Resiliencia en Ciberseguridad: Evaluación del Conocimiento Operativo en Especia-listas de Infraestructuras Críticas de Red

Cybersecurity Resilience: Evaluating Operational Knowledge in Critical Network Infrastructure Specialists

Vílchez Oscar
Código ORCID: 0009-0003-3928-7846
Correo: oscarevilchez@gmail.com
Inversiones Primo C.A. Maracaibo, Venezuela.

Andrés Amaya
Código ORCID: 0009-0000-0768-9961
Universidad Privada Dr. Rafael Belloso Chacín. Venezuela
Correo: aamaya@urbe.edu.ve
Maracaibo, Venezuela

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Resumen

El objetivo fundamental de la investigación fue evaluar la resiliencia en ciberseguridad a través del nivel de conocimiento técnico en especialistas de infraestructuras críticas de red. La investigación se fundamentó teóricamente en los postulados internacionales de la norma ISO/IEC 27001, el framework del National Institute of Standards and Technology (NIST, 2024) y las contribuciones académicas de Malik (2021). Metodológicamente el trabajo se tipificó como una investigación descriptiva, con un diseño de campo, no experimental y transeccional. La población objeto de estudio estuvo conformada por setenta y cuatro (74) especialistas de tecnología pertenecientes a organizaciones de sectores estratégicos. Para la recolección de los datos se empleó un instrumento enfocado en la dimensión de conocimiento técnico, evaluando la identificación de amenazas, fundamentos de protección, marcos de seguridad y firewalls, el cual fue validado por expertos y presentó una confiabilidad de 0,895 según el coeficiente Alfa de Cronbach. Los resultados indica-ron un dominio operativo satisfactorio en la configuración de firewalls y protocolos de protección; no obstante, se detectaron brechas críticas en la identificación proactiva de vectores de ataque complejos, evidenciando una desalineación con la nueva función de Gobernanza del framework NIST (2024). A partir de estos hallazgos, se diseña una Ruta Crítica de Alineación Predictiva (RCAP) como propuesta innovadora para la gestión del talento humano, transformando el diagnóstico en un modelo de respuesta estratégica para la protección de activos esenciales.

Palabras clave: Resiliencia, Ciberseguridad, Infraestructuras críticas, Gestión del conocimiento, Seguridad de los datos.

Abstract

The fundamental purpose of this research was to evaluate cybersecurity resilience through the level of technical knowledge in critical network infrastructure specialists. The study was theoretically grounded on the international tenets of the ISO/IEC 27001 standard, the National Institute of Standards and Technology framework (NIST, 2024), and the academic contributions of Malik (2021). Methodologically, the work was typified as descriptive research with a field, non-experimental, and cross-sectional design. The population under study consisted of seventy-four (74) technology specialists belonging to organizations in strategic sectors. For data collection, an instrument focused on the tech-nical knowledge dimension was used, evaluating threat identification, protection funda-mentals, security frameworks, and firewalls; it was validated by experts and demonstra-ted a reliability of 0.895 according to Cronbach's

alpha coefficient. The results indicated a satisfactory operational domain in firewall configuration and protection protocols; however, critical gaps were detected in the proactive identification of complex attack vec-tors, evidencing a misalignment with the new Governance function of the NIST frame-work (2024). Based on these findings, a Critical Path of Predictive Alignment (CPPA) is designed as an innovative proposal for human talent management, transforming the diagnosis into a strategic response model for the protection of essential assets.

Keywords: Resilience, Cybersecurity, Critical infrastructures, Knowledge management, Data security.

Introducción

En la nueva era de las telecomunicaciones la ciberseguridad ha trascendido su rol estrictamente operativo para posicionarse como el pilar fundamental de la resiliencia en infraestructuras críticas. Las organizaciones encargadas de la gestión de activos estratégicos se enfrentan hoy a un ecosistema de amenazas asimétricas y disruptivas que ponen en riesgo la continuidad de servicios vitales para el Estado. Según Malik (2021), la salva-guarda de estas redes exige una capacidad de respuesta técnica que no solo dependa de la arquitectura de hardware, sino que integre el nivel de conocimiento especializado como el componente más crítico de la defensa activa. No obstante, se observa una diferencia persistente entre la sofisticación de los ataques y el dominio técnico proactivo de quienes custodian estas plataformas.

El National Institute of Standards and Technology (NIST, 2024) plantea un paradigma basado en la resiliencia operativa permitiendo a las instituciones no solo disminuir ataques, sino desarrollar capacidades de identificación y protección ante incidentes de alta complejidad. La efectividad de estos marcos de trabajo está supeditada a la competencia técnica de los especialistas en áreas clave como la identificación de amenazas, los principios de protección y el manejo de firewalls. Para el contexto de los sectores estratégicos, esta capacidad técnica es obligatoria y destinada a reducir las vulnerabilidades estructurales que surgen ante el desconocimiento de protocolos avanzados de defensa, reforzando la seguridad de cualquier institución.

La presente investigación surge ante la necesidad de diagnosticar la solidez de la primera línea de defensa: el factor humano técnico. Tras un estudio analítico exhaustivo aplicado a setenta y cuatro (74) informantes clave en el área de tecnología, se determinó que, si bien existe un manejo sobresaliente de protocolos operativos básicos, persiste una marcada desalineación con los marcos de seguridad globales y una visión predominante-mente reactiva de la protección. Esta realidad expone a los activos nacionales a riesgos sistémicos que demandan una evaluación específica del conocimiento operativo para fortalecer la resiliencia institucional, justificando la necesidad de diseñar una Ruta Crítica de Alineación Predictiva (RCAP) como respuesta estratégica.

Por lo expuesto, el propósito medular de este artículo es examinar la resiliencia en ciberseguridad a través del nivel de conocimiento técnico en especialistas de infraestructuras críticas de red. El estudio se fundamenta rigurosamente en los estándares de la norma ISO/IEC 27001, el framework NIST (2024) y los lineamientos de Malik (2021). Final-mente, se plantea la siguiente interrogante: ¿Cuál es el nivel de conocimiento técnico sobre identificación de amenazas, fundamentos de protección y marcos de seguridad en los especialistas encargados de la resiliencia de las infraestructuras críticas de red? Con el propósito de dar respuesta a este planteamiento, el artículo se estructura de manera sistemática a través de una fundamentación teórica de las variables, el abordaje metodológico cuantitativo, el análisis y contrastación crítica de los resultados obtenidos y las conclusiones finales que sustentan la propuesta de optimización técnica.

Fundamentación teórica

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

La comprensión de la resiliencia en entornos digitales contemporáneos exige un abordaje paradigmático que trascienda la visión puramente instrumental y se inserte en la evaluación de las capacidades cognitivas del talento humano. La ciberseguridad en las infraestructuras críticas no representa únicamente una barrera tecnológica, sino que se constituye como el pilar fundamental de la resiliencia operativa. De acuerdo con Malik (2021), la protección de activos estratégicos debe articularse mediante un dominio profundo de los protocolos técnicos, permitiendo que las instituciones continúen su operativa y se mantengan ante incidentes disruptivos de gran escala mediante una respuesta informada y proactiva.

Esta capacidad de respuesta se relaciona directamente con el indicador de Identificación de Amenazas. Malik (2021) sostiene que la seguridad no es un estado estático, sino un proceso dinámico de adaptación donde el conocimiento sobre los vectores de ataque actúa como la primera línea de defensa sistémica. Para las organizaciones que gestionan servicios esenciales, la eficacia de esta fase predictiva depende de la habilidad del especialista para reconocer indicadores de compromiso (IoC) y patrones complejos. Al respecto, Ortiz (2020) señala que la detección temprana y el análisis de alertas sobre vectores críticos resultan indispensables para neutralizar vulnerabilidades antes de que afecten la continuidad operativa de los dispositivos interconectados en la red.

Por su parte, el indicador de Fundamentos de Protección exige una alineación simbiótica entre la preparación del talento humano y los mecanismos de defensa en profundidad. La brecha de conocimiento en esta área no solo debilita la respuesta técnica, sino que incrementa la superficie de exposición ante malware emergente y amenazas persistentes avanzadas (APT). Como sostienen las investigaciones en entornos tecnológicos de alta disponibilidad (Mena, 2021), el desconocimiento sobre la lógica interna y las vulnerabilidades de los activos conectados constituye el principal factor de riesgo, generando falsas sensaciones de seguridad perimetral si el operador técnico carece de una sólida base conceptual sobre los protocolos de resguardo.

El debate sobre la resiliencia operativa conduce necesariamente al indicador de Mar-cos de Seguridad y Firewalls. El National Institute of Standards and Technology (NIST, 2024), a través de su marco CSF 2.0, enfatiza que la resiliencia depende de la capacidad de los especialistas para tomar decisiones técnicas basadas en el riesgo y en la nueva función de Gobernanza. Esta visión encuentra su ejecución en el despliegue estratégico de tecnologías de contención, como firewalls de última generación, y en la adhesión estricta a la norma ISO/IEC 27001 (2022). Según Solarte (2015), esta estandarización permite transformar la tríada de confidencialidad, integridad y disponibilidad en un activo de confianza institucional, donde el conocimiento normativo asegura una ejecución técnica alineada con las mejores prácticas globales. En este sentido, autores como Merino (2022) demuestran que la adopción rigurosa de un marco referencial internacional reduce significativamente los niveles de riesgo sistémico, siempre que el personal técnico cuente con la formación continua requerida para implementar y auditar eficazmente dichos controles de seguridad.
de seguridad.

Metodología

La estructura metodológica de la presente investigación se fundamenta en un paradigma cuantitativo orientado hacia la evaluación sistemática del conocimiento técnico mediante la recolección y análisis de datos empíricos. El estudio se define como una investigación descriptiva, ya que se orienta a caracterizar el nivel de dominio operativo de los especialistas frente a las amenazas digitales. Según su nivel de profundidad, el trabajo busca detallar las propiedades y perfiles de la resiliencia en infraestructuras críticas sin la manipulación deliberada de las variables.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

En cuanto al diseño, la investigación es no experimental, de campo y transeccional. Es de campo, puesto que los datos fueron recolectados directamente en el contexto operativo de los sectores estratégicos, permitiendo un abordaje de la realidad institucional conforme a los lineamientos de Palella y Martins (2012). El carácter transeccional se debe a que la recolección de la información se realizó en un único momento temporal. La población se constituyó bajo un criterio de representatividad estratégica, conformada por setenta y cuatro (74) informantes clave con perfil técnico en redes y ciberseguridad.

Estos especia-listas pertenecen a organizaciones de diversos estratos (pequeñas, medianas y grandes empresas), proveedores de servicios de internet (ISP) y entidades vinculadas a los sectores energético y petroquímico. Debido al acceso directo a la totalidad de los sujetos que cumplen con el perfil especializado para el análisis de infraestructuras críticas, se trabajó con un censo poblacional, técnica avalada por Tamayo (2012) cuando la población es finita, conocida y accesible en su totalidad.

Se empleó la encuesta como técnica de recolección, utilizando un cuestionario formulado bajo una escala de tipo Likert con cinco opciones de respuesta (siempre, casi siempre, a veces, casi nunca, nunca). Para los fines de este artículo, el análisis se centró en la dimensión de Nivel de Conocimiento Técnico, conformada por reactivos distribuidos en los indicadores: identificación de amenazas, fundamentos de protección, y marcos de seguridad y firewalls. La validez de contenido fue certificada mediante juicio de diez (10) expertos en las áreas de telemática, ciberseguridad y metodología, quienes evaluaron la pertinencia, coherencia y suficiencia de los reactivos. Para determinar la confiabilidad, se realizó una prueba piloto dirigida a treinta (30) sujetos con características similares a la población objeto de estudio; los datos obtenidos fueron procesados mediante el coeficiente Alfa de Cronbach, el cual arrojó un valor de 0,895 para el instrumento global, indicando una consistencia interna muy alta.

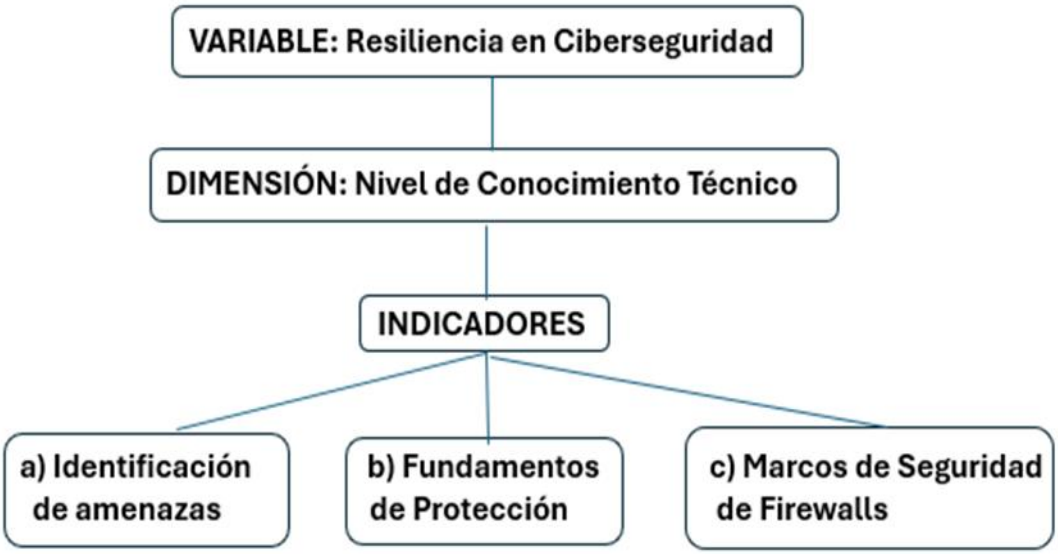
Para el tratamiento y análisis de la información, los datos recolectados fueron codifica-dos y tabulados utilizando el software Microsoft Excel. Se aplicaron técnicas de estadística descriptiva que incluyeron: (a) cálculo de frecuencias absolutas para determinar el número de respuestas en cada categoría de la escala Likert; (b) cálculo de frecuencias relativas expresadas en porcentajes para estandarizar los resultados y permitir la comparación entre indicadores; y (c) construcción de cuadros de distribución de frecuencias para organizar visualmente los hallazgos por cada ítem y dimensión evaluada. Asimismo, se calcularon medidas de tendencia central (media aritmética) para cada indicador, permitiendo identificar el nivel de conocimiento predominante en la población estudiada. Los resulta-dos fueron organizados en matrices tabulares para facilitar su interpretación. Finalmente, los resultados cuantitativos fueron contrastados mediante un análisis técnico-crítico frente a los estándares internacionales de la norma ISO/IEC 27001 (2022) y el framework NIST (2024), permitiendo diagnosticar la brecha de resiliencia en la capa humana de la red y sustentar las conclusiones del estudio.

Resultados

Una vez procesada y analizada la información recolectada de los setenta y cuatro (74) especialistas de tecnología pertenecientes a los sectores estratégicos, se procedió a realizar una interpretación sistemática de los hallazgos técnicos. La fundamentación de este análisis parte de la estructuración lógica de la dimensión evaluada en este estudio, la cual permite una transición coherente entre los estándares internacionales de seguridad y la evidencia empírica, como se detalla a continuación:

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Figura 1
Operacionalización de la Variable



Fuente: Elaboración propia (2026)

Indicador: Identificación de Amenazas

Este indicador presentó los niveles más bajos de toda la evaluación. Solo el 32% de los especialistas (24 de 74 encuestados) demostró capacidad para identificar correctamente vectores de ataque avanzados, como amenazas persistentes avanzadas (APT), malware emergente y técnicas de evasión de firewalls. El 41% (30 especialistas) se ubicó en un nivel medio, reconociendo únicamente amenazas comunes y patrones de ataque convencionales. Preocupa especialmente que el 27% restante (20 especialistas) mostrara un nivel bajo de preparación para anticipar y detectar intrusiones complejas. La media aritmética para este indicador fue de 2,8 sobre 5, lo que indica un nivel medio-bajo de preparación que compromete la resiliencia proactiva de las infraestructuras críticas.

Indicador: Fundamentos de Protección

Los resultados obtenidos para el indicador de Fundamentos de Protección mostraron una distribución más dispersa. El 42% de los especialistas (31 de 74) alcanzó un nivel alto de conocimiento sobre protocolos de seguridad en capas de red y principios de defensa en profundidad. Sin embargo, el 35% (26 especialistas) se ubicó en un nivel medio, y el 23% restante (17 especialistas) evidenció un conocimiento deficiente de los fundamentos teóricos que sustentan las medidas de protección implementadas. La media aritmética para este indicador fue de 3,1 sobre 5, revelando una brecha significativa entre la capacidad operativa y la comprensión de los principios subyacentes de seguridad.

Indicador: Marcos de Seguridad y Firewalls

Este indicador registró los puntajes más elevados de toda la evaluación. El 68% de los especialistas (50 de 74 encuestados) demostró un dominio alto en la configuración de firewalls de última generación y políticas de segmentación de redes. Asimismo, el 22% (16 especialistas) se ubicó en un nivel medio,

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

mientras que solo el 10% (8 especialistas) presentó dificultades significativas en la administración de estos dispositivos perimetrales. La media aritmética para este indicador fue de 4,2 sobre 5, lo que indica una fortaleza operativa consolidada en el manejo de herramientas de protección perimetral. Este dominio es particularmente notable en los sectores de proveedores de servicios de internet (ISP) y las industrias estratégicas de energía y petróleo.

Análisis Comparativo y Contrastación Teórica

Al relacionar estos hallazgos con los postulados de Malik (2021), se confirma que la resiliencia en infraestructuras críticas no puede depender exclusivamente del manejo de herramientas perimetrales. Según el autor, el conocimiento técnico debe ser evolutivo; el hecho de que los especialistas muestren fortalezas en la gestión de firewalls (media de 4,2) pero debilidades significativas en la identificación de amenazas complejas (media de 2,8) sugiere que la defensa se mantiene en un plano mayoritariamente reactivo.

La diferencia observada entre el dominio operativo de dispositivos perimetrales (media de 4,2) y la deficiente identificación proactiva de amenazas (media de 2,8) no es un fenómeno aislado, sino que sugiere un sesgo persistente en la formación técnica dentro del contexto venezolano. Esta tendencia revela que la capacitación profesional ha priorizado en la administración de hardware comercial sobre el análisis estratégico de riesgos, contraviniendo la visión de Malik (2021), quien sostiene que la seguridad no es un estado estático basado en equipos, sino un proceso dinámico dependiente del factor humano.

Al analizar este hallazgo a la luz de las realidades institucionales, se observa que el especialista tiende a preferir soluciones "enlatadas" extranjeras, muchas veces tratadas como "cajas negras" de las que se desconoce su lógica interna debido a que ofrecen una respuesta inmediata pero superficial. Como señala Mena (2021), este desconocimiento técnico sobre el funcionamiento profundo de los activos es el principal factor de riesgo en entornos conectados, pues genera una falsa sensación de seguridad que compromete la resiliencia proactiva.

Esta dependencia operativa de tecnologías foráneas sin una capacidad de análisis endógeno representa una vulnerabilidad crítica para la soberanía tecnológica nacional. La resiliencia de las infraestructuras estratégicas no puede delegarse únicamente a la robustez de un hardware que el técnico local no puede auditar plenamente. En consecuencia, se requiere una política de Estado que, en sintonía con lo propuesto por Ortiz (2020), trascienda la configuración de perímetros y priorice la formación de un talento humano capaz de desarrollar capacidades de defensa soberanas, basadas en el conocimiento profundo de los indicadores de compromiso y la inteligencia de amenazas propia.

La evidencia empírica señala una desconexión entre la operatividad técnica y los estándares globales de resiliencia del NIST (2024). Mientras que el 68% de los especialistas configura adecuadamente los firewalls, solo el 32% aplica los principios de identificación proactiva que exige el marco CSF 2.0. Esta brecha justifica la necesidad de una formación técnica continua que trascienda la simple administración de equipos.

Asimismo, los resultados reflejan una aplicación parcial de los requisitos de la norma ISO/IEC 27001 (2022). La capacidad de detectar amenazas (intrusiones) antes de que afecten la continuidad del servicio factor diferenciador entre una infraestructura vulnerable y una resiliente se ve comprometida por el bajo desempeño en la identificación de amenazas, donde un 27% de los especialistas presenta un nivel deficiente. Esta vulnerabilidad cognitiva ante ataques de alta complejidad representa el principal reto para la

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

protección de los activos estratégicos nacionales, demandando una alineación urgente con las mejores prácticas internacionales de seguridad digital.

Conclusiones

Tras la finalización de la investigación y el análisis sistemático de los datos recolectados de los setenta y cuatro (74) especialistas, se presentan las siguientes conclusiones en estricta correspondencia con los indicadores evaluados en la dimensión de Nivel de Cono-cimiento Técnico.

En relación con la Identificación de Amenazas, se concluye que existe una desigualdad crítica en la detección proactiva. Solo el 32% de los especialistas demostró capacidad para identificar vectores de ataque avanzados, con una media de 2,8 sobre 5, el puntaje más bajo de toda la evaluación. Este hallazgo ratifica lo expuesto por Malik (2021), evidenciando que la formación del talento humano en los sectores estratégicos analizados sigue anclada en un paradigma reactivo. La limitada capacidad de anticipación ante incidentes de alta complejidad constituye un factor de riesgo que compromete la estabilidad de la infraestructura nacional de red. Esta situación es particularmente preocupante si se considera que, como señala Ortiz (2020), los indicadores de compromiso (IoC) son esenciales para detectar ataques como denegación de servicio por inundación o envenenamiento ARP en dispositivos conectados, lo que permitiría una respuesta temprana ante las amenazas.

En cuanto a los Fundamentos de Protección, se determinó una desvinculación entre la experticia técnica individual y la aplicación de protocolos estandarizados. Con una media de 3,1 sobre 5 y un 23% de especialistas en nivel deficiente, el conocimiento sobre medidas preventivas se ejecuta mayoritariamente de manera empírica. Esto valida la tesis sobre la fragilidad de la resiliencia operativa cuando no existe una alineación simbiótica entre el personal y los estándares internacionales. Esta carencia procedimental incrementa la superficie de ataque, especialmente en las organizaciones encargadas de gestionar activos vitales para los sectores de energía y telecomunicaciones. Al respecto, los hallazgos de Merino (2022) demuestran que la aplicación de un marco referencial basado en ISO 27001 puede reducir significativamente los niveles de riesgo en organizaciones que manejan datos sensibles, siempre que el personal técnico cuente con la formación adecuada para implementar los controles establecidos.

Finalmente, sobre Marcos de Seguridad y Firewalls, se concluye que, aunque representa el área de mayor fortaleza técnica con una media de 4,2 sobre 5 y un 68% de dominio alto, su aplicación es predominantemente perimetral. Al no integrar plenamente los frameworks de resiliencia proactiva del NIST (2024) e ISO/IEC 27001 (2022), el profesional de las tecnologías de información delega la seguridad de los activos estratégicos en la robustez del hardware, debilitando la capacidad de respuesta del Estado ante incidentes disruptivos de gran escala. Estudios como el de Mena (2021) evidencian que el desconocimiento técnico sobre la lógica interna de los activos críticos conectados constituye el principal factor de riesgo en entornos industriales, situación que se agrava cuando no se proporciona formación continua sobre los marcos normativos y las mejores prácticas internacionales.

En virtud de los hallazgos, se afirma que la ciberseguridad ha trascendido la configuración de equipos para convertirse en un imperativo de resiliencia estratégica con implicaciones directas en la seguridad nacional. Se concluye que existe una dependencia crítica de tecnologías foráneas que, al ser operadas como soluciones cerradas, limitan la capacidad de respuesta autónoma del especialista ante incidentes complejos. No es suficiente la robustez de la infraestructura tecnológica; el factor determinante radica en la formación de un talento humano con capacidad de auditoría y análisis proactivo.

En consecuencia, se recomienda implementar programas de formación continua que trasciendan el manejo de hardware comercial y se enfoquen en la identificación proactiva de amenazas y la soberanía tecnológica.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026

Es necesario que el estado y la academia fomenten el desarrollo de capacidades para la detección temprana de incidentes mediante el uso de indicadores de compromiso, tal como lo sugiere la literatura especializada (Ortiz, 2020; Merino, 2022). Bajo esta premisa, los hallazgos de este diagnóstico sustentan de manera concluyente el diseño de la Ruta Crítica de Alineación Predictiva (RCAP), la cual se erige como la respuesta estratégica y operativa necesaria para transformar la gestión del talento humano y garantizar que la experticia técnica nacional se constituya como la verdadera primera línea de defensa resiliente ante los desafíos del ecosistema digital global.

Referencias

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and pri-vacy protection Information security management systems — Requirements*. International Organization for Standardization.

Malik, S. (2021). Network security principles and practices. Cisco Press.

Mena, V. (2021). Guía metodológica para el control de vulnerabilidades informáticas en dispositivos IoT para redes HAN [Tesis de maestría, Escuela Superior Politécni-ca de Chimborazo].

Merino, J. (2022). Marco referencial de seguridad para reducir riesgos en el tratamiento de datos personales en empresas prestadoras de servicios de acceso a internet, uti-lizando ISO 27001. Caso MUNDOTRONIC [Tesis de maestría, Escuela Supe-rior Politécnica de Chimborazo].

NIST. (2024). Framework for improving critical infrastructure cybersecurity (Version 2.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Ortiz, D. (2020). Plan de alertas basado en indicadores de compromiso para dispositivos Smart Switch/plug en IoT [Tesis de maestría, Instituto Tecnológico Metropoli-tano].

Palella, S., & Martins, F. (2012). Metodología de la investigación cuantitativa. FEDU-PEL.

Solarte, R. (2015). Gestión de la Seguridad de la Información: Enfoque basado en ISO 27001. Editorial Académica Española.

Tamayo y Tamayo, M. (2012). El proceso de la investigación científica (5ta ed.). Limusa.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 25 Edición No 01– Año 2026