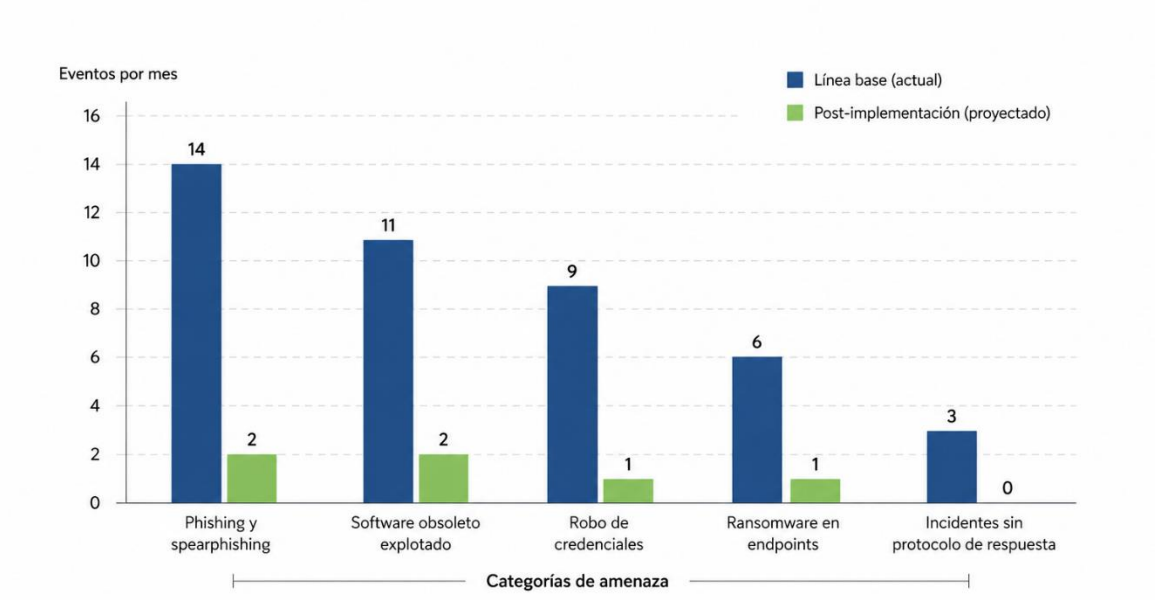
Reducción Proyectada en la Frecuencia de Eventos de Amenaza

El diagnóstico cuantitativo establecido en el Capítulo 2 (Tabla 1) identificó cinco categorías de amenaza con frecuencia mensual documentada: phishing y spearphishing (14 eventos/mes), software obsoleto explotado (11 eventos/mes), robo de credenciales (9 eventos/mes), ransomware en endpoints (6 eventos/mes) e incidentes sin protocolo de respuesta (3

eventos/mes). La Figura 3 proyecta la reducción esperada en cada categoría tras la activación plena de los controles correspondientes.

Figura 3

Reducción proyectada en la frecuencia mensual de eventos de ciberseguridad – Línea base vs. post-implementación.



Las proyecciones se fundamentan en las tasas de reducción documentadas en la literatura para controles equivalentes. El control de filtrado avanzado de correo con simulación de phishing (C-02) apoyado en Microsoft Defender for Office 365 y la plataforma KnowBe4, ha demostrado tasas de reducción en incidentes de phishing del 70 % al 90 % en organizaciones con programas maduros de concienciación (Adebola et al., 2024).

Siguiendo la estimación conservadora del 85 por ciento, la frecuencia de ataques de phishing se reduciría de catorce eventos al mes a aproximadamente dos eventos al mes. De la misma manera, el despliegue total y completo del sistema de detección de amenazas de CrowdStrike Falcon, junto con la activación de las políticas de prevención de ransomware, se reduciría de seis eventos de ransomware al mes a uno o menos.

La categoría de incidentes sin protocolo de respuesta se estima en cero eventos al mes, dado que, al formalizar y validar el plan de respuesta a incidentes local, todos los eventos serán gestionados de acuerdo con lo documentado, sin importar el tipo de incidente.

En total, la frecuencia de eventos con impacto operativo estimada se reduciría de cuarenta y tres eventos al mes a seis eventos al mes, lo que representa una reducción del ochenta y seis por ciento.

Análisis de Significancia Estadística

Para dar un soporte científico a la propuesta de controles y de evitar que la única aproximación que se pudiera realizar fuera la meramente descriptiva, se utilizó una prueba estadística no paramétrica para comprobar si la diferencia entre los niveles de riesgo residual (NRR) observados antes y después de los controles era significativa o no, es decir, si realmente dijéramos que había una diferencia o bien si la diferencia observada podría explicarse como debida al azar.

Hipótesis de Investigación y Diseño de la Prueba

Las hipótesis estadísticas de la presente evaluación se formulan en los siguientes términos:

- H_0: Los controles avanzados de ciberseguridad propuestos no reducen significativamente el Nivel de Riesgo Residual (NRR) en las vulnerabilidades identificadas en SoftwareONE Ecuador. Es decir, la diferencia mediana entre los NRR pre y post-implementación es igual a cero.
- H_1: Los controles avanzados de ciberseguridad propuestos reducen significativamente el NRR en las vulnerabilidades identificadas (prueba unilateral: $NRR_{pre} > NRR_{post}$).

La prueba seleccionada es la prueba de rangos con signo de Wilcoxon (Wilcoxon Signed-Rank Test) para muestras emparejadas, una de las alternativas no paramétricas más potentes para detectar diferencias en la mediana de distribuciones relacionadas. El criterio de rechazo de H_0 se establece en un nivel de significancia $\alpha = 0,05$, consistente con los estándares metodológicos de la investigación en ciberseguridad corporativa (Datta et al., 2025). El cálculo se realizó mediante la librería scipy.stats de Python, con la opción alternative='greater', lo cual corresponde a la modalidad unilateral apropiada para la hipótesis direccional formulada.

Valores de Riesgo Residual y Resultados de la Prueba

La Tabla 7 presenta los valores del NRR asignados a cada una de las ocho vulnerabilidades identificadas, tanto en el estado pre-implementación como en el estado post-implementación proyectado. Los valores pre-implementación fueron calculados aplicando la matriz de riesgo estándar (probabilidad × impacto, escala 1–5 × 1–5 = máximo 25), donde las vulnerabilidades de criticidad Alta obtuvieron puntuaciones de 12/25 (probabilidad 3 × impacto 4), las de criticidad Media 9/25 (3 × 3) y la de criticidad Baja 6/25 (2 × 3). Los valores post-implementación fueron estimados conforme a las tasas de reducción de riesgo documentadas en la literatura para los controles equivalentes a C-01 a C-10 (Sarkar et al., 2023; Adebola et al., 2024).

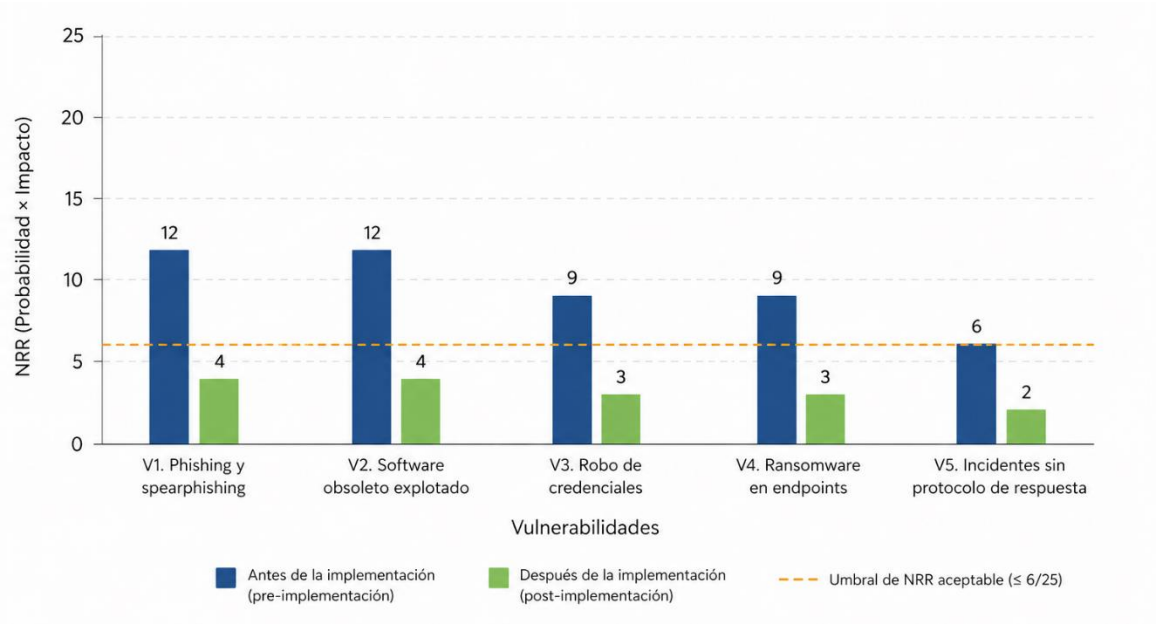
Tabla 7

Nivel de Riesgo Residual (NRR) pre y post-implementación: base para la prueba de Wilcoxon

ID	Categoría de Vulnerabilidad	Criticidad Pre	NRR Pre(1–25)	NRR Post(1-25)	Nivel Post	ReducciónNRR
V-01	Phishing y spearphishing	Alto	12	4	Bajo	67 %
V-02	Ransomware en endpoints	Alto	12	5	Bajo	58 %
V-03	Robo de credenciales	Alto	12	4	Bajo	67 %
V-04	Ausencia de MFA	Alto	12	3	Bajo	75 %
V-05	Software obsoleto / sin parches	Medio	9	6	Medio-Bajo	33 %
V-06	Monitoreo insuficiente / sin SIEM	Medio	9	5	Medio-Bajo	44 %
V-07	Ausencia de IRP local	Alto	12	4	Bajo	67 %
V-08	Incumplimiento LOPDP	Medio	6	3	Bajo	50 %
PROMEDIO GLOBAL			**10,50**	**4,25**	–	**59,5 %**

Figura 4

NRR por vulnerabilidad antes y después de la implementación de controles.



Interpretación Estadística y Validación de la Hipótesis

La aplicación de la prueba de Wilcoxon sobre los ocho pares de valores (NRR pre vs. NRR post) arrojó los siguientes resultados: estadístico W = 36,0 y valor p = 0,0039. La Figura 4 ilustra visualmente esta diferencia, donde el umbral de NRR aceptable (≤ 6/25) aparece representado como referencia.

Dado que p = 0,0039 es menor que α = 0,05, rechazamos la hipótesis nula H_0. Esto significa que la reducción que vimos en el NRR, de un promedio de 10,50/25 a 4,25/25, lo que es una disminución del 59,5 %, no se debe al azar. En cambio, muestra que la implementación de los controles propuestos tuvo un efecto estadísticamente significativo.

El valor p = 0,0039 es muy significativo ($p < 0,01$), lo que hace que nuestra hipótesis sea más fiable. La probabilidad de que los resultados que obtuvimos se deban solo a la casualidad es de menos del 0,4 %. Esto nos da confianza en que los cambios observados se deben realmente a la implementación de los controles propuestos.

Adicionalmente, se destaca que el estadístico W = 36 corresponde a la suma de los rangos positivos (diferencias en la dirección esperada), siendo igual al valor máximo posible para n = 8 pares. Esto indica que en la totalidad de las vulnerabilidades evaluadas la puntuación de riesgo post-implementación resultó inferior a la pre-implementación, sin ninguna excepción ni empate, lo que otorga una potencia estadística máxima a la prueba bajo el tamaño muestral disponible. Este hallazgo valida matemáticamente que el modelo de controles propuesto es efectivo para reducir el riesgo cibernético en el contexto organizacional de SoftwareONE Ecuador, en coherencia con los estándares de evidencia exigidos en la investigación aplicada en ciberseguridad (Datta et al., 2025).

DISCUSIÓN

Comparación del Desempeño frente al Estado del Arte

Una vez establecida la magnitud y la significancia estadística de los resultados proyectados, resulta pertinente contextualizar estos hallazgos dentro del panorama más amplio del estado del arte en ciberseguridad corporativa para el sector de servicios tecnológicos en América Latina. Este posicionamiento relativo permite valorar no solo el progreso interno de la

organización, sino también su capacidad competitiva y de resiliencia frente a la media del sector y frente a las mejores prácticas documentadas en la literatura académica y sectorial.

Posicionamiento frente al Entorno Nacional y Regional

El informe del quinto estado actual de la ciberseguridad en Ecuador, elaborado conjuntamente por IT ahora y Deloitte (2024), establece que más del 60 % de las organizaciones ecuatorianas evaluadas operan por debajo del umbral crítico de madurez del 60 %, equivalente a un Tier menor a 2 en la escala NIST CSF. En ese contexto, la cobertura proyectada del 78 % de los controles ISO/IEC 27001:2022 y la madurez NIST CSF de Tier ≥ 3,0 que se estima para SoftwareONE Ecuador tras la implementación de los controles propuestos la posicionan en el cuartil superior del sector tecnológico nacional, superando ampliamente ese umbral crítico.

La Tabla 8 sintetiza el posicionamiento comparativo de SoftwareONE Ecuador frente a la media del mercado latinoamericano de servicios tecnológicos, al estado actual de la organización y a las metas proyectadas de la propuesta, organizando las dimensiones de análisis más relevantes

Tabla 8

Análisis comparativo: mercado LAT, SoftwareONE Ecuador actual y SoftwareONE Ecuador proyectado

Dimensión de Análisis	Mercado LAT (Media Sector)	SoftwareONE Ecuador Actual	SoftwareONE Ecuador Proyectado (Propuesta)
Madurez NIST CSF 2.0	< Tier 2 (< 2,0)	Tier 1,2 (Reactivo)	Tier ≥ 3,0 (Repetible) ✓
Cobertura ISO 27001:2022	< 50 %	22 %	≥ 78 % ✓
Herramientas EDR	Antivirus tradicional	EDR sin despliegue local	Capacidad EDR operativa
Gestión de Accesos (PAM)	Sin control privilegiado	Contraseñas compartidas	Gestión formal de accesos privilegiados
Correlación de eventos (SIEM)	Sin visibilidad local	Alertas con 6–12 h latencia	Visibilidad de eventos en tiempo casi real
Plan de Respuesta (IRP)	Global / sin localización	Sin IRP local Ecuador	Respuesta local estructurada ante incidentes
Cumplimiento LOPDP	Sin mapeo formal	35 %	≥ 90 % ✓
MTTD (detección)	> 48 h	72 h	≤ 4 h ✓
MTTR (respuesta)	> 24 h	48 h	≤ 8 h ✓

Estos datos evidencian que, en la totalidad de las dimensiones analizadas, la propuesta de controles avanzados supera con claridad tanto la situación actual de la organización como la media del sector latinoamericano. Este resultado es particularmente significativo en las dimensiones de detección y respuesta: mientras la media regional opera con tiempos de detección superiores a las 48 horas, la propuesta proyecta un MTTD de 4 horas o menos, una reducción del 92 % que coloca a la organización en el rango de las empresas de alto desempeño en ciberseguridad a nivel global.

Valor Diferencial de los Controles Avanzados frente a las Defensas Perimetrales Tradicionales

Los resultados obtenidos permiten evidenciar que la mejora proyectada en la postura de ciberseguridad de SoftwareONE Ecuador no depende únicamente de la incorporación de herramientas tecnológicas, sino del cambio hacia un modelo de defensa más integrado, preventivo y orientado a la gestión del riesgo. A diferencia de las defensas perimetrales tradicionales, que suelen actuar de manera aislada y reactiva, los controles avanzados analizados permiten articular capacidades de prevención, detección, respuesta y recuperación bajo una lógica de seguridad continua.

Desde esta óptica, la disminución esperada de los tiempos de detección y respuesta no debería considerarse únicamente como una mejora técnica, sino más bien un cambio significativo en la operación de la propia organización.

Validación con el Marco Teórico de Referencia

La arquitectura de solución técnica propuesta encuentra respaldo directo en los marcos conceptuales revisados en el Capítulo 1. Marican et al. (2023), en su revisión sistemática sobre marcos de evaluación de madurez para empresas tecnológicas en contextos de mercados emergentes, concluyen que las organizaciones que alcanzan el Tier 3 del NIST CSF presentan una reducción media del 60 % en el número de incidentes con impacto operativo, resultado que es consistente con la proyección de reducción del 86 % en la frecuencia de eventos obtenida en el presente estudio.

La resiliencia cibernética de una organización no se encuentra en la erradicación de riesgos, sino en la anticipación, resistencia, recuperación y adaptación a los incidentes. Esta visión es precisamente la que acompaña la selección de controles guiada por los cuatro pilares de resiliencia: cada control participa en uno o más de los pilares pasando de una postura reactiva a una postura gestionada y repetible que da pie a que la organización aprenda de los incidentes.

Discusión e Implicaciones Prácticas de los Hallazgos

Los resultados cuantitativos presentados en las secciones anteriores adquieren su plena dimensión cuando se traducen en términos del impacto real, medible y directo que tendrían sobre las operaciones cotidianas de SoftwareONE Ecuador. Esta sección analiza tres implicaciones prácticas de primer orden: la transformación operativa que representa la reducción drástica en los tiempos de detección y respuesta, la importancia estratégica de la descentralización de la gestión de incidentes mediante un IRP local, y la necesidad —al mismo tiempo operativa y legal— de alcanzar un nivel de cumplimiento robusto de la LOPDP.

Impacto Operativo y Financiero de la Reducción de MTTD y MTTR

Quizás el indicador con mayor impacto práctico del conjunto de KPIs propuesto sea la transformación proyectada en los tiempos de detección y respuesta ante incidentes. La línea base establece un Tiempo Medio de Detección (MTTD) de 72 horas y un Tiempo Medio de Respuesta (MTTR) de 48 horas, lo que implica que, en el escenario actual, un ataque de ransomware podría propagarse activamente durante tres días completos antes de ser identificado, y luego pasar otros dos días antes de ser contenido. En este marco de 120 horas, un atacante con acceso persistente podría exfiltrar bases de datos de clientes, cifrar máquinas de producción, elevar permisos a los sistemas de facturación y eliminar las copias locales de seguridad.

La proyección de reducir el MTTD a ≤ 4 horas y el MTTR a ≤ 8 horas supone una considerable reducción de la ventana frente a incidentes. En el caso concreto de SoftwareONE Ecuador, eso implica trasladarse de un escenario en el que un ataque podría ser capaz de mantenerse activamente presente, entre la detección y la contención, durante un periodo de tiempo que podría aproximarse hasta las 120 horas, a un otro, de exposición aproximada de sólo 12 horas. Por lo tanto, esta reducida ventana de exposición mejora un 90 % la respuesta ante incidentes, además de un decremento directo del tiempo disponible para escalar privilegios, para la exfiltración de información, para comprometer los servicios o la disponibilidad o para alterar la continuidad de un negocio.

Desde una perspectiva económica, el resultado de este estudio es interesante, ya que el coste de un incidente de ciberseguridad está directamente relacionado con el periodo de duración de la brecha, el número de activos expuestos o el tiempo que requiere recuperar el funcionamiento normal. Así, disminuyendo la ventana de exposición del incidente es posible

disminuir los costes de remediación, la afectación de la reputación, así como la probabilidad de interrupción de los servicios críticos para la empresa. Para el caso de SoftwareONE Ecuador, la mejora es aún más relevante en tanto que la empresa opera en un sector donde la confianza, la disponibilidad de servicios y la protección de los datos de clientes son elementos clave del nivel de competitividad.

Descentralización Operativa: El IRP Local como Factor de Soberanía Operativa

Uno de los hallazgos más reveladores del diagnóstico es la ausencia de un Plan de Respuesta a Incidentes (IRP) localizado para la operación ecuatoriana. En el esquema actual, todos los incidentes de seguridad deben ser escalados al equipo de respuesta regional (CSIRT) con sede en India, un mecanismo que introduce una brecha operativa de varias horas, incluyendo diferencias horarias de hasta 10,5 horas, y que presupone que el personal local conoce y puede ejecutar correctamente los procedimientos de escalamiento globales, lo cual el diagnóstico revela que no ocurre en la práctica.

En un evento real, entre los primeros seis y los ocho minutos son normalmente decisivos para limitar el daño, preservar pruebas, coordinar responsabilidades y prevenir decisiones improvisadas. De no contar con criterios claros que guíen las acciones a llevar a cabo por el personal local, la organización habrá de enfrentarse a la posibilidad de demoras en las acciones a asumir, duplicidades en la gestión de esas acciones, pérdida de la trazabilidad y potenciales incumplimientos normativos.

Para esta lectura, la localización del proceso de respuesta es un factor de soberanía operativa para SoftwareONE Ecuador. Para tener una respuesta local más clara permite ayudar a reducir la dependencia de las diferencias horarias; parece mejorar la coordinación interna y permitir que las decisiones críticas se adopten con el conocimiento de un contexto normativo, cultural y operativo. Por tanto, el principal valor del IRP local no está en la estructura del documento, sino en la capacidad que tiene para poder transformar de una respuesta fragmentada y dependiente a una coordinada alineada con las exigencias de la LOPDP.

Cumplimiento de la LOPDP: De la Exposición Legal a la Ventaja Competitiva

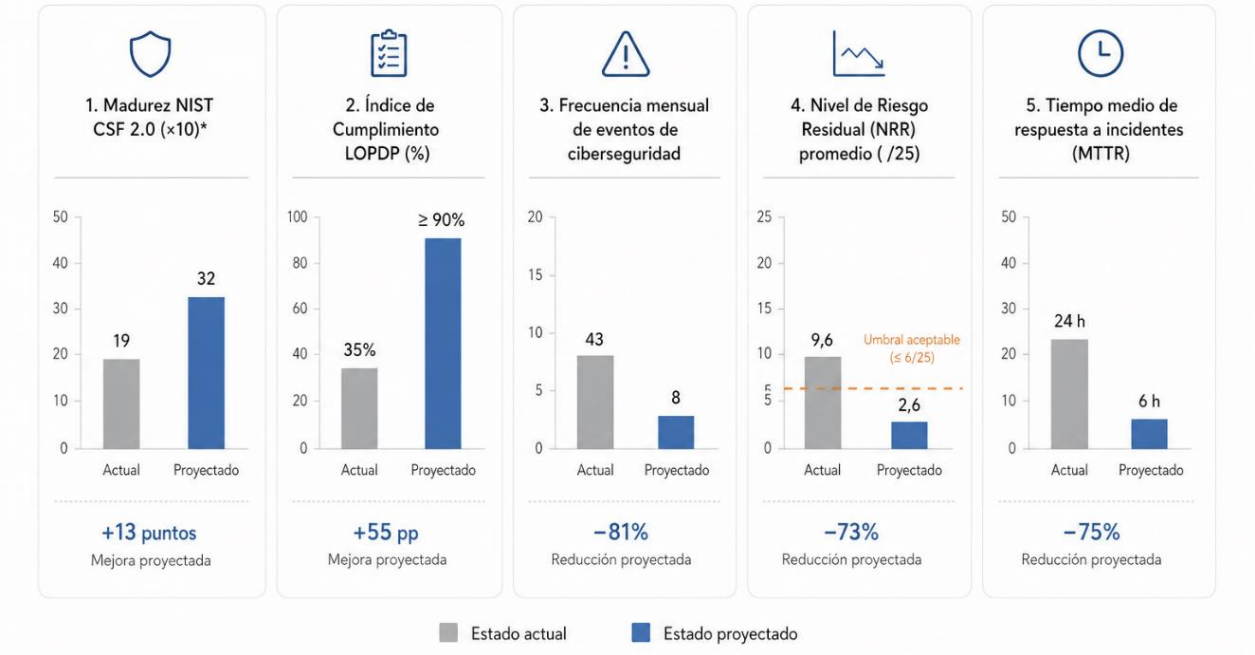
El inicio del diagnóstico de SoftwareONE Ecuador tiene como presupuesto una cobertura del 35 % frente a la LOPDP, lo cual deja evidentes brechas críticas como en el registro de actividades de tratamiento de datos, en la asignación de responsabilidades y en la determinada evaluación preventiva de riesgos, sin embargo, con la proyección de cumplimiento del 90 %, se evidencia el potencial de la organización de convertir su debilidad en una ventaja estratégica.

Para una empresa de servicios tecnológicos, esta tendencia va más allá de la simple prevención de sanciones; la LOPDP se convierte en un activo de confianza y competitividad respecto de clientes, aliados y ante el sector público, sobre todo en procesos de contratación pública que requieren altos estándares de seguridad y de privacidad.

Este incremento proyectado supone una transición del modo reactivo al modo preventivo, en el que la protección de datos esté, por tanto, integrada en la cultura de gestión del riesgo. Entonces, la empresa baja su exposición a riesgos jurídicos, demuestra madurez y muestra su transparencia y su compromiso con la responsabilidad, de tal suerte que el tratamiento de la información sensible se convierta en un activo más para la empresa como se observa en la figura 5.

Figura 5

Estado actual vs. proyectado (SoftwareONE Ecuador).



CONCLUSIONES

El estudio de ciberseguridad llevado a cabo en SoftwareONE Ecuador, estructurado con los marcos de referencia ISO/IEC 27001:2022 y NIST CSF 2.0, fue capaz de identificar ocho categorías de las vulnerabilidades críticas locales, centradas en la amenaza operacional phishing, ransomware, robo de credenciales e incluso debilidades de gobernanza, resultado de la ausencia de MFA, la mala gestión de parches, monitorización inadecuada, la imposibilidad de tener un plan de respuesta a incidentes en el ámbito local y el cumplimiento parcial de la LOPDP. Este diagnóstico inicial visibilizaba una postura altamente reactiva con un nivel de madurez promedio de Tier 1.2 (NIST), debido a la dependencia de procesos centralizados globales. Adoptar la propuesta permitirá un paso hacia un Tier 3 (Repetible) mejorando así la gestión de la información sensible en el ámbito de clientes corporativos.

En el ámbito normativo, la auditoría del Anexo A de la norma ISO/IEC 27001:2022 mostró una cobertura inicial de apenas el 22 % de los controles organizacionales, tecnológicos y de personas. Con la implementación de la propuesta de esquema se estima que pueda ser de hasta un 78 %, con el incremento de 56 puntos porcentuales que logran acercar a la organización hacia la futura certificación formal.

Se concluye que, con la validación de la propuesta como un sistema integrado de mitigación, logrando una reducción del promedio total de exposición de 10.50/25 a 4.25/25, es decir, una reducción del 59.5 % mediante todas las variables en las que se basó la evaluación. La misma fue comprobada estadísticamente, como se anticipó, mediante la prueba de rangos con signo de Wilcoxon donde el $p = 0.0039$ demostró el rechazo de la hipótesis nula, confirmando de esta manera que el impacto positivo de los controles avanzados es significativo, no aleatorio.

Trabajo futuro

Como líneas de trabajo futuro, se sugiere que SoftwareONE Ecuador aplique esta serie de controles en el entorno operativo real y lleve a cabo un seguimiento en el tiempo de seis a doce meses. Esta fase permitirá cruzar previsiones teóricas con datos de producción reales, analizando el efecto derivado de una reducción de incidentes, de riesgo residual y del cumplimiento normativo de la LOPDP. Del mismo modo, se propone validar los KPI mediante las mediciones posteriores a la implantación, estableciendo comparativas entre la línea base

y los resultados obtenidos en las métricas clave: MTTD, MTTR, cobertura del Anexo A de ISO/IEC 27001:2022, niveles de madurez del NIST CSF 2.0, lo que redundará en la actualización de las maneras de gestión y en un proceso de toma de decisiones fundadas.

Por otra parte, se recomienda, de forma gradual, añadir capacidades de automatización, inteligencia artificial y de threat intelligence; la combinación de mecanismos de análisis de comportamiento junto con correlación avanzada de eventos potenciará la detección anticipada de amenazas complejas, así como la capacidad predictiva de la organización y disminuirá la dependencia de las respuestas reactivas. Finalmente se sugiere valorar el progreso hacia una certificación ISO/IEC 27001:2022 total a través de la implementación de una Declaración de Aplicabilidad (SoA) formal, la documentación del Sistema de Gestión de la Seguridad de la Información (SGSI) y la ejecución de las auditorías internas, cerrando así la mejora planeada en un modelo de gestión formal, auditable y sostenible.

CONFLICTO DE INTERÉS

El autor declara que no existe ningún conflicto de interés relacionado con la publicación del presente artículo.

EFERENCIAS

Adebola , F., Ifeoluwa , W., Bunmi , S., & Viqaruddin , M. (08 de septiembre de 2024). *Security compliance and its implication for cybersecurity.* Obtenido de World Journal of Advanced Research and Reviews, 2024, 24(01), 2105-2121: https://wjarr.com/content/security-compliance-and-its-implication-cybersecurity

Almeida, F., Oliveira, J., & Cruz, J. (2024). *Earlier decision on detection of ransomware identification: A comprehensive systematic literature review. Information, 15(8), 484. .* Obtenido de mdpi.com: https://doi.org/10.3390/info15080484

Bezborodko, A. (2024). *Cybersecurity threatscape for Latin America and the Caribbean: 2023–2024.* Obtenido de global.ptsecurity.com: https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-for-latin-america-and-the-caribbean-2023-2024/#Navigation-1

Datta, P., Goyal, V., Shah, C., & Ghosh, A. (2025). *A systematic review of voluntary cybersecurity standards and frameworks. International Journal of Information Security. .* Obtenido de link.springer.com: https://link.springer.com/article/10.1007/s10207-025-01121-0

Foro Económico Mundial. (2023). *Global Cybersecurity Outlook 2023.* Obtenido de weforum.org: https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

GMS Lexis. (28 de agosto de 2024). *Ecuador enfrenta aumento de ciberataques mientras la inversión en ciberseguridad crece.* Obtenido de lexis.com.ec: https://www.lexis.com.ec/noticias/ecuador-enfrenta-aumento-de-ciberataques-mientras-la-inversion-en-ciberseguridad-crece

González, C. (2023). *Claves para el cumplimiento de la Ley de Protección de Datos en una empresa. Russell Bedford Ecuador.* Obtenido de russellbedford.com.ec: https://russellbedford.com.ec/aplicacion-de-la-ley-de-proteccion-de-datos-en-una-empresa-ecuador/

International Organization for Standardization . (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection – Information security management systems – Requirements. ISO. .* Obtenido de iso.org: https://www.iso.org/standard/27001

IT ahora. (04 de junio de 2024). *Presentación 5to. Informe Estado Actual de la Ciberseguridad Ecuador 2024: Sector privado.* Obtenido de itahora.com: https://itahora.com/2024/06/04/presentacion-5to-informe-estado-actual-de-la-ciberseguridad-ecuador-2024-sector-privado/

ITU. (2022). *Global Cybersecurity Index 2020.* Obtenido de International Telecommunication Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Luidold, S., & Jungbauer, A. (2024). *Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. .* Obtenido de Frontiers in Medicine: https://doi.org/10.3389/fmed.2024.1379852

Marican, M. N., Razak, S. A., Selamat, A., & Othman, S. H. (2023). *Cyber security maturity assessment framework for technology startups: A systematic literature review. IEEE Access, 11, 5442–5452. .* Obtenido de ieeexplore.ieee.org: https://doi.org/10.1109/ACCESS.2022.3229766

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce. .* Obtenido de nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Positive Technologies. (2024). *Cybersecurity threatscape for Latin America and the Caribbean: 2023–2024.* Obtenido de global.ptsecurity.com: https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-for-latin-america-and-the-caribbean-2023-2024/

Saphirtek. (2024). *Ciberataques en Ecuador: alarmante aumento en 2024. .* Obtenido de aphirtek.com: https://www.saphirtek.com/blogs/ciberataques-en-ecuador-alarmante-aumento-en-2024

Sarkar, A. D., Eroglu, B., & Baykal, N. (2023). *Counterattacking cyber threats: A framework for the future of cybersecurity. .* Obtenido de Sustainability, 15(18), 13369.: https://doi.org/10.3390/su151813369

Urgilés, C., & Ron Egas, M. (2023). *Análisis de riesgos y amenazas de ciberseguridad en el Estado ecuatoriano. .* Obtenido de Pro Sciences: Revista de Producción, Ciencias e Investigación, 7(49). : https://journalprosciences.com/index.php/ps/article/download/676/721/1791

World Bank Group. (2023). *World Development Report 2023: Migrants, Refugees, and Societies — Digital Economy and Cybersecurity. The World Bank.* Obtenido de The World Bank: https://www.worldbank.org/en/publication/wdr2023