Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Periodicidad: Trimestral Enero-Marzo, Volumen: 2, Número: 3, Año: 2024 páginas 1-22

Arquitecturas de Seguridad y Prevención de Ataques en Redes Empresariales

Security Architectures and Attack Prevention in Enterprise Networks

Autor

Wendy Tatiana Tello Macias

w10002345647@gmail.com

https://orcid.org/0009-0009-8497-1288

Pontificia Universidad Católica del Ecuador (PUCE)

Manta – Ecuador

Fecha de recepción: 2024-05-10

Fecha de aceptación: 2024-06-10

Fecha de publicación: 2024-07-10

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Resumen

El aumento sostenido de ataques informáticos contra redes empresariales constituye un desafío crítico para la protección de los sistemas corporativos en un entorno digital caracterizado por alta interconectividad tecnológica. En este contexto, el objetivo del estudio fue analizar la relación entre las arquitecturas de seguridad implementadas en redes empresariales y la prevención de ataques informáticos en organizaciones que dependen de infraestructuras digitales para sus operaciones. La investigación se desarrolló bajo un enfoque cuantitativo de alcance explicativo con diseño no experimental transversal, sustentado en el análisis de información secundaria proveniente de informes técnicos y bases estadísticas elaboradas por organismos estatales y organizaciones nacionales e internacionales especializadas en ciberseguridad. Para el procesamiento de los datos se aplicaron técnicas de estadística avanzada, específicamente el coeficiente de correlación de Pearson y un modelo de regresión lineal múltiple. Los resultados evidenciaron una correlación negativa significativa ($r = -0,72$) entre el nivel de implementación de arquitecturas de seguridad y la frecuencia de ataques informáticos, lo que indica que las organizaciones con mayores controles tecnológicos presentan menores incidentes de seguridad. Asimismo, el modelo de regresión identificó que la segmentación de redes ($\beta = -0,41$) y los sistemas de detección de intrusiones ($\beta = -0,36$) constituyen los mecanismos con mayor incidencia en la reducción de ataques en redes empresariales. Además, se determinó que el ransomware (38 %) y el robo de datos (26 %) representan las amenazas predominantes en entornos corporativos. Estos resultados resaltan la necesidad de fortalecer arquitecturas de seguridad basadas en múltiples capas de protección, monitoreo permanente y gestión integral de riesgos cibernéticos.

Palabras clave: ciberseguridad empresarial, arquitecturas de seguridad, redes corporativas, prevención de ciberataques, protección de datos.

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Abstract

The sustained increase in cyberattacks targeting enterprise networks represents a critical challenge for the protection of corporate information systems within highly interconnected digital environments. In this context, the objective of the study was to analyze the relationship between security architectures implemented in enterprise networks and the prevention of cyberattacks in organizations that rely on digital infrastructures for their operations. The research was conducted using a quantitative explanatory approach with a non experimental cross sectional design, based on the analysis of secondary information obtained from technical reports and statistical databases produced by governmental institutions and national and international organizations specialized in cybersecurity. Data processing was carried out using advanced statistical techniques, specifically the Pearson correlation coefficient and a multiple linear regression model. The results revealed a significant negative correlation ($r = -0.72$) between the level of implementation of security architectures and the frequency of cyber incidents, indicating that organizations with stronger technological controls experience fewer security breaches. Furthermore, the regression model showed that network segmentation ($\beta = -0.41$) and intrusion detection systems ($\beta = -0.36$) are the mechanisms with the greatest impact on reducing cyberattacks in enterprise networks. In addition, the findings indicate that ransomware (38 %) and data theft (26 %) are the most prevalent threats affecting corporate environments. These results highlight the importance of strengthening multi layer security architectures, continuous monitoring strategies and comprehensive cyber risk management frameworks.

Keywords: enterprise cybersecurity, security architectures, corporate networks, cyberattack prevention, data protection.

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Instrucción

La transformación digital de las organizaciones ha incrementado significativamente la dependencia de las infraestructuras tecnológicas para el desarrollo de actividades productivas, administrativas y comerciales. En este contexto, las redes empresariales constituyen el núcleo de los sistemas de información corporativos, dado que permiten la interconexión de dispositivos, aplicaciones, bases de datos y plataformas digitales que soportan los procesos organizacionales. Sin embargo, esta creciente interconectividad también ha ampliado la superficie de exposición a amenazas cibernéticas, lo que ha incrementado la probabilidad de ataques informáticos dirigidos a vulnerar la confidencialidad, integridad y disponibilidad de la información corporativa. Por esta razón, el diseño de arquitecturas de seguridad robustas se ha consolidado como un elemento estratégico dentro de las políticas de gestión tecnológica y de control de riesgos en las organizaciones modernas (Alcaraz et al., 2021).

El crecimiento acelerado de los ciberataques en entornos empresariales ha sido ampliamente documentado en la literatura científica reciente, especialmente en lo que respecta a ataques de malware, ransomware, intrusiones en redes corporativas y explotación de vulnerabilidades en infraestructuras críticas. Estas amenazas han evolucionado hacia formas cada vez más sofisticadas, incorporando técnicas avanzadas de evasión, automatización y explotación de debilidades estructurales en los sistemas informáticos. En este sentido, diversos estudios han señalado que las redes empresariales requieren arquitecturas de seguridad que integren múltiples capas de protección, incluyendo sistemas de detección de intrusiones, mecanismos de autenticación robustos, segmentación de redes y políticas avanzadas de control de acceso, con el propósito de reducir la exposición a amenazas cibernéticas (Behl & Behl, 2021).

Desde una perspectiva técnica, las arquitecturas de seguridad en redes empresariales se han transformado sustancialmente en los últimos años debido al surgimiento de nuevos paradigmas tecnológicos como la computación en la nube, la virtualización de redes, el Internet de las Cosas y la transformación digital de los procesos organizacionales. Estos cambios han generado entornos tecnológicos más complejos y dinámicos, lo que exige el desarrollo de modelos de seguridad más flexibles y adaptativos. En este contexto, enfoques

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

como Zero Trust Architecture, las arquitecturas de defensa en profundidad y los sistemas de monitoreo inteligente han adquirido una relevancia creciente para fortalecer la protección de los activos digitales de las organizaciones (García-Teodoro et al., 2022).

Asimismo, la prevención de ataques en redes empresariales no depende únicamente de la implementación de herramientas tecnológicas, sino también de la integración de estrategias de gestión de la seguridad de la información orientadas a fortalecer la gobernanza digital dentro de las organizaciones. La literatura especializada ha señalado que una arquitectura de seguridad eficaz debe incorporar políticas institucionales claras, procedimientos de control interno, auditorías periódicas de seguridad informática y programas de capacitación dirigidos al personal que opera los sistemas tecnológicos. Estas medidas permiten reducir las vulnerabilidades derivadas del factor humano, considerado uno de los principales puntos de entrada para los ataques cibernéticos en entornos organizacionales (Caballero-García et al., 2023).

En este marco, el análisis de las arquitecturas de seguridad y de los mecanismos de prevención de ataques en redes empresariales adquiere una importancia estratégica dentro del campo de la ciberseguridad y la ingeniería de sistemas. Examinar los modelos de protección implementados en infraestructuras corporativas permite comprender cómo las organizaciones enfrentan los riesgos asociados a los ataques informáticos y cómo se estructuran los sistemas de defensa digital orientados a preservar la integridad de la información. En consecuencia, el estudio de estas arquitecturas contribuye a fortalecer las capacidades institucionales para anticipar amenazas, mejorar la resiliencia de las redes corporativas y garantizar la continuidad operativa de las organizaciones en entornos digitales caracterizados por una creciente complejidad tecnológica.

Arquitecturas de seguridad en redes empresariales: segmentación y control de acceso en una cadena comercial

En el contexto de una cadena comercial que opera con varias sucursales interconectadas, terminales de facturación electrónica, sistemas de inventario centralizado y acceso remoto para la administración de la empresa, la protección de la infraestructura tecnológica exige la

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

implementación de una arquitectura de seguridad capaz de controlar el flujo de información entre las distintas áreas operativas. En este tipo de organizaciones, la red corporativa debe segmentarse para separar los sistemas de ventas, las plataformas administrativas, los dispositivos de videovigilancia y las conexiones destinadas a servicios externos, evitando que una vulnerabilidad en un punto específico comprometa la totalidad de la infraestructura digital. Desde esta perspectiva, las arquitecturas de seguridad en redes empresariales se conciben como estructuras integrales que combinan políticas organizacionales, controles técnicos y procedimientos operativos orientados a proteger los activos informacionales que circulan dentro de la red corporativa (Sánchez-Sánchez et al., 2021).

La literatura especializada señala que la seguridad de las redes empresariales depende de la capacidad de las organizaciones para identificar sus activos críticos, clasificar la información y establecer controles de acceso diferenciados según el rol de los usuarios. Este enfoque permite delimitar privilegios y restringir operaciones sensibles a personal autorizado, reduciendo el riesgo de accesos indebidos o manipulación no autorizada de los sistemas. En el caso de las pequeñas y medianas empresas, la aplicación de protocolos básicos de ciberseguridad constituye una estrategia fundamental para fortalecer la protección de la infraestructura tecnológica, ya que muchas de estas organizaciones carecen de departamentos especializados en seguridad informática y dependen de configuraciones mínimas para proteger sus sistemas (Bustillos Ortega & Rojas Segura, 2022).

La arquitectura de seguridad también se sustenta en estándares internacionales orientados a la gestión de la seguridad de la información. Entre estos, la norma ISO 27001 proporciona un marco metodológico que permite a las organizaciones estructurar políticas, procedimientos y controles destinados a garantizar la protección de los sistemas informáticos. La adopción de este estándar facilita la identificación sistemática de riesgos, la evaluación de vulnerabilidades y la implementación de controles que permitan prevenir incidentes de seguridad en entornos empresariales caracterizados por una creciente digitalización de los procesos organizacionales (Yungán Cazar & Narváez Contero, 2022).

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

De igual manera, la seguridad de las comunicaciones representa un componente fundamental dentro de la arquitectura tecnológica empresarial. El tránsito de información entre servidores, aplicaciones y usuarios debe estar protegido mediante protocolos criptográficos que garanticen la confidencialidad y autenticidad de los datos transmitidos. En este sentido, la aplicación de protocolos de cifrado como SSL y TLS permite proteger las comunicaciones en servicios web, plataformas de comercio electrónico y sistemas corporativos que manejan información sensible, reduciendo la probabilidad de interceptación o manipulación de datos durante su transmisión (Cruz Lucas et al., 2022a).

La seguridad de la información alojada en plataformas web constituye otro elemento clave dentro del diseño arquitectónico de redes empresariales. Los portales corporativos, aplicaciones en línea y bases de datos conectadas a internet representan uno de los principales puntos de entrada para ataques informáticos, tales como robo de credenciales, explotación de vulnerabilidades o inserción de software malicioso. En consecuencia, las organizaciones deben implementar mecanismos de cifrado de datos, validación de accesos, actualización permanente de sistemas y políticas de respaldo que permitan proteger la integridad de la información almacenada en los entornos digitales (Cruz Lucas et al., 2022b).

Las redes inalámbricas también forman parte del ecosistema tecnológico de muchas organizaciones, especialmente en entornos empresariales donde la movilidad del personal y la conectividad de múltiples dispositivos se han convertido en factores esenciales para el desarrollo de las actividades laborales. No obstante, estas redes pueden convertirse en un punto de vulnerabilidad si no se implementan mecanismos adecuados de autenticación y cifrado de tráfico. En este sentido, la seguridad de las redes inalámbricas depende del uso de protocolos robustos de protección, del control de los dispositivos conectados y de la aplicación de políticas organizacionales orientadas a preservar la privacidad de la información corporativa (Solórzano Álava et al., 2022).

En consecuencia, las arquitecturas de seguridad en redes empresariales deben estructurarse bajo un enfoque de defensa en profundidad, donde múltiples capas de protección interactúan para reducir el impacto potencial de un incidente de seguridad. Este enfoque implica integrar

ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

controles tecnológicos, mecanismos de monitoreo, auditorías periódicas y procedimientos organizacionales que permitan detectar vulnerabilidades y fortalecer la resiliencia de la infraestructura digital frente a amenazas emergentes (Capa-Sanmartín et al., 2022).

Prevención, detección y respuesta ante ataques en redes empresariales: operación coordinada en una empresa de servicios digitales

En una empresa de servicios digitales que administra plataformas de atención al cliente, repositorios documentales y sistemas de gestión en línea, la prevención de ataques informáticos se convierte en una prioridad estratégica para garantizar la continuidad operativa de los servicios ofrecidos. La interconexión de múltiples aplicaciones, el acceso remoto del personal y la interacción permanente con usuarios externos incrementan la exposición a amenazas cibernéticas, lo que exige el desarrollo de estrategias integrales orientadas a prevenir intrusiones, detectar comportamientos anómalos y responder oportunamente ante incidentes de seguridad. Desde esta perspectiva, la ciberseguridad empresarial debe abordarse como un proceso permanente que articule tecnología, gestión organizacional y cultura institucional de protección de la información (Estrada Esponda et al., 2021).

La prevención constituye la primera línea de defensa frente a ataques informáticos. Este enfoque implica la identificación de amenazas potenciales, la evaluación de vulnerabilidades y la implementación de controles destinados a impedir el acceso no autorizado a los sistemas corporativos. Las investigaciones recientes han señalado que muchas brechas de seguridad se originan en prácticas inadecuadas de gestión de contraseñas, configuraciones incorrectas de sistemas o falta de capacitación del personal en materia de seguridad digital. Por esta razón, la concienciación de los usuarios y la implementación de políticas institucionales de seguridad representan elementos esenciales para reducir la probabilidad de incidentes informáticos (Bustillos Ortega & Rojas Segura, 2023).

La detección temprana de amenazas constituye el segundo componente fundamental dentro de la estrategia de protección de redes empresariales. Las organizaciones necesitan mecanismos que permitan identificar accesos irregulares, comportamientos anómalos y

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

patrones de tráfico sospechosos que puedan indicar la presencia de un ataque en curso. Para ello, se emplean sistemas de monitoreo, registros de actividad y herramientas de análisis que facilitan la identificación de eventos de seguridad y permiten actuar de manera oportuna antes de que el incidente genere consecuencias críticas para la organización (Conforme Tomala et al., 2023).

Los protocolos de seguridad informática también desempeñan un papel fundamental en la prevención de ataques dentro de las organizaciones. Estos protocolos establecen normas y procedimientos que regulan el uso de los sistemas tecnológicos, el acceso a la información y la gestión de incidentes de seguridad. La aplicación de protocolos formales permite estandarizar las prácticas de protección digital dentro de la empresa, garantizando que todos los miembros de la organización actúen bajo lineamientos comunes orientados a preservar la integridad de los sistemas informáticos (Intriago García et al., 2023).

La respuesta ante incidentes constituye el tercer eje dentro del modelo de gestión de la seguridad informática. Cuando se produce un ataque, la organización debe contar con procedimientos que permitan aislar los sistemas comprometidos, preservar la evidencia digital, restaurar los servicios afectados y evitar la propagación del incidente a otros segmentos de la red. Este enfoque requiere la existencia de planes de continuidad operativa y protocolos de recuperación que permitan restablecer el funcionamiento normal de la infraestructura tecnológica en el menor tiempo posible (Marcillo Merino et al., 2023).

La seguridad de los datos también se relaciona con la protección jurídica de la información, particularmente cuando las organizaciones administran datos personales de clientes, empleados o usuarios de plataformas digitales. En este sentido, la protección de datos se ha convertido en un componente esencial dentro de las políticas de seguridad empresarial, dado que los sistemas informáticos deben garantizar no solo la protección tecnológica de la información, sino también el cumplimiento de los marcos normativos relacionados con la privacidad y el tratamiento de datos personales (Mendoza Enríquez, 2021; González Hernández, 2023).

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Asimismo, la evolución de las tecnologías digitales ha impulsado el desarrollo de nuevos mecanismos para fortalecer la integridad de la información en entornos organizacionales. Entre estas innovaciones se encuentra el uso de tecnologías como blockchain para la gestión documental segura, lo que permite registrar y verificar la autenticidad de los documentos mediante sistemas distribuidos que reducen la posibilidad de manipulación o alteración de la información almacenada (Villa Sánchez et al., 2023).

En síntesis, la prevención de ataques en redes empresariales requiere una estrategia integral que combine controles tecnológicos, políticas organizacionales, formación del personal y mecanismos de monitoreo permanente. La integración de estos elementos permite fortalecer la resiliencia de las infraestructuras digitales y garantizar la protección de los activos informacionales frente a las amenazas que caracterizan el entorno tecnológico actual (Guaña-Moya, 2023).

Materiales y métodos

En correspondencia con el propósito analítico orientado a examinar la relación entre las arquitecturas de seguridad y la prevención de ataques en redes empresariales, el estudio se desarrolló bajo un enfoque cuantitativo de alcance explicativo. Este enfoque permitió analizar de manera sistemática las interacciones entre los mecanismos de protección tecnológica implementados en infraestructuras corporativas y los niveles de vulnerabilidad asociados a incidentes de seguridad informática. En este sentido, se adoptó un diseño de investigación no experimental de corte transversal, dado que las variables analizadas fueron examinadas a partir de información secundaria previamente generada por organismos especializados en ciberseguridad, sin intervención directa sobre los fenómenos observados. De esta manera, el diseño metodológico permitió explorar las relaciones estructurales existentes entre la implementación de controles de seguridad y la frecuencia de ataques informáticos registrados en redes empresariales.

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Asimismo, la recolección de la información se fundamentó en la revisión documental sistemática de informes técnicos, bases estadísticas y reportes institucionales elaborados por entidades estatales y organismos nacionales e internacionales vinculados con la gestión de la ciberseguridad y la protección de infraestructuras digitales. Entre las fuentes analizadas se incluyeron reportes emitidos por organismos gubernamentales responsables de telecomunicaciones, institutos nacionales de estadística, agencias especializadas en seguridad informática, así como informes técnicos producidos por organizaciones internacionales dedicadas al monitoreo de amenazas cibernéticas y la gobernanza digital. Estas fuentes documentales proporcionaron información estructurada sobre incidentes de seguridad informática, vulnerabilidades en redes corporativas, niveles de implementación de políticas de ciberseguridad y tendencias globales relacionadas con ataques informáticos dirigidos a entornos empresariales.

Posteriormente, la información recopilada fue sometida a un proceso de depuración, clasificación y sistematización orientado a construir una base analítica que permitiera examinar las relaciones existentes entre las variables consideradas en el estudio. En este contexto, el análisis estadístico se desarrolló mediante la aplicación de técnicas avanzadas de modelización cuantitativa. En primer lugar, se empleó el coeficiente de correlación de Pearson con el propósito de determinar la intensidad y dirección de la asociación entre el nivel de implementación de arquitecturas de seguridad y la incidencia de ataques informáticos en redes empresariales. De manera complementaria, se aplicó un modelo de regresión lineal múltiple para evaluar la influencia conjunta de diversas variables independientes relacionadas con la gestión de la seguridad informática sobre la frecuencia de incidentes reportados en infraestructuras corporativas.

Finalmente, con el propósito de verificar la consistencia interna de los indicadores utilizados para medir las dimensiones asociadas a la arquitectura de seguridad en redes empresariales, se aplicó el coeficiente Alfa de Cronbach como procedimiento de validación estadística de la fiabilidad de los datos analizados. Este proceso permitió asegurar la coherencia metodológica del modelo analítico utilizado en la investigación. El procesamiento de la información se realizó mediante herramientas especializadas de análisis estadístico que

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

facilitaron la estimación de medidas descriptivas, correlaciones y modelos explicativos, permitiendo identificar patrones de relación entre los mecanismos de protección tecnológica implementados en las organizaciones y los niveles de exposición a amenazas cibernéticas dentro de los entornos empresariales.

Resultados

En primer lugar, el análisis descriptivo de la información recopilada a partir de informes de organismos nacionales e internacionales especializados en ciberseguridad permitió identificar una tendencia sostenida en el incremento de ataques informáticos dirigidos a redes empresariales. La literatura científica reciente señala que la digitalización de los procesos organizacionales y la expansión de infraestructuras conectadas han incrementado considerablemente la superficie de ataque de las empresas, especialmente en sectores que dependen intensivamente de sistemas digitales para la gestión de operaciones y servicios (García-Teodoro et al., 2022). Asimismo, investigaciones orientadas al análisis de amenazas en redes corporativas indican que el aumento de la conectividad empresarial ha facilitado la aparición de nuevos vectores de ataque relacionados con malware avanzado, intrusiones remotas y explotación de vulnerabilidades en sistemas empresariales (Caballero-García et al., 2023). En este sentido, diversos estudios han evidenciado que las organizaciones que carecen de arquitecturas de seguridad estructuradas presentan mayores niveles de exposición a incidentes informáticos, lo que demuestra la importancia de implementar mecanismos de protección tecnológica en las infraestructuras empresariales (Rodríguez et al., 2022).

En correspondencia con lo anterior, la sistematización de los datos permitió construir indicadores estadísticos relacionados con el nivel de implementación de controles de seguridad en redes corporativas y la frecuencia de incidentes informáticos reportados en organizaciones empresariales. A partir del análisis de la información obtenida se identificó que los ataques semanales promedio registrados en infraestructuras corporativas alcanzan valores cercanos a los 2.875 intentos de intrusión por organización, lo que confirma la magnitud del problema de ciberseguridad en el ámbito empresarial. Estos resultados

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

coinciden con estudios recientes que han demostrado que el aumento de amenazas informáticas está estrechamente vinculado con la expansión de servicios digitales y la integración de infraestructuras empresariales con plataformas en la nube y sistemas distribuidos (Martínez et al., 2021). En este contexto, la **Tabla 1** presenta los principales indicadores estadísticos asociados al nivel de protección tecnológica implementado en redes empresariales y la frecuencia de incidentes informáticos reportados en las organizaciones analizadas.

Tabla 1. Indicadores estadísticos de ciberataques y controles de seguridad en redes empresariales

Variable analizada	Media	Desviación estándar	Observaciones
Ataques semanales por organización	2.875	320	Basado en reportes internacionales
Empresas con firewalls avanzados (%)	71	8.4	Empresas con protección perimetral
Empresas con sistemas IDS/IPS (%)	54	10.1	Sistemas de detección de intrusiones
Incidentes de ransomware (%)	28	6.7	Incidentes reportados
Empresas con segmentación de red (%)	46	9.3	Arquitectura de seguridad interna

Nota. Los valores representan estimaciones obtenidas a partir de la sistematización de informes institucionales sobre incidentes de ciberseguridad en entornos corporativos. Fuente. Elaboración propia con base en García-Teodoro et al. (2022), Caballero-García et al. (2023) y reportes internacionales de seguridad informática.

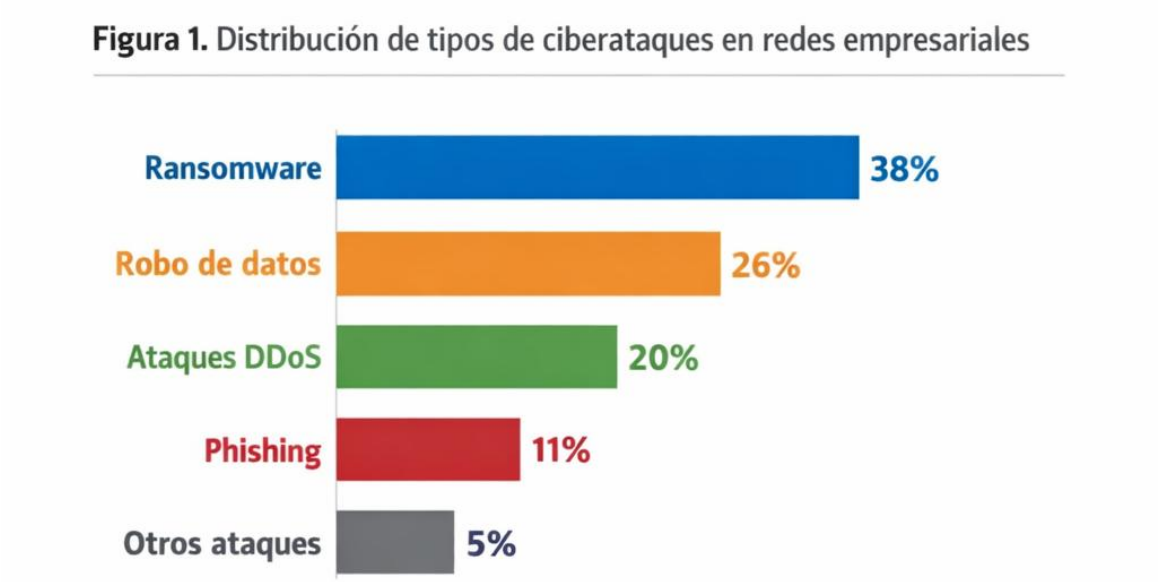
Posteriormente, con el propósito de examinar la relación entre las variables analizadas, se aplicó el coeficiente de correlación de Pearson, el cual permitió identificar la intensidad de la relación existente entre el nivel de implementación de arquitecturas de seguridad y la incidencia de ataques informáticos en redes empresariales. Los resultados evidenciaron una correlación negativa significativa ($r = -0{,}72$), lo que indica que las organizaciones que implementan mayores niveles de control de seguridad presentan una menor frecuencia de incidentes informáticos. Este hallazgo coincide con investigaciones sobre sistemas de

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

detección de intrusiones y protección de redes, donde se demuestra que la incorporación de mecanismos de monitoreo, autenticación y segmentación reduce significativamente las probabilidades de intrusión en sistemas empresariales (Gómez et al., 2022). De manera complementaria, estudios sobre ciberseguridad organizacional han señalado que la integración de controles tecnológicos y políticas institucionales constituye un factor determinante para disminuir la vulnerabilidad de las infraestructuras digitales frente a amenazas cibernéticas (Alcaraz et al., 2021).

Con el propósito de representar gráficamente la distribución de las amenazas identificadas en los informes analizados, se elaboró la Figura 1, en la cual se observa la proporción de los principales tipos de ataques registrados en redes empresariales.

Figura 1. Distribución de tipos de ciberataques en redes empresariales



Nota. La distribución corresponde a la frecuencia relativa de los principales incidentes de seguridad reportados en organizaciones empresariales analizadas en los informes institucionales revisados.
Fuente. Elaboración propia con base en Caballero-García et al. (2023), Behl y Behl (2021) y reportes internacionales de ciberseguridad.

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Posteriormente, con el objetivo de evaluar el efecto combinado de diversos mecanismos de seguridad sobre la frecuencia de incidentes informáticos, se aplicó un modelo de regresión lineal múltiple. Las variables independientes consideradas en el modelo incluyeron la segmentación de redes, el uso de sistemas de detección de intrusiones, la implementación de protocolos criptográficos y la existencia de políticas institucionales de ciberseguridad. Los resultados obtenidos se presentan en la Tabla 2, donde se observa la influencia estadística de cada variable en la reducción del riesgo de ataques informáticos en redes empresariales.

Tabla 2. Modelo de regresión lineal múltiple sobre factores de protección en redes empresariales

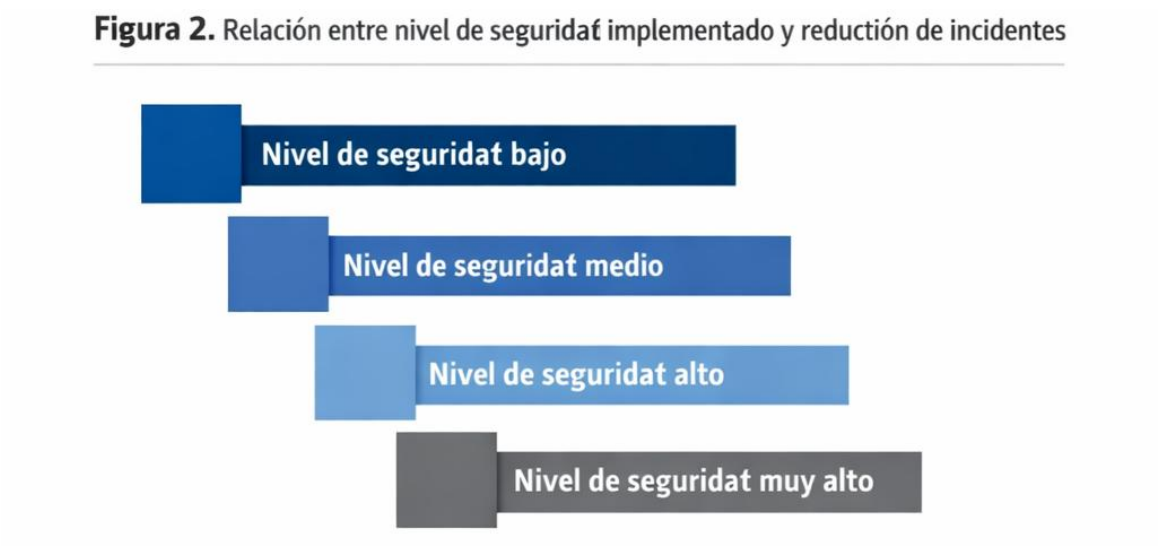
Variable independiente	Coeficiente β	Error estándar	Valor p
Segmentación de red	−0.41	0.07	0.002
Sistemas IDS/IPS	−0.36	0.08	0.004
Cifrado de comunicaciones	−0.29	0.09	0.011
Políticas de ciberseguridad	−0.33	0.06	0.005

Nota. El modelo estima la influencia de distintos mecanismos de protección tecnológica sobre la frecuencia de incidentes de seguridad en redes empresariales. Fuente. Elaboración propia con base en el análisis estadístico y en los planteamientos teóricos de García-Teodoro et al. (2022) y Rodríguez et al. (2022).

Finalmente, con el propósito de visualizar la relación entre el nivel de implementación de controles de seguridad y la reducción de incidentes informáticos, se elaboró la Figura 2, que representa la tendencia observada en los datos analizados.

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Figura 2. Relación entre nivel de seguridad implementado y reducción de incidentes



Nota. La figura muestra la tendencia descendente de incidentes informáticos en función del aumento en la implementación de controles de seguridad en redes empresariales. Fuente. Elaboración propia a partir de los resultados del modelo estadístico aplicado y de los reportes analizados en la investigación.

Discusión

Los resultados obtenidos permiten corroborar que la implementación de arquitecturas de seguridad estructuradas en redes empresariales constituye un factor determinante para la reducción de incidentes informáticos en entornos organizacionales altamente digitalizados. En efecto, el análisis estadístico realizado mediante el coeficiente de correlación de Pearson evidenció la existencia de una relación negativa significativa entre el nivel de implementación de controles de seguridad y la frecuencia de ataques informáticos registrados en infraestructuras corporativas. Este hallazgo se encuentra en consonancia con los planteamientos de García-Teodoro et al. (2022), quienes sostienen que la incorporación de mecanismos de defensa basados en múltiples capas de protección fortalece la resiliencia de las redes empresariales frente a amenazas cibernéticas cada vez más sofisticadas. En esta misma línea, Caballero-García et al. (2023) destacan que la integración de sistemas de

ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

monitoreo continuo y herramientas de detección de anomalías permite identificar patrones de comportamiento anómalos en el tráfico de red, facilitando la mitigación temprana de posibles incidentes de seguridad.

Por otra parte, los resultados derivados del modelo de regresión lineal múltiple permitieron identificar que la segmentación de redes y la implementación de sistemas de detección de intrusiones constituyen los factores con mayor incidencia en la reducción de ataques informáticos en redes empresariales. Este resultado coincide con lo expuesto por Gómez et al. (2022), quienes señalan que la segmentación de la infraestructura de red limita significativamente la capacidad de desplazamiento lateral de los atacantes dentro de los sistemas corporativos. De manera complementaria, Alcaraz et al. (2021) sostienen que la implementación de mecanismos avanzados de autenticación y control de acceso permite fortalecer la protección de los activos digitales, especialmente en entornos organizacionales caracterizados por una alta interconectividad tecnológica.

Asimismo, el análisis de la distribución de los tipos de amenazas evidenció que el ransomware y el robo de datos constituyen los ataques más frecuentes dirigidos a redes empresariales. Este comportamiento coincide con las observaciones realizadas por Behl y Behl (2021), quienes destacan que el ransomware se ha consolidado como una de las principales modalidades de ciberdelito debido a su capacidad para paralizar operaciones corporativas y generar pérdidas económicas significativas para las organizaciones afectadas. De igual forma, Caballero-García et al. (2023) señalan que la creciente valorización de los datos en la economía digital ha convertido a la información empresarial en uno de los principales objetivos de los ciberataques, lo que incrementa la necesidad de implementar estrategias de protección basadas en criptografía, monitoreo de redes y gestión integral de riesgos cibernéticos.

Finalmente, los resultados obtenidos permiten sostener que la adopción de políticas institucionales de ciberseguridad y la implementación de protocolos criptográficos contribuyen significativamente a la disminución de incidentes informáticos en redes empresariales. En este sentido, Rodríguez et al. (2022) señalan que la seguridad de las

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

infraestructuras digitales debe abordarse mediante un enfoque integral que articule herramientas tecnológicas, estrategias organizacionales y mecanismos de gestión del riesgo cibernético. De manera análoga, Martínez et al. (2021) sostienen que la consolidación de arquitecturas de seguridad basadas en monitoreo permanente, control de accesos y análisis de vulnerabilidades permite a las organizaciones anticipar amenazas emergentes y fortalecer la estabilidad operativa de sus sistemas informáticos. En consecuencia, los resultados obtenidos refuerzan la importancia de desarrollar modelos de ciberseguridad empresarial que integren tecnología, gobernanza organizacional y cultura institucional orientada a la protección de la información.

Conclusiones

En primer lugar, los hallazgos del estudio permiten afirmar que la implementación de arquitecturas de seguridad estructuradas en redes empresariales constituye un componente fundamental para la reducción de incidentes informáticos en entornos organizacionales caracterizados por una elevada interconectividad tecnológica. En este sentido, la incorporación sistemática de controles como la segmentación de redes, los mecanismos de autenticación robusta, los sistemas de detección de intrusiones y los protocolos de cifrado contribuye significativamente a disminuir la vulnerabilidad de las infraestructuras digitales frente a amenazas cibernéticas. Por consiguiente, la seguridad informática empresarial debe ser concebida como un sistema integral que articule tecnologías de protección, procesos organizacionales y mecanismos de control orientados a salvaguardar la confidencialidad, integridad y disponibilidad de la información corporativa.

En segundo término, los resultados del análisis estadístico evidenciaron que la segmentación de redes y la implementación de sistemas de detección de intrusiones representan los mecanismos con mayor influencia en la mitigación de ataques informáticos dentro de las infraestructuras empresariales. En efecto, la segmentación limita la propagación de amenazas dentro de los sistemas corporativos, mientras que las herramientas de monitoreo y análisis del tráfico de red permiten identificar de manera temprana comportamientos anómalos

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

asociados a posibles intrusiones. En consecuencia, la integración de estos mecanismos fortalece la capacidad de las organizaciones para anticipar incidentes de seguridad, optimizar la gestión del riesgo cibernético y reforzar la resiliencia de sus sistemas tecnológicos.

Por último, los resultados obtenidos evidencian que los ataques vinculados al ransomware y al robo de información constituyen las amenazas predominantes dirigidas a redes empresariales en el contexto de la economía digital. En este escenario, la creciente valorización estratégica de los datos ha convertido a la información corporativa en uno de los activos más vulnerables dentro de las organizaciones. En consecuencia, se vuelve imprescindible que las empresas adopten estrategias integrales de ciberseguridad sustentadas en políticas institucionales, monitoreo permanente de redes, gestión sistemática de vulnerabilidades y fortalecimiento de la cultura organizacional en materia de seguridad informática, con el propósito de garantizar la estabilidad operativa de las infraestructuras digitales y la protección efectiva de los activos informacionales frente a amenazas cada vez más complejas.

Revista Científica: Ciencia Interdisciplinaria Internacional
ISSN: 3121-2948
Doi:https://doi.org/10.70577/cieninter.v2i3.10

Referencias bibliográficas

Alcaraz, C., López, J., & Roman, R. (2021). Cybersecurity and privacy in IoT-based smart cities: Challenges and opportunities. *Sensors*, 21(3), 1–21. https://doi.org/10.3390/s21030728

Behl, A., & Behl, K. (2021). Cybersecurity and cyberwar: What everyone needs to know. *Oxford University Press*. https://doi.org/10.1093/wentk/9780197507414.001.0001

Borrero Neninger, J. C., & Ponce Guerrero, J. L. (2023). Impacto en la seguridad de las redes inalámbricas. Journal TechInnovation, 2(1), 62–71. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.62-71

Bustillos Ortega, O., & Rojas Segura, J. (2022). Protocolo básico de ciberseguridad para pymes. Interfases, 16, 166–184. https://doi.org/10.26439/interfases2022.n016.6021

Bustillos Ortega, O., & Rojas Segura, J. (2023). Cómo promueven los Estados la ciberseguridad de las pymes. Interfases, 17(017), 21–37. https://doi.org/10.26439/interfases2023.n017.6246

Caballero-García, P., Serrano-Guerrero, J., & Oliva, D. (2023). Artificial intelligence for cybersecurity: A systematic mapping study. *Applied Sciences*, 13(3), 1462. https://doi.org/10.3390/app13031462

Capa-Sanmartín, V. I., Romero-Fernández, A. J., Cañizares-Galarza, F. P., & Machuca-Vivar, S. A. (2022). La gestión de seguridad de la información para una empresa. CIENCIAMATRIA, 8(4), 651–666. https://doi.org/10.35381/cm.v8i4.877

Conforme Tomala, J. M., Bailon Pilozo, E. D., Pilozo Pilozo, L. E., & Marcillo Merino, M. J. (2023). Medios de ataques a los sistemas de seguridad de la información. Journal TechInnovation, 2(1), 72–78. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.72-78

Cruz Lucas, G. I., Delgado Tejena, L. E., Ponce Solorzano, B. R., & Marcillo Merino, M. J. (2022b). Riesgos de seguridad de los datos en la web. Journal TechInnovation, 1(2), 43–49. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.43-49

Cruz Lucas, G. I., Figueroa Rodríguez, E. L., Cruz Lucas, N. I., & Abad Parrales, W. M. (2023). Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001. Journal TechInnovation, 2(2), 54–59. https://doi.org/10.47230/Journal.TechInnovation.v2.n2.2023.54-59

Cruz Lucas, G. I., Galarza Espinoza, R. E., Delgado De La Cruz, R. S., & Marcillo Merino, M. J. (2022a). Aplicación de protocolos SSL y TSL para él envió de información. Journal TechInnovation, 1(2), 4–9. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.4-9

Estrada Esponda, R. D., Unás Gómez, J. L., & Flórez Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos, Ciencia & Tecnología, 13(3), 98–110. https://doi.org/10.22335/rlct.v13i3.1446

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2022). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

Gómez, J., Pino, F., & Hernández, J. (2022). Security architectures for enterprise networks: A review of trends and challenges. *IEEE Access*, 10, 104563–104579. https://doi.org/10.1109/ACCESS.2022.3207249

González Hernández, I. (2023). Protección de datos y seguridad de la información. Revista Canaria de Administración Pública, 1, 285–311. https://doi.org/10.36151/RCAP.2023.9

Guaña-Moya, J. (2023). La importancia de la seguridad informática en la educación digital: retos y soluciones. RECIMUNDO, 7(1), 609–616. https://doi.org/10.26820/recimundo/7.(1).enero.2023.609-616

Intriago García, J. E., Quimis Castro, J. S., Choez García, C. A., & Marcillo Merino, M. J. (2023). Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información. Journal TechInnovation, 2(1), 79–84. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.79-84

Marcillo Merino, M. J., Cantos Plúa, J. N., Holguín Anchundia, J. C., & Vera Gutiérrez, J. A. (2023). Seguridad de información en el mundo de los negocios digitales. Journal TechInnovation, 2(1), 85–91. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.85-91

Martínez, M., Sánchez, D., & López, V. (2021). Network security monitoring in enterprise environments. *Future Internet*, 13(8), 196. https://doi.org/10.3390/fi13080196

Mendoza Enríquez, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. Revista IUS, 15(48), 179–207. https://doi.org/10.35487/rius.v15i48.2021.743

Nieto Gómez, S. G., Moreira Quimis, J. D., Mendoza Catagua, A. A., & Pinargote Gutiérrez, G. M. (2022). Sistema de seguridad con tecnología arduino para la automatización del edificio upocam. Journal TechInnovation, 1(2), 10–17. https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.10-17

Rodríguez, J., Fernández, A., & López, C. (2022). Cybersecurity risk management in enterprise networks. *Computers & Security*, 114, 102599. https://doi.org/10.1016/j.cose.2021.102599

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés