Artículo Científico

BLEZ TECNOLÓGICO ONLINE

CEC Revista Científica Enfoques del Conocimiento

ISSN: 3151-8486

Seguridad informática y prevención de ataques cibernéticos en sistemas organizacionales

IT Security and Cyberattack Prevention in Organizational Systems

Galarza-Sánchez, Paulo César [1]
https://orcid.org/0000-0003-4668-1158
paulogalarza@tsachila.edu.ec
Ecuador, Santo Domingo, Instituto Superior Tecnológico Tsa´chila.

Herrera-Ramírez, César Daniel [2]
https://orcid.org/0009-0009-7600-8643
chherrera15@espe.edu.ec
Ecuador, Sangolqui, Universidad de las Fuerzas Armadas - ESPE.

Borja-Almeida, Luis Gonzalo [3]
https://orcid.org/0009-0001-1338-1493
lugoboal.espe@gmail.com
México, Cancún, Universidad Americana de Europa.

Autor de correspondencia [1]

DOI / URL: https://doi.org/10.55813/gaea/revistacec/v2/n3/39

Resumen: La transformación digital ha incrementado la exposición de los sistemas organizacionales a amenazas capaces de comprometer la confidencialidad, integridad y disponibilidad de la información, por lo que este estudio tuvo como propósito analizar las principales amenazas, vulnerabilidades y estrategias preventivas aplicables a la gestión de la seguridad informática. Se desarrolló una revisión bibliográfica de enfoque cualitativo, diseño no experimental, alcance exploratorio y carácter descriptivo-analítico, mediante la selección de literatura científica y documentos técnicos en español e inglés, priorizando publicaciones recientes. La información fue organizada en una matriz documental y examinada mediante análisis temático de contenido y comparación narrativa. Los resultados evidenciaron que los ataques suelen originarse en la convergencia de vulnerabilidades técnicas, configuraciones inadecuadas, credenciales comprometidas, prácticas inseguras y debilidades de gestión. Asimismo, se identificó que la defensa en profundidad, la autenticación reforzada, la segmentación, el monitoreo, las copias de seguridad verificadas, la capacitación continua y el liderazgo institucional fortalecen la capacidad preventiva. Se concluye que la ciberseguridad debe gestionarse como una responsabilidad estratégica y sociotécnica, sustentada en la integración de tecnología, cultura organizacional, gobierno, respuesta planificada, recuperación operativa y mejora continua.

Palabras clave: seguridad informática; ciberseguridad; ataques cibernéticos; gestión del riesgo; resiliencia organizacional.

Check for updates

Received: 15/Jun/2025
Accepted: 14/Jul/2025
Published: 16/Ago/2025

Cita: Galarza-Sánchez, P. C., Herrera-Ramírez, C. D., & Borja-Almeida, L. G. (2025). Seguridad informática y prevención de ataques cibernéticos en sistemas organizacionales. *Revista Científica Enfoques Del Conocimiento*, *2*(3), 49-73. https://doi.org/10.55813/gaea/revistacec/v2/n3/39

Revista Científica Enfoques del Conocimiento (RCEC)
https://www.blez.edu.ec
https://revistacec.blez.edu.ec
revistacec@blez.edu.ec

Abstract:

Digital transformation has increased the exposure of organizational systems to threats capable of compromising the confidentiality, integrity, and availability of information. Therefore, this study aimed to analyze the main threats, vulnerabilities, and preventive strategies applicable to information security management. A qualitative literature review was conducted using a non-experimental design, an exploratory scope, and a descriptive-analytical approach through the selection of scientific literature and technical documents published in English and Spanish, with priority given to recent publications. The information was organized in a documentary analysis matrix and examined through thematic content analysis and narrative comparison. The findings showed that cyberattacks commonly arise from the convergence of technical vulnerabilities, inadequate configurations, compromised credentials, unsafe practices, and management weaknesses. Likewise, defense-in-depth strategies, enhanced authentication, network segmentation, continuous monitoring, verified backups, ongoing training, and institutional leadership were identified as factors that strengthen preventive capacity. It is concluded that cybersecurity should be managed as a strategic and sociotechnical responsibility based on the integration of technology, organizational culture, governance, planned incident response, operational recovery, and continuous improvement.

Keywords: information security; cybersecurity; cyberattacks; risk management; organizational resilience.

1. Introducción

La transformación digital ha incrementado la dependencia de las organizaciones respecto de infraestructuras conectadas, servicios en la nube, aplicaciones empresariales y flujos permanentes de información, por lo que una interrupción o intrusión puede comprometer procesos esenciales. En este contexto, la seguridad informática ha dejado de constituir una responsabilidad exclusivamente técnica para convertirse en un componente de la gestión integral del riesgo. El panorama continúa siendo dinámico: la Agencia de la Unión Europea para la Ciberseguridad examinó 4.875 incidentes ocurridos entre julio de 2024 y junio de 2025, lo que evidencia la persistencia y diversidad de las amenazas dirigidas contra entornos digitales interconectados (European Union Agency for Cybersecurity [ENISA], 2025; National Institute of Standards and Technology [NIST], 2024).

Asimismo, la exposición de los sistemas organizacionales se intensifica por la convergencia de vulnerabilidades técnicas, configuraciones inadecuadas, controles débiles de identidad y acceso, demora en la actualización de software, dependencia de terceros y limitada articulación entre la estrategia institucional y la gestión tecnológica. A estos factores se añaden prácticas inseguras de los usuarios,

desconocimiento de las políticas internas y respuestas inadecuadas ante eventos sospechosos. Por consiguiente, la inversión en herramientas tecnológicas no garantiza por sí sola una protección efectiva, debido a que los comportamientos, conocimientos y actitudes del personal influyen en la capacidad preventiva de la organización y en el cumplimiento cotidiano de los controles establecidos (da Veiga et al., 2020; Khando et al., 2021; Zwilling et al., 2022).

Las afectaciones derivadas de un ataque cibernético pueden extenderse más allá del daño inmediato a los equipos o aplicaciones. La pérdida de confidencialidad expone información estratégica, financiera o personal; la alteración de datos compromete su integridad y puede distorsionar decisiones; mientras que la indisponibilidad de servicios interrumpe operaciones y reduce la continuidad institucional. De igual manera, los incidentes pueden generar pérdidas económicas, disminución de la productividad, costos de recuperación, deterioro reputacional y pérdida de confianza entre clientes, trabajadores y aliados. Cuando los sistemas se encuentran interconectados, estas consecuencias pueden propagarse hacia proveedores y otros actores de la cadena organizacional, aumentando la complejidad de la respuesta y la recuperación (Khando et al., 2021; Prümmer et al., 2024).

Frente a este escenario, la literatura reconoce que los controles técnicos —como la autenticación reforzada, la gestión de vulnerabilidades, la segmentación, el monitoreo y las copias de seguridad— son indispensables, aunque deben integrarse con gobierno institucional, políticas comprensibles, capacitación continua y mecanismos de respuesta. La cultura de ciberseguridad adquiere especial relevancia porque vincula valores, percepciones y comportamientos compartidos con la protección diaria de la información. En consecuencia, el respaldo de la alta dirección, la comunicación interna, la formación contextualizada y la participación activa del personal constituyen condiciones necesarias para superar un cumplimiento meramente formal y consolidar prácticas preventivas sostenibles (Alshaikh, 2020; Sutton & Tompson, 2025; Uchendu et al., 2021).

No obstante, la revisión crítica de los estudios revela limitaciones que dificultan trasladar el conocimiento disponible a decisiones organizacionales consistentes. Aunque se han propuesto numerosos modelos de cultura, concienciación y capacitación, gran parte de las evaluaciones utiliza cuestionarios de autopercepción, mientras que pocos marcos han sido comprobados de manera prolongada en entornos reales. Además, las investigaciones sobre formación presentan diferencias en contenidos, duración, poblaciones y criterios de efectividad; varios estudios emplean muestras reducidas, diseños no experimentales o participantes ajenos al contexto laboral. Estas inconsistencias impiden determinar con suficiente claridad qué combinaciones de controles técnicos, prácticas de gestión y estrategias conductuales producen resultados preventivos sostenibles en organizaciones con características distintas (Prümmer et al., 2024; Uchendu et al., 2021).

En consecuencia, una revisión bibliográfica resulta pertinente para integrar evidencia dispersa, contrastar enfoques y reconocer relaciones entre amenazas, vulnerabilidades, cultura organizacional, controles preventivos y capacidad de respuesta. Su relevancia social se relaciona con la protección de servicios, información y usuarios; su valor teórico radica en articular perspectivas técnicas y socioconductuales; y su utilidad metodológica consiste en organizar criterios comparables para evaluar estrategias de prevención. El estudio es viable debido a la disponibilidad de literatura científica indexada, estándares internacionales y documentos técnicos de acceso público, sin requerir intervención directa sobre personas o sistemas. La rigurosidad dependerá de una búsqueda trazable, criterios explícitos de selección y atribución fiel de las fuentes consultadas (NIST, 2024; Snyder, 2019).

Sobre esta base, el objetivo general de la revisión es analizar críticamente la evidencia científica y técnica relacionada con la seguridad informática y la prevención de ataques cibernéticos en sistemas organizacionales. Para alcanzarlo, se plantean como objetivos específicos identificar las principales amenazas, vulnerabilidades y condiciones organizacionales asociadas al riesgo; comparar los controles técnicos, administrativos y humanos utilizados para prevenir incidentes; y sintetizar criterios, indicadores y prácticas que orienten la gestión integral de la ciberseguridad. La contribución esperada consiste en superar la descripción aislada de herramientas y proponer una comprensión articulada entre gobierno, tecnología, cultura y comportamiento, atendiendo la brecha existente entre la adopción formal de medidas y su efectividad verificable en contextos organizacionales (NIST, 2024; Sutton & Tompson, 2025).

2. Materiales y métodos

La investigación se desarrolló mediante un enfoque cualitativo, con diseño no experimental y de carácter documental, debido a que la unidad de análisis estuvo constituida por publicaciones científicas y documentos técnicos relacionados con la seguridad informática y la prevención de ataques cibernéticos en sistemas organizacionales. El estudio adoptó un alcance exploratorio y descriptivo-analítico, orientado a reconocer las principales perspectivas teóricas, amenazas, vulnerabilidades, controles preventivos y factores organizacionales abordados en la literatura. Asimismo, se emplearon los métodos analítico y sintético para examinar individualmente los aportes de las fuentes y, posteriormente, integrarlos en categorías interpretativas. Debido a la naturaleza documental del estudio, no se definió una población humana ni se efectuó un cálculo estadístico de muestra; el corpus quedó determinado por la pertinencia y suficiencia conceptual de los documentos seleccionados (Picoy-Gonzales et al., 2023).

Se priorizaron documentos publicados entre enero de 2019 y julio de 2026 con el propósito de recuperar evidencia relacionada con amenazas, tecnologías y estrategias

organizacionales contemporáneas. No obstante, se admitieron publicaciones anteriores cuando presentaron modelos teóricos, conceptos fundamentales o procedimientos metodológicos indispensables para interpretar el desarrollo del campo. La búsqueda se ejecutó en español e inglés y contempló artículos científicos, revisiones bibliográficas, estudios empíricos, actas académicas relevantes, estándares técnicos y documentos emitidos por organismos especializados. La combinación de distintas fuentes permitió ampliar la cobertura temática y disminuir la posibilidad de omitir estudios pertinentes (Celi-Párraga et al., 2023a).

Para recuperar la información se emplearon términos normalizados y expresiones equivalentes relacionadas con el objeto de estudio. La ecuación general en inglés integró los descriptores “information security” OR “cybersecurity” OR “cyber security”, combinados mediante el operador AND con “cyberattack prevention” OR “security controls” OR “cybersecurity awareness” OR “cyber risk management” y “organization” OR “enterprise” OR “organizational systems”. De forma complementaria, se utilizaron las expresiones en español “seguridad informática”, “ciberseguridad”, “prevención de ataques cibernéticos”, “controles de seguridad”, “gestión del riesgo cibernético” y “sistemas organizacionales”. Las ecuaciones fueron adaptadas a las características de cada base de datos mediante operadores booleanos, comillas y truncamientos. El procedimiento mantuvo flexibilidad para incorporar términos emergentes identificados durante la lectura preliminar, sin modificar el propósito central de la revisión (Celi-Párraga et al., 2023b).

Los criterios de inclusión comprendieron publicaciones con texto completo disponible, redactadas en español o inglés y vinculadas directamente con amenazas cibernéticas, vulnerabilidades, controles técnicos, políticas institucionales, cultura de seguridad, comportamiento de los usuarios, gestión de incidentes o resiliencia organizacional. También se incorporaron investigaciones cuantitativas, cualitativas y mixtas, así como revisiones y documentos técnicos que aportaran información verificable para el análisis. Se excluyeron registros duplicados, publicaciones sin identificación de autoría, documentos de carácter exclusivamente comercial, contenidos sin respaldo metodológico y estudios centrados únicamente en dispositivos personales sin relación con procesos organizacionales. La selección se efectuó mediante la revisión sucesiva del título, el resumen y el texto completo. Las decisiones de inclusión se registraron en una matriz de control para conservar la trazabilidad del proceso, sin atribuir a la investigación el carácter de revisión sistemática ni realizar metaanálisis (Mina-Bone, 2024).

Posteriormente, la información se organizó mediante una matriz documental diseñada para registrar autoría, año de publicación, país o contexto, propósito del estudio, enfoque metodológico, tipo de amenaza analizada, vulnerabilidades identificadas, medidas preventivas, factores humanos y organizacionales, principales resultados y limitaciones. La extracción mantuvo criterios uniformes para facilitar la comparación entre publicaciones con diseños y perspectivas diferentes. Además, se valoraron la correspondencia entre objetivos y resultados, la claridad metodológica, la pertinencia

respecto del tema y la solidez de las conclusiones presentadas. Los documentos institucionales se examinaron considerando la autoridad del organismo emisor, la vigencia de la versión y la transparencia de la información. Este procedimiento permitió integrar evidencia teórica, empírica y técnica sin asumir que todas las fuentes poseían el mismo alcance o nivel de respaldo científico.

Finalmente, los datos fueron procesados mediante análisis temático de contenido y comparación narrativa. La lectura analítica permitió identificar regularidades, diferencias, relaciones conceptuales y vacíos de conocimiento, mientras que la síntesis agrupó la evidencia en cinco ejes: amenazas y vulnerabilidades; controles tecnológicos; gobierno y gestión del riesgo; cultura organizacional y comportamiento humano; y respuesta, recuperación y resiliencia. Las conclusiones se formularon a partir de la convergencia entre distintas fuentes y se señalaron las discrepancias cuando los resultados dependían del contexto, el sector o el diseño metodológico. Debido a la heterogeneidad de los documentos, no se realizaron estimaciones estadísticas ni inferencias causales. En el ámbito ético, se respetaron la autoría intelectual, la atribución de las ideas y la presentación fiel de los resultados originales, sin intervención sobre personas, organizaciones o sistemas informáticos (Casanova-Villalba & Casanova-Villalba, 2024).

3. Resultados

3.1. Estrategias integrales para la prevención de ataques cibernéticos en sistemas organizacionales

La revisión de la literatura evidencia que la prevención de ataques cibernéticos constituye un proceso multidimensional cuya efectividad depende de la integración equilibrada de capacidades tecnológicas, estructuras de gobierno, prácticas de gestión, mecanismos de respuesta y comportamientos humanos. En consecuencia, la seguridad informática no debe concebirse como la acumulación de herramientas defensivas independientes, sino como un sistema articulado de decisiones y controles orientados a proteger la confidencialidad, integridad y disponibilidad de la información, así como a preservar la continuidad de las operaciones. Esta perspectiva resulta especialmente relevante porque las amenazas actuales explotan simultáneamente deficiencias técnicas, errores de configuración, debilidades procedimentales, accesos excesivos y conductas humanas susceptibles de manipulación. Por ello, las organizaciones requieren estrategias capaces de anticipar riesgos, reducir superficies de exposición, detectar actividades anómalas y recuperar funciones esenciales después de un incidente (Pascoe et al., 2024; Ross et al., 2021).

Tabla 1

Dimensiones estratégicas para la prevención integral de ataques cibernéticos

Dimensión	Elementos principales	Propósito en la seguridad informática
Capacidades tecnológicas	Herramientas de protección, monitoreo, detección y control de amenazas	Prevenir accesos no autorizados, reducir vulnerabilidades e identificar actividades anómalas
Gobierno de la seguridad	Políticas, responsabilidades, toma de decisiones y supervisión institucional	Garantizar una gestión coordinada y alineada con los objetivos organizacionales
Prácticas de gestión	Evaluación de riesgos, configuración segura, control de accesos y actualización de sistemas	Disminuir las superficies de exposición y corregir debilidades técnicas o procedimentales
Mecanismos de respuesta	Protocolos de actuación, contención de incidentes, recuperación y continuidad operativa	Reducir el impacto de los ciberataques y restablecer las funciones esenciales
Comportamiento humano	Capacitación, concienciación, buenas prácticas y prevención de la ingeniería social	Disminuir errores humanos y conductas susceptibles de manipulación
Protección de la información	Confidencialidad, integridad y disponibilidad de los datos	Preservar la seguridad, confiabilidad y accesibilidad de la información
Enfoque integral	Articulación de tecnologías, procesos, personas y controles	Consolidar un sistema multidimensional de prevención, detección, respuesta y recuperación

Nota: La tabla sintetiza los principales componentes que intervienen en la prevención de ataques cibernéticos, destacando la necesidad de articular capacidades tecnológicas, estructuras de gobierno, prácticas de gestión, mecanismos de respuesta y factores humanos para proteger la confidencialidad, integridad y disponibilidad de la información, así como garantizar la continuidad operativa. Elaboración propia con base en Pascoe et al. (2024) y Ross et al. (2021) (Autores, 2026).

Desde una perspectiva sistémica, la prevención efectiva exige abandonar la lógica reactiva basada exclusivamente en corregir daños después de una intrusión. El Marco de Ciberseguridad 2.0 propone organizar la gestión mediante las funciones de gobernar, identificar, proteger, detectar, responder y recuperar, las cuales conforman un ciclo continuo y adaptable a organizaciones de diferente tamaño, sector y nivel de madurez. Esta estructura permite comprender que la protección tecnológica debe encontrarse precedida por decisiones de gobierno y evaluación del riesgo, y complementada por capacidades de detección, respuesta y recuperación. En este sentido, la integralidad no implica aplicar indiscriminadamente todos los controles disponibles, sino seleccionar medidas proporcionales a la criticidad de los activos, las amenazas previsibles, los recursos institucionales y las consecuencias potenciales de una interrupción (Pascoe et al., 2024).

3.1.1. Principales amenazas y vulnerabilidades identificadas

Los resultados muestran que el panorama contemporáneo de amenazas se caracteriza por la coexistencia de campañas masivas, ataques dirigidos y operaciones híbridas que combinan ingeniería social, explotación de vulnerabilidades, compromiso de credenciales, instalación de software malicioso y afectación deliberada de servicios. El informe de ENISA correspondiente a 2025 examinó 4.875 incidentes ocurridos entre julio de 2024 y junio de 2025, evidenciando que las organizaciones se

enfrentan a actores que reutilizan herramientas, perfeccionan técnicas conocidas, incorporan nuevos modelos de ataque y aprovechan vulnerabilidades en infraestructuras digitales interdependientes. Esta evolución demuestra que la amenaza no se limita a códigos maliciosos aislados, sino que comprende ecosistemas delictivos capaces de adaptar sus procedimientos a las defensas existentes y de combinar mecanismos técnicos con tácticas de manipulación humana (European Union Agency for Cybersecurity [ENISA], 2025).

Entre las amenazas más recurrentes se encuentran el *phishing*, el ransomware, el malware, el robo de credenciales, la denegación de servicio, la exfiltración de información y el acceso no autorizado a sistemas institucionales. El *phishing* conserva una elevada relevancia debido a que permite obtener contraseñas, distribuir archivos maliciosos o inducir acciones perjudiciales mediante mensajes que imitan comunicaciones legítimas. Su peligrosidad aumenta cuando se combina con técnicas de ingeniería social dirigidas, puesto que los atacantes pueden utilizar información pública para construir mensajes verosímiles y explotar factores como la urgencia, la autoridad, la confianza o el temor. En consecuencia, la sofisticación de un ataque no depende únicamente de la complejidad del código empleado, sino también de la capacidad del adversario para comprender los procesos internos y manipular las decisiones de los usuarios (Khando et al., 2021; ENISA, 2025).

El ransomware representa una amenaza particularmente crítica porque trasciende el cifrado de archivos y puede comprometer simultáneamente la continuidad operativa, la confidencialidad de la información y la reputación institucional. Las variantes contemporáneas pueden incorporar mecanismos de doble o múltiple extorsión, mediante los cuales los atacantes extraen información antes de cifrarla y posteriormente amenazan con divulgarla o intensificar la interrupción. El análisis empírico realizado por Connolly et al. sobre 55 ataques ocurridos en 50 organizaciones evidenció que la gravedad del impacto se relacionaba con la postura de seguridad institucional, mientras que el tamaño organizacional no explicaba por sí mismo la severidad experimentada. Por consiguiente, la vulnerabilidad frente al ransomware depende menos de la dimensión de la entidad que de la calidad de sus controles, la segmentación de sus redes, la protección de sus respaldos y su preparación para responder (Connolly et al., 2020).

Las vulnerabilidades identificadas en la literatura no corresponden exclusivamente a fallos de programación. También incluyen configuraciones inseguras, sistemas sin actualización, aplicaciones heredadas, servicios expuestos innecesariamente, privilegios excesivos, autenticación insuficiente, ausencia de segmentación y desconocimiento de los activos conectados. Estas debilidades pueden acumularse hasta conformar rutas de ataque que permiten a un adversario pasar desde un acceso inicial aparentemente limitado hacia recursos de mayor criticidad. De esta manera, una credencial comprometida puede convertirse en el punto de partida para el desplazamiento lateral, la elevación de privilegios, la desactivación de mecanismos defensivos y la afectación de servidores esenciales. La evidencia indica, por tanto,

que la severidad de un incidente suele surgir de la interacción entre múltiples deficiencias y no de una única vulnerabilidad aislada (Connolly et al., 2020; Pascoe et al., 2024).

Asimismo, la expansión de los servicios en la nube, el trabajo remoto, los dispositivos móviles, las plataformas colaborativas y los proveedores externos ha incrementado la superficie de exposición organizacional. Las fronteras tradicionales de la red se han vuelto menos definidas, debido a que los datos y aplicaciones pueden encontrarse distribuidos entre infraestructuras internas, entornos virtuales y servicios administrados por terceros. En estas condiciones, una organización puede resultar afectada por vulnerabilidades presentes en componentes que no controla directamente, como bibliotecas de software, plataformas compartidas, proveedores de servicios o sistemas integrados. Por consiguiente, el análisis del riesgo debe incorporar las relaciones de dependencia tecnológica y la seguridad de la cadena de suministro, evitando limitar la evaluación al perímetro físico de la institución (Rose et al., 2020; Pascoe et al., 2024).

Otro hallazgo relevante es la necesidad de interpretar las amenazas mediante secuencias de ataque y no únicamente a partir de categorías independientes. Un incidente puede comenzar con la obtención de información pública, continuar con el envío de un mensaje fraudulento, producir el compromiso de una cuenta y culminar con la extracción de datos o la interrupción de servicios. Esta visión permite reconocer que cada etapa ofrece oportunidades diferentes de prevención, detección o contención. La inteligencia de amenazas contribuye a este propósito mediante la recopilación, evaluación y difusión de información sobre actores, indicadores, tácticas y procedimientos, lo que favorece la contextualización de alertas y la priorización de riesgos. Sin embargo, su utilidad depende de que la información obtenida se vincule con los activos y procesos específicos de cada organización (Saeed et al., 2023).

3.1.2. Medidas tecnológicas para la prevención de incidentes

La literatura revisada identifica la defensa en profundidad como uno de los principios fundamentales para disminuir la probabilidad y el impacto de los ataques cibernéticos. Este enfoque plantea la implementación de controles complementarios en diferentes niveles, de modo que la falla de una medida no implique la pérdida inmediata de todos los mecanismos de protección. La combinación de inventarios de activos, controles de acceso, segmentación, actualización de sistemas, protección de terminales, monitoreo, cifrado y respaldos permite construir múltiples barreras frente a las acciones del adversario. No obstante, la eficacia de esta arquitectura depende de la coherencia entre sus componentes, debido a que una herramienta avanzada puede perder utilidad cuando existen activos desconocidos, configuraciones deficientes o responsabilidades operativas ambiguas (Pascoe et al., 2024; Ross et al., 2021).

El punto de partida de una estrategia tecnológica debe ser el conocimiento preciso de los recursos que requieren protección. La identificación de servidores, aplicaciones, bases de datos, dispositivos, cuentas, servicios externos y flujos de información

permite establecer prioridades de acuerdo con su criticidad. Sin un inventario actualizado, la organización puede mantener sistemas expuestos que no reciben mantenimiento, activos que operan con configuraciones obsoletas o servicios cuya existencia es desconocida para los responsables de seguridad. Por ello, la gestión de activos debe vincularse con procesos de clasificación de información y evaluación de riesgos, de manera que los recursos esenciales reciban medidas de protección proporcionales a las consecuencias que produciría su pérdida, alteración o indisponibilidad (Pascoe et al., 2024).

La gestión de vulnerabilidades constituye otra capacidad prioritaria y debe desarrollarse como un proceso permanente de descubrimiento, evaluación, corrección y verificación. La aplicación oportuna de actualizaciones reduce oportunidades de explotación, aunque la priorización no debería basarse exclusivamente en la gravedad técnica asignada a cada vulnerabilidad. También es necesario considerar si existe evidencia de explotación, si el sistema afectado se encuentra expuesto, si almacena información sensible y si participa en procesos críticos. De este modo, la corrección se orienta hacia los riesgos con mayor probabilidad e impacto, evitando que los equipos concentren recursos en vulnerabilidades de escasa relevancia mientras permanecen desatendidos fallos con capacidad real de comprometer la operación. La evidencia sobre ransomware confirma que las posturas deficientes de actualización y protección incrementan la severidad potencial de los incidentes (Connolly et al., 2020; Pascoe et al., 2024).

En materia de identidad y acceso, la autenticación multifactor, el principio de privilegio mínimo y la revisión periódica de permisos constituyen mecanismos indispensables para reducir el uso indebido de credenciales. La autenticación multifactor dificulta que una contraseña comprometida sea suficiente para acceder a los recursos institucionales, mientras que el privilegio mínimo limita las acciones disponibles para cada usuario según sus responsabilidades. Esta lógica se fortalece mediante el enfoque de confianza cero, el cual elimina la concesión automática de confianza basada únicamente en la ubicación del usuario o del dispositivo dentro de la red. En consecuencia, cada solicitud debe evaluarse considerando la identidad, el estado del dispositivo, la sensibilidad del recurso y el contexto de acceso, con verificaciones proporcionales al nivel de riesgo (Rose et al., 2020).

La segmentación de redes complementa la gestión de identidades porque restringe el desplazamiento lateral de un atacante después del acceso inicial. En una infraestructura sin divisiones adecuadas, una cuenta o dispositivo comprometido puede facilitar la exploración y afectación de múltiples recursos internos. Por el contrario, la separación de servidores, usuarios, dispositivos críticos y entornos administrativos permite establecer controles diferenciados y contener la propagación de actividades maliciosas. La microsegmentación amplía esta lógica mediante políticas específicas aplicadas a recursos y cargas de trabajo, reduciendo la dependencia del perímetro tradicional. No obstante, la segmentación requiere planificación y supervisión continua, puesto que reglas excesivamente permisivas o

configuraciones inconsistentes pueden mantener rutas de comunicación no previstas (Rose et al., 2020; Ross et al., 2021).

La detección temprana requiere visibilidad sobre redes, terminales, identidades, aplicaciones y servicios externos. Los sistemas de gestión y correlación de eventos, las herramientas de detección y respuesta en terminales, los mecanismos de supervisión de tráfico y las soluciones de análisis de comportamiento pueden facilitar la identificación de actividades inusuales. Sin embargo, la incorporación de estas tecnologías no garantiza automáticamente una detección eficaz, ya que su desempeño depende de la calidad de los registros, la correcta configuración de reglas, la disponibilidad de personal capacitado y la capacidad para diferenciar comportamientos legítimos de eventos potencialmente maliciosos. En este contexto, la inteligencia de amenazas puede enriquecer el análisis mediante indicadores y conocimientos sobre tácticas adversarias, siempre que dicha información se adapte al entorno institucional y no se utilice de forma descontextualizada (Saeed et al., 2023).

El cifrado constituye una medida relevante para limitar la exposición de información sensible cuando se produce acceso no autorizado, pérdida de dispositivos o interceptación de comunicaciones. Su aplicación debe abarcar datos almacenados y datos en tránsito, acompañada por una gestión segura de claves y procedimientos que aseguren la disponibilidad legítima de la información. No obstante, el cifrado no reemplaza la prevención de accesos indebidos, debido a que un atacante que obtiene credenciales válidas o compromete una aplicación puede acceder a los datos después de que estos han sido descifrados por el sistema. Por consiguiente, debe implementarse como parte de una estrategia más amplia que incluya controles de identidad, supervisión, clasificación de información y protección de los entornos donde se procesan los datos (Pascoe et al., 2024; Ross et al., 2021).

Las copias de seguridad representan una de las principales capacidades para disminuir las consecuencias del ransomware y otros eventos destructivos; sin embargo, su existencia no garantiza la recuperación. Los respaldos pueden resultar inutilizados cuando permanecen conectados permanentemente al mismo entorno, cuando comparten credenciales administrativas con los sistemas principales o cuando nunca han sido sometidos a pruebas de restauración. En consecuencia, las organizaciones deben conservar versiones protegidas, controlar rigurosamente el acceso y verificar periódicamente la integridad de la información almacenada. Además, la recuperación debe asociarse con objetivos definidos de tiempo y disponibilidad, de modo que las prioridades técnicas respondan a las necesidades reales de continuidad institucional (Connolly et al., 2020; Ross et al., 2021).

En conjunto, las medidas tecnológicas deben diseñarse para operar bajo el supuesto de que alguna barrera puede ser superada. La prevención absoluta resulta difícil en entornos complejos e interconectados; por ello, las arquitecturas deben incorporar capacidades de contención, redundancia, recuperación y adaptación. La ingeniería de resiliencia propone desarrollar sistemas capaces de anticipar condiciones adversas,

resistir afectaciones, recuperar funciones esenciales y modificar sus defensas después de un evento. Esta concepción transforma la seguridad desde una estrategia centrada únicamente en impedir intrusiones hacia un enfoque orientado a preservar las funciones críticas incluso cuando se produce un compromiso parcial (Ross et al., 2021).

3.1.3. Influencia del factor humano y la cultura de ciberseguridad

La evidencia analizada demuestra que el factor humano no debe interpretarse únicamente como una debilidad o como el denominado “eslabón más débil” de la seguridad. Las decisiones de los usuarios se producen dentro de entornos organizacionales que pueden facilitar o dificultar los comportamientos seguros. Políticas ambiguas, procedimientos complejos, presión por cumplir metas, cargas excesivas de trabajo y tecnologías poco intuitivas pueden inducir prácticas inseguras incluso entre personas que poseen conocimientos sobre ciberseguridad. Por ello, atribuir los incidentes exclusivamente al error individual simplifica un fenómeno que también depende del diseño de procesos, la comunicación institucional y las prioridades establecidas por la dirección. Una estrategia integral debe considerar a los trabajadores como participantes activos capaces de identificar amenazas, reportar situaciones anómalas y contribuir a la protección colectiva (Khando et al., 2021; Sutton & Tompson, 2025).

La cultura de ciberseguridad comprende valores, conocimientos, percepciones, normas y comportamientos compartidos que influyen en la manera en que los miembros de una organización protegen la información. Su relevancia radica en que las políticas formales no necesariamente se traducen en prácticas cotidianas. Una institución puede disponer de procedimientos técnicamente adecuados y, al mismo tiempo, mantener una cultura que normalice el intercambio de contraseñas, la omisión de actualizaciones o el uso de mecanismos informales para transferir información. Por consiguiente, la fortaleza cultural depende de la correspondencia entre las expectativas declaradas, las decisiones directivas, los recursos disponibles y las conductas observadas. La evidencia señala que una cultura sólida favorece comportamientos conscientes, cumplimiento razonado de las políticas y mayor compromiso con la protección institucional (da Veiga et al., 2020; Uchendu et al., 2021).

El compromiso de la alta dirección constituye uno de los factores más influyentes en la consolidación de una cultura preventiva. Cuando los responsables institucionales participan activamente, asignan recursos, comunican prioridades y cumplen las mismas normas exigidas al personal, la seguridad adquiere legitimidad organizacional. Por el contrario, cuando se considera una responsabilidad exclusiva del área tecnológica, los usuarios pueden percibir las medidas como restricciones ajenas a sus funciones. El liderazgo debe traducirse en decisiones visibles, objetivos verificables y responsabilidades distribuidas entre unidades administrativas, técnicas y operativas. La revisión de Sutton y Tompson determinó que la participación directiva, el

modelamiento de conductas, la educación, la supervisión y el respaldo organizacional son dimensiones centrales para vincular cultura y comportamiento (Sutton & Tompson, 2025).

La literatura también destaca la utilidad de establecer redes internas de promotores o referentes de ciberseguridad. Estos actores pueden facilitar la comunicación entre los equipos técnicos y las diferentes áreas, adaptar los mensajes a las necesidades operativas y fortalecer la confianza para reportar dudas o incidentes. Alshaikh identificó iniciativas organizacionales orientadas a reconocer comportamientos prioritarios, crear redes de promotores, desarrollar una identidad comunicativa para los equipos de seguridad y vincular las campañas con actividades institucionales. Tales medidas contribuyen a superar el cumplimiento mínimo porque convierten la seguridad en una práctica social compartida y no únicamente en una obligación normativa. Sin embargo, estas iniciativas requieren continuidad y respaldo, puesto que las campañas aisladas difícilmente modifican hábitos consolidados (Alshaikh, 2020).

La capacitación constituye una herramienta indispensable, aunque su efectividad depende del diseño, la frecuencia, el contenido y la relación con las tareas reales de los participantes. Los programas basados exclusivamente en exposiciones generales pueden incrementar el conocimiento sin modificar necesariamente las decisiones cotidianas. En contraste, los ejercicios interactivos, las simulaciones, los escenarios contextualizados y las actividades basadas en problemas permiten practicar respuestas frente a situaciones semejantes a las que podrían presentarse en el entorno laboral. La revisión sistemática de Prümmer et al. analizó 142 investigaciones y encontró una tendencia general hacia resultados positivos; no obstante, también identificó muestras pequeñas, diseños no experimentales y evaluaciones realizadas en poblaciones distintas de los trabajadores, lo que limita la generalización de algunas conclusiones (Prümmer et al., 2024).

La evidencia reciente permite profundizar esta discusión al diferenciar entre cambios cognitivos y transformaciones conductuales. El metaanálisis desarrollado por Prümmer et al. identificó un efecto global positivo de las intervenciones formativas; sin embargo, los resultados fueron mayores en conocimientos, actitudes y otros antecedentes del comportamiento que en las conductas observadas. Esta diferencia resulta fundamental porque demuestra que conocer una práctica segura no garantiza su aplicación bajo condiciones reales de presión, urgencia o complejidad. Por tanto, los programas deberían combinar capacitación con modificaciones en el diseño de procesos, recordatorios contextuales, mecanismos de retroalimentación y reducción de obstáculos operativos. La efectividad debe medirse por la capacidad de mejorar decisiones y no únicamente por la asistencia o la aprobación de evaluaciones teóricas (Prümmer et al., 2025).

Las simulaciones de *phishing* pueden aportar información sobre la exposición organizacional y permitir intervenciones formativas inmediatas, pero deben utilizarse con criterios éticos y pedagógicos. Una estrategia basada exclusivamente en

sancionar a quienes interactúan con mensajes simulados puede producir temor, ocultamiento de errores o desconfianza hacia los equipos de seguridad. Por el contrario, el propósito debería ser identificar patrones, reconocer áreas que requieren apoyo y fortalecer la capacidad colectiva para detectar intentos de manipulación. Las métricas deben considerar no solo la interacción con mensajes fraudulentos, sino también la rapidez del reporte, la identificación de señales de riesgo y la disminución sostenida de comportamientos vulnerables. De esta manera, la evaluación contribuye al aprendizaje institucional en lugar de convertirse en un mecanismo punitivo (Khando et al., 2021; Sutton & Tompson, 2025).

La medición de la cultura de ciberseguridad requiere utilizar indicadores múltiples. Los cuestionarios de percepción permiten conocer actitudes, conocimientos y opiniones, aunque pueden verse afectados por respuestas socialmente deseables. Por ello, deberían complementarse con observaciones conductuales, resultados de ejercicios, niveles de participación, calidad de los reportes, cumplimiento de procedimientos y análisis de incidentes. La evaluación multidimensional facilita la identificación de diferencias entre áreas, funciones y niveles jerárquicos, evitando asumir que toda la organización comparte las mismas prácticas. Además, los resultados deben emplearse para orientar mejoras y no para responsabilizar indiscriminadamente a los trabajadores, debido a que la cultura representa una propiedad colectiva influida por liderazgo, políticas, tecnología y condiciones laborales (da Veiga et al., 2020; Sutton & Tompson, 2025).

3.1.4. Gestión organizacional, respuesta y resiliencia ante incidentes

La gestión organizacional constituye el mecanismo encargado de integrar recursos tecnológicos, capacidades humanas y objetivos institucionales dentro de una estrategia coherente. La incorporación de la función de gobierno en el Marco de Ciberseguridad 2.0 refuerza la necesidad de relacionar el riesgo cibernético con las decisiones empresariales, la continuidad operativa y las responsabilidades directivas. Esta aproximación implica definir estructuras de autoridad, criterios de priorización, niveles aceptables de riesgo, mecanismos de supervisión e indicadores de desempeño. La seguridad informática deja así de ser una responsabilidad exclusiva de los departamentos técnicos y se convierte en un componente transversal que requiere participación de la dirección, áreas jurídicas, recursos humanos, gestión de riesgos, operaciones y proveedores estratégicos (Pascoe et al., 2024).

Una gobernanza efectiva debe establecer responsabilidades antes de que ocurra un incidente. Las organizaciones necesitan determinar quién autoriza medidas de contención, quién coordina la investigación, quién comunica información a las partes interesadas y quién decide las prioridades de recuperación. La ausencia de estas definiciones puede generar respuestas tardías, decisiones contradictorias y pérdida de evidencia relevante. Asimismo, la asignación de responsabilidades debe acompañarse de recursos, competencias y mecanismos de rendición de cuentas, debido a que una política sin capacidades operativas puede convertirse en una

declaración formal sin aplicación efectiva. La gestión del riesgo requiere que las decisiones se revisen periódicamente conforme cambian las amenazas, las tecnologías y los procesos institucionales (Pascoe et al., 2024; Nelson et al., 2025).

La gestión de terceros constituye una dimensión cada vez más relevante, puesto que las organizaciones dependen de proveedores de software, servicios en la nube, plataformas de comunicación, operadores tecnológicos y contratistas. Una vulnerabilidad o interrupción en estos actores puede afectar indirectamente a múltiples entidades, incluso cuando sus controles internos funcionan adecuadamente. Por esta razón, la selección y supervisión de proveedores debería considerar requisitos de seguridad, mecanismos de notificación, responsabilidades contractuales, niveles de servicio y procedimientos de recuperación. El riesgo asociado con terceros no desaparece mediante la contratación externa, debido a que las consecuencias operativas, jurídicas y reputacionales pueden continuar recayendo sobre la organización que utiliza el servicio (Pascoe et al., 2024; ENISA, 2025).

La respuesta a incidentes debe concebirse como una capacidad permanente integrada en la gestión general del riesgo. La actualización de la guía NIST SP 800-61 plantea que las actividades de respuesta no comienzan únicamente después de detectar un ataque, sino que dependen de la preparación previa, la identificación de activos, la implementación de controles y el desarrollo de capacidades de recuperación. Esta visión permite reducir tanto la probabilidad como el impacto de los eventos y mejorar la eficiencia de la detección, contención y restauración. En consecuencia, los planes deben ser conocidos por los responsables, encontrarse alineados con los procesos institucionales y contemplar diferentes escenarios, en lugar de consistir en documentos genéricos que se consultan únicamente durante una crisis (Nelson et al., 2025).

Durante un incidente, la organización debe disponer de procedimientos para analizar señales, determinar el alcance, contener la propagación, eliminar mecanismos de persistencia y restablecer las funciones afectadas. Sin embargo, la velocidad no debe sustituir la rigurosidad, ya que decisiones apresuradas pueden destruir evidencia, interrumpir procesos innecesariamente o permitir que el adversario mantenga accesos ocultos. La coordinación entre equipos técnicos, directivos y jurídicos resulta indispensable para equilibrar continuidad operativa, preservación de evidencia, obligaciones institucionales y comunicación. Asimismo, la respuesta debe considerar la posibilidad de que los medios habituales de comunicación se encuentren comprometidos, por lo que resulta conveniente disponer de canales alternativos previamente definidos (Nelson et al., 2025).

Los ejercicios y simulaciones constituyen instrumentos esenciales para validar la capacidad de respuesta. Los ejercicios de mesa permiten analizar escenarios hipotéticos, revisar responsabilidades y detectar contradicciones en los procedimientos, mientras que las simulaciones técnicas evalúan la capacidad para identificar, contener y recuperar sistemas bajo condiciones controladas. Estas

actividades revelan problemas que pueden permanecer ocultos durante la revisión documental, como información de contacto desactualizada, ausencia de permisos, dependencia excesiva de una persona o dificultades de coordinación. Por tanto, la preparación debe evaluarse mediante la ejecución y no únicamente por la existencia de planes escritos. Los resultados de cada ejercicio deben traducirse en acciones correctivas verificables y asignarse a responsables concretos (Nelson et al., 2025; Ross et al., 2021).

La resiliencia cibernética amplía el enfoque preventivo al reconocer que ciertos ataques pueden superar las barreras establecidas. Una organización resiliente no es aquella que nunca experimenta incidentes, sino la que mantiene o recupera sus funciones esenciales bajo condiciones adversas. Para ello, necesita identificar procesos críticos, establecer prioridades, reducir puntos únicos de fallo, disponer de alternativas operativas y desarrollar capacidades de adaptación. La resiliencia debe incorporarse desde el diseño y durante todo el ciclo de vida de los sistemas, debido a que resulta más difícil y costoso introducirla después de que las infraestructuras se encuentran consolidadas. NIST plantea que los sistemas ciberresilientes deben ser capaces de anticipar, resistir, recuperarse y adaptarse frente a compromisos y condiciones adversas (Ross et al., 2021).

La recuperación debe contemplar dimensiones técnicas, operativas y comunicacionales. Restaurar servidores o aplicaciones no significa necesariamente que la organización haya recuperado su capacidad de prestar servicios, puesto que también pueden existir procesos manuales interrumpidos, información pendiente de validación, obligaciones regulatorias y pérdida de confianza entre usuarios o clientes. Por ello, la recuperación requiere verificar la integridad de los sistemas, restablecer servicios según su prioridad, comunicar información coherente y supervisar posibles indicadores de persistencia. La coordinación con la continuidad del negocio permite evitar que la recuperación tecnológica se desarrolle de forma aislada respecto de las necesidades institucionales (Nelson et al., 2025; Ross et al., 2021).

Finalmente, la mejora continua transforma los incidentes y ejercicios en oportunidades de aprendizaje. Las revisiones posteriores deben analizar causas técnicas, decisiones humanas, fallos de coordinación y condiciones organizacionales que facilitaron el evento. El propósito no consiste únicamente en identificar responsables, sino en comprender por qué las barreras existentes no evitaron o limitaron el incidente. Los resultados deben traducirse en ajustes de políticas, controles, arquitecturas, procedimientos y programas formativos, acompañados por indicadores que permitan verificar su implementación. Esta capacidad de aprender diferencia una respuesta temporal de una estrategia de resiliencia sostenible, debido a que favorece la adaptación frente a amenazas que cambian con mayor rapidez que los ciclos tradicionales de planificación institucional (Nelson et al., 2025; Sutton & Tompson, 2025).

Los resultados de la revisión evidencian que la prevención de ataques cibernéticos requiere una arquitectura sociotécnica en la que las medidas tecnológicas, la cultura institucional, la gobernanza y la resiliencia funcionen de manera complementaria. La protección basada únicamente en herramientas deja sin atender factores humanos y organizacionales, mientras que la capacitación sin controles técnicos mantiene abiertas rutas de explotación. De igual modo, la respuesta carece de efectividad cuando no existe preparación previa, y la recuperación resulta limitada cuando no se encuentra vinculada con la continuidad de los procesos esenciales. En consecuencia, la madurez en ciberseguridad depende de la capacidad para integrar prevención, detección, respuesta, aprendizaje y adaptación dentro de un ciclo permanente de gestión del riesgo (Pascoe et al., 2024; Ross et al., 2021; Sutton & Tompson, 2025).

4. Discusión

Realiza Los hallazgos derivados de la revisión permiten sostener que la seguridad informática constituye un fenómeno organizacional de naturaleza sociotécnica y no una problemática exclusivamente asociada con la infraestructura tecnológica. La convergencia entre amenazas externas, vulnerabilidades internas, prácticas laborales, decisiones administrativas y dependencias digitales demuestra que la prevención requiere una arquitectura integral capaz de coordinar gobierno, identificación de riesgos, protección, detección, respuesta y recuperación. Esta interpretación coincide con el Marco de Ciberseguridad 2.0, cuya estructura desplaza la atención desde la implementación aislada de controles hacia la gestión continua del riesgo y la articulación de la ciberseguridad con los objetivos institucionales. En consecuencia, la madurez organizacional no debería valorarse únicamente por la cantidad o sofisticación de las herramientas adquiridas, sino por la capacidad para integrarlas dentro de procesos verificables, responsabilidades definidas y mecanismos permanentes de adaptación (Pascoe et al., 2024; Ross et al., 2021).

La evidencia examinada también permite cuestionar la presunción de que las organizaciones de mayor tamaño se encuentran necesariamente mejor protegidas por disponer de más recursos económicos y tecnológicos. El estudio de Connolly et al. (2020), basado en 55 ataques registrados en 50 organizaciones, no encontró diferencias significativas en la severidad del ransomware asociadas exclusivamente con el tamaño institucional; en cambio, las entidades con posturas de seguridad débiles experimentaron consecuencias considerablemente más graves. Este resultado sugiere que la disponibilidad de recursos no produce protección de forma automática, debido a que su efectividad depende de la calidad de la gobernanza, la coherencia de las políticas, la actualización tecnológica y la preparación operativa. Asimismo, implica que las organizaciones pequeñas no deberían asumir que la ciberseguridad avanzada es inaccesible, puesto que medidas priorizadas —como control de accesos, respaldo probado, actualización y respuesta planificada— pueden

reducir sustancialmente la exposición aun cuando existan restricciones presupuestarias (Connolly et al., 2020; Pascoe et al., 2024).

Respecto de las medidas tecnológicas, los resultados respaldan la defensa en profundidad como una estrategia más consistente que la dependencia de un único mecanismo preventivo. La autenticación multifactor puede disminuir el riesgo derivado del robo de contraseñas, pero pierde eficacia cuando existen permisos excesivos, configuraciones inseguras o sistemas sin supervisión. De igual manera, la actualización reduce oportunidades de explotación, aunque no impide ataques basados en manipulación humana, abuso de credenciales válidas o vulnerabilidades aún desconocidas. Por consiguiente, los controles deben operar de manera complementaria y responder a una lógica de reducción progresiva del riesgo: identificar los activos, disminuir la superficie de exposición, limitar privilegios, dificultar el desplazamiento lateral, detectar anomalías y preservar capacidades de recuperación. Esta interpretación coincide con la orientación del Marco de Ciberseguridad 2.0, que no prescribe una tecnología específica, sino resultados de seguridad adaptables al tamaño, sector, nivel de madurez y contexto de cada organización (Pascoe et al., 2024).

No obstante, la incorporación de tecnologías avanzadas puede generar una percepción engañosa de protección cuando no se encuentra acompañada por capacidades de administración, monitoreo y evaluación. Las herramientas de detección, correlación de eventos o análisis automatizado producen grandes volúmenes de información cuya utilidad depende de la calidad de los registros, la pertinencia de las reglas y la disponibilidad de personal capaz de interpretar las alertas. Por ello, una infraestructura tecnológicamente sofisticada puede conservar vulnerabilidades significativas si los activos no están identificados, los controles permanecen mal configurados o las alertas no reciben tratamiento oportuno. Desde esta perspectiva, la eficacia de las medidas tecnológicas no reside únicamente en sus prestaciones técnicas, sino en la forma en que se incorporan a los procesos institucionales. La selección de controles debería basarse en riesgos concretos y resultados esperados, evitando la adquisición fragmentaria de soluciones que incrementen la complejidad operativa sin fortalecer proporcionalmente la protección (Pascoe et al., 2024; Ross et al., 2021).

En cuanto al factor humano, la revisión cuestiona la representación del trabajador como un elemento inherentemente débil dentro de la seguridad organizacional. Aunque las decisiones individuales pueden facilitar incidentes, dichas conductas se producen en entornos configurados por políticas, tecnologías, cargas laborales, incentivos y prácticas institucionales. Considerar al usuario como único responsable puede ocultar deficiencias estructurales, tales como procedimientos excesivamente complejos, ausencia de orientación, limitada participación directiva o mecanismos de reporte poco accesibles. Por ello, el personal debería comprenderse como una capacidad activa de prevención y detección, capaz de reconocer señales de riesgo, reportar anomalías y contribuir a la protección colectiva. Esta perspectiva requiere

sustituir el enfoque culpabilizador por modelos centrados en el aprendizaje, la corresponsabilidad y el diseño de condiciones que faciliten comportamientos seguros durante las actividades laborales ordinarias (Khando et al., 2021; Sutton & Tompson, 2025).

La formación en ciberseguridad representa un componente indispensable, aunque los resultados indican que el incremento del conocimiento no equivale necesariamente a una modificación sostenida del comportamiento. La revisión sistemática de Prümmer et al. (2024) identificó efectos favorables en numerosos programas, pero también reveló limitaciones relacionadas con muestras pequeñas, diseños no experimentales y evaluaciones realizadas fuera de contextos laborales. Posteriormente, el metaanálisis de Prümmer et al. (2025) encontró efectos más intensos sobre conocimientos, actitudes y antecedentes conductuales que sobre las conductas observadas. Esta diferencia resulta relevante porque demuestra que una persona puede reconocer conceptualmente una amenaza y, aun así, actuar de manera insegura frente a situaciones de urgencia, presión o ambigüedad. En consecuencia, las organizaciones deberían complementar la capacitación con simulaciones contextualizadas, retroalimentación oportuna, simplificación de procedimientos y controles técnicos que reduzcan la dependencia exclusiva de la decisión humana (Prümmer et al., 2024, 2025).

La gestión organizacional constituye el componente integrador de las dimensiones técnicas y humanas identificadas. La incorporación explícita de la función de gobierno en el Marco de Ciberseguridad 2.0 confirma que la gestión del riesgo cibernético debe vincularse con la misión, los objetivos operativos y las decisiones estratégicas. Esta orientación implica establecer responsabilidades, prioridades, niveles aceptables de riesgo, mecanismos de supervisión y criterios para distribuir recursos. La ciberseguridad deja así de ser un asunto exclusivo de los departamentos tecnológicos y se convierte en una responsabilidad compartida entre dirección, operaciones, gestión de riesgos, recursos humanos, áreas jurídicas y proveedores. Esta transversalidad es necesaria porque las decisiones adoptadas fuera del ámbito tecnológico —contratación de servicios, adquisición de plataformas, gestión del personal o continuidad operativa— pueden modificar significativamente la exposición institucional. Por consiguiente, una gobernanza eficaz debe asegurar coherencia entre decisiones estratégicas, controles técnicos y prácticas cotidianas (Pascoe et al., 2024; Uchendu et al., 2021).

La respuesta a incidentes debe interpretarse, además, como una capacidad integrada al ciclo de gestión del riesgo y no como una actividad improvisada después de que se materializa una intrusión. La actualización de la guía NIST SP 800-61 vincula la respuesta con las actividades previas de gobierno, identificación y protección, de manera que la preparación contribuya tanto a disminuir la probabilidad de incidentes como a reducir sus consecuencias. Esta integración exige procedimientos de detección, análisis, contención, recuperación y comunicación, acompañados por funciones previamente asignadas y mecanismos de coordinación. La existencia de un

plan, por sí sola, no garantiza capacidad operativa; su efectividad depende de que sea conocido, actualizado y sometido a ejercicios periódicos. Por ello, las simulaciones y ejercicios de mesa resultan relevantes para identificar dependencias, inconsistencias y vacíos antes de una crisis real, especialmente cuando los canales habituales de comunicación o los sistemas institucionales pueden encontrarse comprometidos (Nelson et al., 2025).

En términos integradores, la evidencia permite proponer que la efectividad preventiva depende de la interacción entre cuatro capacidades: reducción de vulnerabilidades, protección tecnológica estratificada, cultura organizacional y preparación para responder y recuperarse. Ninguna de estas dimensiones resulta suficiente de manera independiente. Los controles técnicos pueden ser eludidos cuando existen prácticas inseguras; la capacitación pierde alcance cuando los sistemas mantienen configuraciones vulnerables; la respuesta resulta tardía cuando las responsabilidades no están definidas; y los respaldos son insuficientes cuando no se prueban o no se relacionan con prioridades operativas. Por tanto, la principal contribución conceptual de la revisión consiste en mostrar que la seguridad informática debe gestionarse como un sistema de capacidades interdependientes y no como una colección fragmentada de soluciones. Esta interpretación se corresponde con los enfoques contemporáneos que articulan riesgo, comportamiento, gobernanza y resiliencia dentro de una estructura institucional común (Pascoe et al., 2024; Sutton & Tompson, 2025; Ross et al., 2021).

Desde una perspectiva práctica, los resultados sugieren que las organizaciones deberían priorizar acciones de acuerdo con la criticidad de sus procesos y no mediante la adopción indiscriminada de tecnologías. La identificación de activos, la gestión oportuna de vulnerabilidades, el control de privilegios, la segmentación, la autenticación reforzada, la supervisión continua y las pruebas de recuperación conforman una base técnica que debe complementarse con liderazgo, formación contextualizada y procedimientos de respuesta. Esta priorización facilita el uso racional de recursos y permite establecer indicadores verificables de avance. Asimismo, evita que la ciberseguridad se convierta en una sucesión de proyectos independientes sin continuidad institucional. La adopción de perfiles de situación actual y deseada, acompañados por evaluaciones periódicas, puede contribuir a identificar brechas y orientar inversiones según riesgos específicos, manteniendo la flexibilidad necesaria para adaptarse a diferentes tamaños, sectores y niveles de madurez organizacional (Pascoe et al., 2024; Nelson et al., 2025).

No obstante, los resultados deben interpretarse considerando las limitaciones inherentes al carácter exploratorio y bibliográfico del estudio. La heterogeneidad de las fuentes, los contextos organizacionales, las metodologías y los indicadores dificulta establecer comparaciones directas o determinar la superioridad universal de una medida preventiva. Además, la rápida evolución de las amenazas puede reducir la vigencia de ciertos hallazgos técnicos, mientras que la predominancia de estudios basados en autoinformes limita la evaluación del comportamiento real. Al no

corresponder a un metaanálisis ni a una revisión sistemática con estimaciones agregadas, la presente investigación no permite establecer relaciones causales ni cuantificar la efectividad comparativa de los controles. Sin embargo, la revisión bibliográfica conserva valor para integrar conocimientos fragmentados, reconocer convergencias conceptuales, identificar contradicciones y formular una interpretación articulada del fenómeno, siempre que sus procedimientos y alcances se presenten con transparencia (Snyder, 2019; Prümmer et al., 2024).

Las investigaciones futuras deberían avanzar hacia diseños longitudinales y evaluaciones desarrolladas en entornos organizacionales reales, con indicadores que integren resultados técnicos, conductuales y operativos. Resulta necesario determinar qué combinaciones de controles producen mejoras sostenibles según el sector, tamaño, madurez y nivel de exposición de las organizaciones, así como examinar la relación entre liderazgo, cultura, comportamiento y resiliencia. También conviene ampliar el análisis de las cadenas de suministro digital, los servicios en la nube y las dependencias de terceros, debido a que la seguridad institucional se encuentra cada vez más condicionada por infraestructuras externas. En este sentido, la originalidad de la revisión radica en articular amenazas, vulnerabilidades, medidas tecnológicas, cultura y gestión de incidentes dentro de una comprensión común: la prevención efectiva no consiste en eliminar toda posibilidad de ataque, sino en reducir la exposición, limitar las consecuencias y fortalecer la capacidad organizacional para aprender y adaptarse continuamente (ENISA, 2025; Sutton & Tompson, 2025; Ross et al., 2021).

5. Conclusiones

La revisión permitió determinar que la seguridad informática debe asumirse como una responsabilidad estratégica y transversal, debido a que la prevención de ataques cibernéticos no depende únicamente de la incorporación de herramientas tecnológicas, sino de la articulación entre gobierno institucional, gestión del riesgo, protección de activos, vigilancia continua, respuesta planificada y recuperación operativa. En este sentido, la eficacia de las estrategias preventivas se fortalece cuando la ciberseguridad se integra en los procesos de toma de decisiones y se vincula con la continuidad de las funciones críticas de la organización.

Asimismo, se concluye que las principales amenazas cibernéticas aprovechan la convergencia entre vulnerabilidades técnicas, deficiencias administrativas y comportamientos humanos susceptibles de manipulación. El *phishing*, el ransomware, el compromiso de credenciales, la explotación de vulnerabilidades y el acceso no autorizado adquieren mayor capacidad de afectación cuando existen sistemas desactualizados, configuraciones inseguras, privilegios excesivos, redes insuficientemente segmentadas y mecanismos de respaldo deficientes. Por consiguiente, la severidad de los incidentes no depende únicamente del tipo de

ataque, sino también del nivel de preparación y madurez preventiva de cada organización.

De igual manera, la evidencia analizada confirma que las medidas tecnológicas alcanzan mayor efectividad cuando se implementan mediante un enfoque de defensa en profundidad. La identificación y clasificación de activos, la gestión continua de vulnerabilidades, la autenticación multifactor, el principio de privilegio mínimo, la segmentación de redes, el monitoreo permanente, el cifrado y las copias de seguridad verificadas constituyen controles complementarios que reducen la probabilidad de intrusión y limitan la propagación de los ataques. No obstante, ninguna medida garantiza protección absoluta de forma aislada, por lo que su implementación debe responder a una evaluación contextualizada de riesgos y prioridades organizacionales.

Por otra parte, el factor humano representa una capacidad esencial para la prevención y no únicamente una fuente potencial de vulnerabilidad. La consolidación de una cultura de ciberseguridad requiere liderazgo visible, políticas comprensibles, formación continua, comunicación interna y participación activa del personal. Las actividades de capacitación deben superar el cumplimiento formal y orientarse al desarrollo de competencias aplicables en situaciones reales, mediante ejercicios contextualizados, simulaciones y mecanismos de retroalimentación. En consecuencia, el fortalecimiento de los conocimientos debe acompañarse de condiciones organizacionales que faciliten conductas seguras y promuevan el reporte oportuno de incidentes sin recurrir a enfoques exclusivamente punitivos.

Finalmente, la gestión de incidentes y la resiliencia deben considerarse componentes inseparables de la prevención. Las organizaciones necesitan disponer de responsabilidades claramente definidas, procedimientos de detección, mecanismos de contención, estrategias de comunicación, planes de recuperación y ejercicios periódicos que permitan validar su capacidad operativa. La protección efectiva no consiste únicamente en impedir ataques, sino también en mantener las funciones esenciales, reducir las consecuencias de los eventos adversos y transformar cada incidente en una oportunidad de aprendizaje y mejora. En conjunto, la revisión demuestra que una estrategia sostenible de ciberseguridad surge de la integración equilibrada entre tecnología, personas, procesos, liderazgo y capacidad institucional de adaptación.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

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

Andrade-Díaz, K. V. (2024). Integración de tecnologías de realidad aumentada en campañas publicitarias interactivas. *Revista Científica Ciencia Y Método, 2*(4), 26-37. https://doi.org/10.55813/gaea/rcym/v2/n4/51

Carpio-Velasco, F. J., & Garcés-Beltrán, G. M. (2025). Comparación de Estrategias de Control de Temperatura: Controlador PID y Redes Neuronales. *Revista Científica Zambos, 4*(2), 185-196. https://doi.org/10.69484/rcz/v4/n2/113

Casanova-Villalba, C. I., & Casanova-Villalba, L. A. (2024). Uso de análisis de datos avanzados para la detección de fraudes financieros. *Revista Científica Ciencia y Método, 2*(3), 1–12. https://doi.org/10.55813/gaea/rcym/v2/n3/44

Castelo-Vinueza, E. M. (2025). Problemas de la investigación tecnológica y su aplicación en la generación de innovación. *Journal of Economic and Social Science Research*, *5*(1), 146–160. https://doi.org/10.55813/gaea/jessr/v5/n1/166

Celi-Párraga, R. J., Boné-Andrade, M. F., Mora-Olivero, A. P., & Sarmiento-Saavedra, J. C. (2023a). *Ingeniería del software I: Requerimientos y modelado del software*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.21

Celi-Párraga, R. J., Mora-Olivero, A. P., Boné-Andrade, M. F., & Sarmiento-Saavedra, J. C. (2023b). *Ingeniería del software II: Implementación, pruebas y mantenimiento*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.20

Chávez-Rendón, S. D., Pillasagua-Yépez, T. M., Moreira-Noboa, S. M., & Zamora-Mayorga, D. J. (2025). Análisis del funcionamiento tecnológico del ECU 911 de Quevedo en la gestión pública de la seguridad ciudadana. *Revista Científica Ciencia Y Método, 3*(3), 181-193. https://doi.org/10.55813/gaea/rcym/v3/n3/71

Choez-Calderón, C. J. (2024). Realidad aumentada y su aplicación en la educación a distancia. *Revista Científica Ciencia Y Método, 2*(3), 26-38. https://doi.org/10.55813/gaea/rcym/v2/n3/46

Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity, 6*(1), tyaa023. https://doi.org/10.1093/cybsec/tyaa023

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro

Vicente Maldonado. *Journal of Economic and Social Science Research*, *2*(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

García-Peña, V. R. (2023). Desarrollo y Uso de Aplicaciones Móviles en el Contexto Ecuatoriano. *Revista Científica Zambos*, *2*(3), 1-15. https://doi.org/10.69484/rcz/v2/n3/46

Giraldo-Burgos, G. Y., Avilés-Tinitana, V. V., Palacios-Rodríguez, A. M., & Zamora-Mayorga, D. J. (2024). Desafíos de adopción frente a plataformas digitales externas en la biblioteca de la Universidad Técnica Estatal de Quevedo. *Revista Científica Ciencia Y Método,* *3*(3), 194-212. https://doi.org/10.55813/gaea/rcym/v3/n3/67

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security, 106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Mina-Bone, S. G. (2024). Evolución del derecho penal económico frente a los delitos financieros digitales. *Revista Científica Ciencia y Método, 2*(3), 52–66. https://doi.org/10.55813/gaea/rcym/v2/n3/50

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61, Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H., & Omonte-Vilca, A. (2023). *Fortalecimiento metodológico de la seguridad informática en posgrados: Análisis y estrategias de mejora*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.56

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security, 150*, 104206. https://doi.org/10.1016/j.cose.2024.104206

Ramos-Secaira, F. M. (2023). Seguridad Cibernética en Empresas Ecuatorianas: Prácticas y Retos Actuales. *Revista Científica Zambos*, *2*(3), 16-28. https://doi.org/10.69484/rcz/v2/n3/47

Robalino-Latorre, M. C., Ramirez-Klinger, W. N., Guadalupe-Copa, R. C., & Cuello-García, S. A. (2023). Aplicación del Método Montecarlo en flujo de potencias a

través del Software Octave. *Journal of Economic and Social Science Research*, *3*(1), 31–47. https://doi.org/10.55813/gaea/jessr/v3/n1/60

Rodriguez-Vizuete, J. D., Viteri-Ojeda, J. C., & Villa-Feijoó, A. L. (2024). Adopción de tecnologías sostenibles en infraestructuras de tecnologías de la información. *Revista Científica Ciencia Y Método, 2*(1), 55-67. https://doi.org/10.55813/gaea/rcym/v2/n1/3

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273

Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. *Journal of Economic and Social Science Research*, *4*(3), 1–12. https://doi.org/10.55813/gaea/jessr/v4/n3/117

Sangacha-Tapia, L., González-Cañizalez, Y., & Rivas-Herrera, J. (2025). Optimización de Criterios de Búsqueda avanzada para Nuevas Tendencias en la Académica mediante Machine Learning. *Revista Científica Zambos, 4*(2), 197-211. https://doi.org/10.69484/rcz/v4/n2/114

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Solano-Gutiérrez, G. A. (2024). La Tecnología en la Educación a Distancia: Revisión de Progresos y Obstáculos a Superar. *Revista Científica Zambos, 3*(2), 48-73. https://doi.org/10.69484/rcz/v3/n2/17

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, 148*, 104110. https://doi.org/10.1016/j.cose.2024.104110

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269