Gestio et Productio. Revista Electrónica de Ciencias Gerenciales
Año 6. Vol 6. N°11. Julio – Diciembre. 2024
Hecho el depósito de Ley: FA2019000059
ISSN: 2739-0039
INSTITUTO DE INVESTIGACIÓN Y ESTUDIOS AVANZADOS KOINONIA (IIEAK).
Santa Ana de Coro. Venezuela.

DOI 10.35381/gep.v6i11.151

Desafíos y estrategias de ciberseguridad para pequeñas empresas

Cybersecurity challenges and strategies for small businesses

Edwin Mauricio Lucio-Vásquez
edwin.lucio.00@est.ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Azuay
Ecuador
https://orcid.org/0009-0008-4308-4415

Eduardo Mauricio Campaña-Ortega
eduardo.campana@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Azuay
Ecuador
https://orcid.org/0000-0001-7720-5213

Recepción: 10 de marzo 2024
Revisado: 15 de mayo 2024
Aprobación: 15 de junio 2024
Publicado: 01 de julio 2024

Gestio et Productio. Revista Electrónica de Ciencias Gerenciales
Año 6. Vol 6. N°11. Julio – Diciembre. 2024
Hecho el depósito de Ley: FA2019000059
ISSN: 2739-0039
INSTITUTO DE INVESTIGACIÓN Y ESTUDIOS AVANZADOS KOINONIA (IIEAK).
Santa Ana de Coro. Venezuela.

RESUMEN

El objetivo general de la investigación fue describir los desafíos y estrategias de ciberseguridad para pequeñas empresas. Caso: Ferretería, Ecuador. Se adoptó un enfoque de investigación cuantitativa de alcance exploratorio para identificar las amenazas y vulnerabilidades en el ámbito de la ciberseguridad, con un énfasis particular en las (PYMEs). Se recurrió además a la tipología documental-bibliográfica. Se establecieron una serie de pasos para el análisis de vulnerabilidades de ciberseguridad. Se concluye que, es fundamental implementar actualizaciones periódicas de software, incluyendo sistemas operativos y software de seguridad, para protegerse contra las vulnerabilidades conocidas y los últimos vectores de ataque. Las empresas deben invertir en soluciones de seguridad robustas y confiables, como antivirus con licencia, para garantizar una protección efectiva contra las amenazas cibernéticas.

Descriptores: Tecnología; cibercrimen; pequeña empresa. (Tesauro UNESCO).

ABSTRACT

The overall objective of the research was to describe cyber security challenges and strategies for small businesses. Case: Hardware store, Ecuador. An exploratory quantitative research approach was adopted to identify threats and vulnerabilities in the field of cybersecurity, with a particular emphasis on (SMEs). Documentary-bibliographic typology was also used. A series of steps were established for the analysis of cybersecurity vulnerabilities. It is concluded that it is essential to implement regular software updates, including operating systems and security software, to protect against known vulnerabilities and the latest attack vectors. Businesses should invest in robust and reliable security solutions, such as licensed antivirus, to ensure effective protection against cyber threats.

Descriptors: Technology; cybercrime; small business. (UNESCO Thesaurus).

INTRODUCCIÓN

Las pequeñas empresas (Pymes) en la era digital se enfrentan a diversos desafíos en cuanto a la ciberseguridad, debido a la dependencia tecnológica para sus operaciones, así como las limitaciones de los recursos que a menudo evidencian una serie de amenazas y vulnerabilidades en sus entornos digitales. En un ambiente empresarial globalizado a nivel mundial y competitivo como el que existe en la actualidad, las pequeñas y medianas empresa, sociedades y las compañías dependen cada vez más de la tecnología específicamente de un sistema de información (Zuña Macancela et al., 2019).

En este sentido, los ciberataques y en general las vulnerabilidades relacionadas con la seguridad de la información se han hecho cada vez más comunes, en la medida que la informatización de la sociedad se consolida en los diferentes territorios mundiales (Estrada Esponda et al., 2021). De ahí la inherente necesidad de las Pymes para entender cuál es el papel de la seguridad de la información en el entorno de las pequeñas y medianas empresas en el contexto ecuatoriano. La era digital ha impactado en la forma de como las Pymes, realizan las actividades obligando adoptar un conjunto de tecnologías, sistemas y aplicaciones digitales para asegurar la continuidad competitiva en el mercado y satisfacer de esta forma las distintas necesidades y requerimientos de los clientes.

A su vez, Sanabria Rangel y Ospina Díaz (2020), abordan el tema de la seguridad en las pequeñas empresas frente a las amenazas cibernéticas, donde las Pymes reconocen el riesgo de vulneración sobre la exposición a diversas amenazas. Al respecto, Aguilar (2021) en vista de la creciente exposición de las PYMEs a esta nueva realidad, resulta crucial que los gobiernos y organismos de seguridad adopten políticas, normativas y leyes que impulsen a estas empresas a implementar mecanismos y estrategias para proteger sus sistemas, datos e información. Por otro lado, en América Latina, los principales ataques informáticos son dirigidos por malware destinados a robar información y los troyanos dirigidos a la estafa bancaria (Bustamante García, 2020). Atacando, el ciberespacio o en sistemas informáticos interconectados, así como la infraestructura que respalda dicha

información (Piñon et al., 2023). Además, la vulnerabilidad de datos se ve afectada por diferentes componentes, entre ellos se resalta el bajo nivel de seguridad que viene predeterminado en los dispositivos (Peñafiel Lucuy, 2021). Entre los delitos tipificados como ciber-delincuencia encontramos: el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos (Pons Gamon, 2017).

De acuerdo a los argumentos, se plantea como objetivo general describir los desafíos y estrategias de ciberseguridad para pequeñas empresas. Caso: Ferretería, Ecuador.

MÉTODO

En este estudio, se adoptó un enfoque de investigación cuantitativa de alcance exploratorio para identificar las amenazas y vulnerabilidades en el ámbito de la ciberseguridad, con un énfasis particular en las (PYMEs). Caso de estudio Ferretería “Las Fuentes” de la cuidad de Ibarra. Recurriendo a la tipología documental-bibliográfica, lo que permite establecer el análisis del objeto de estudio, con el propósito de describir el tema abordado (Hernández Sampieri et al., 2014).

El punto de partida implicó la revisión de la literatura académica sobre los desafíos de la seguridad cibernética en este sector, así como las estrategias y metodologías de análisis pertinentes para abordar esta problemática. Para el caso específico de se estableció una serie de pasos para el análisis de vulnerabilidades de ciberseguridad (Ver Figura 1).

Figura 1. Pasos para el análisis de vulnerabilidades de ciberseguridad.
Elaboración: Los autores.

Fase I: Definición de alcance. Donde se definió el alcance del estudio, así como las áreas de mejora de la seguridad en los sistemas, procesos y elementos dentro Ferretería “Las Fuentes”.

Fase II: Planificación. Donde se identificó los activos informáticos, plataformas de sistema operativo, redes, aplicaciones y demás recursos tecnológicos objeto de análisis de vulnerabilidades.

Fase III: Análisis de vulnerabilidades. Donde se identificó las amenazas a las que se encuentran expuesta la Ferretería “Las Fuente”, donde se evaluó las amenazas dirigidas a un servidor, fallos de origen físico o lógicos, errores del administrador, denegación de servicios, robo de equipos, entre otros aspectos de seguridad.

Fase IV: Resultados. Donde se presentan los resultados obtenidos a partir del análisis de la información recopilada en la investigación., donde se detalla una visión detallada de las amenazas y vulnerabilidades específicas identificadas en el ámbito de la ciberseguridad del caso de estudio de la Ferretería "Las Fuentes".

RESULTADOS

En el escenario empresarial actual, la ciberseguridad se ha convertido en un pilar fundamental, especialmente para las pequeñas y medianas empresas (PYMEs), que enfrentan una creciente exposición a amenazas digitales. En este contexto, llevamos a cabo un análisis de la situación de ciberseguridad en la ferretería “Las Fuentes” del cantón de Ibarra, para comprender y abordar los desafíos y estrategias de ciberseguridad para pequeñas empresas. El análisis de caso se centró en varios aspectos críticos para obtener una visión completa. Por un lado, examinamos la adopción y uso de software antivirus, evaluando cómo esta medida contribuye a mitigar los riesgos asociados con posibles ataques cibernéticos. La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación (TIC) (Hirare, 2017).

De los resultados se evidencia (Figura 2) que en la ferretería “Las Fuentes”, en la mayoría de los equipos utilizan software antivirus (61%). Mientras que el (23%) hacen uso de software gratuito. Sin embargo, es preocupante observar que un porcentaje considerable de encuestados recurre a software antivirus sin licenciamiento (4%), utilizan el antivirus con crack, infringiendo los derechos de autor, sino que también carecen de la protección necesaria para sus activos informáticos. En la actualidad, los mecanismos de defensa existentes presentan graves deficiencias, bien por la carencia de recursos y/o por la flexibilidad técnica y tecnológica (Márquez Díaz, 2019).

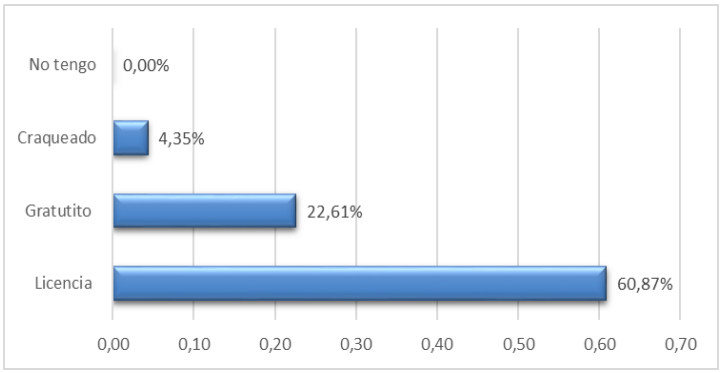

Figura 2. Utilización de software de antivirus.
Elaboración: Los autores.

El análisis revela que el 70% de los equipos cliente ha configurado la actualización del antivirus de forma automática, esta configuración es recomendada, debido que se asegura que el antivirus esté constantemente actualizado sin depender de la intervención manual. Sin embargo, a pesar de que una parte considerable de los encuestados ha optado por la actualización automática, el (14%) no actualiza su antivirus con la frecuencia recomendada y a penas el (17%) lo realiza de forma mensual ver (Figura 3). La infraestructura o equipamiento informático (servidores, equipos de red, computadores, juntamente con sus herramientas de administración), es uno de los pilares base de cualquier organización a nivel mundial. (Cando Segovia et al., 2021).

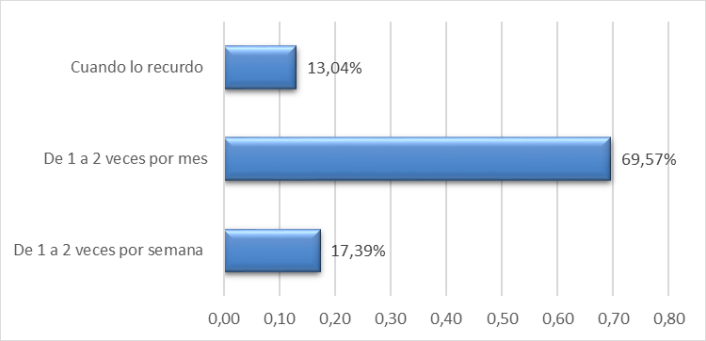

Figura 3. Proceso de actualización de antivirus.
Elaboración: Los autores.

Del análisis de los datos se determina que un pequeño número de encuestados afirmaron tener conocimiento sobre ciberseguridad (8%), hay una proporción considerable que carece de este conocimiento (13%), y una en su mayoría (78%) no respondieron la pregunta (Ver Figura 4).

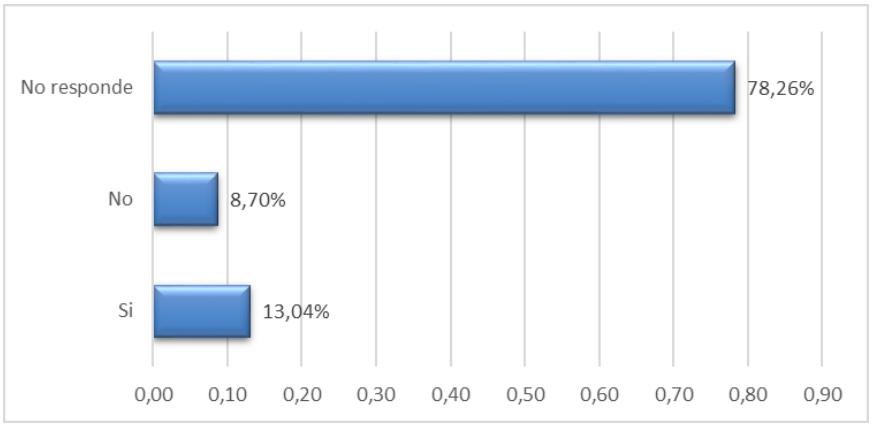

Figura 4. Conocimiento sobre ciberseguridad.
Elaboración: Los autores.

De los resultados de ataques que ha tenido la infraestructura tecnológica de la ferrería “las

Fuentes", se encontró que 4% de los encuestados manifieste tener conocimiento sobre los ataques de inyección SQL, una amenaza común para las Pymes. Sin embargo, es preocupante hay personal que no tiene nociones o conocimiento sobre los diferentes tipos de amenazas a los datos o vulnerabilidades y explotaciones de seguridad (34%). Este resultado refleja una preocupante falta de conocimiento general sobre los diferentes tipos riesgos de seguridad a los que están expuestos ver (Figura 5). La exposición a vulnerabilidades informáticas es un fenómeno que ha venido presentando gran relevancia en las organizaciones. (Sánchez Sánchez et al., 2021).

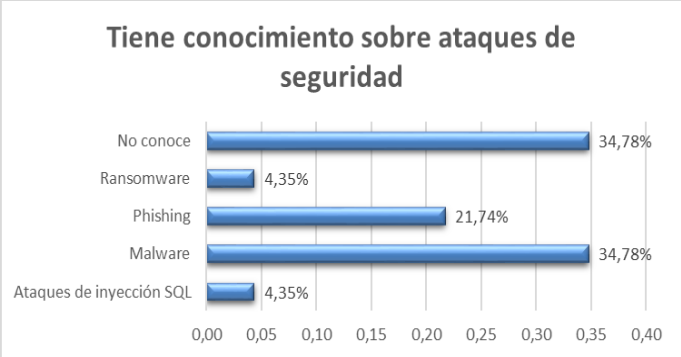

Figura 5. Conocimiento de los tipos de ataques a la seguridad de Pymes.
Elaboración: Los autores.

Del análisis de resultados sobre la situación de la formación en seguridad y la preparación de planes de contingencia se obtuvo que en el criterio de formación en ciberseguridad: Se determina que el 4% de los empleados no han tenido formación o información. Este dato resalta la necesidad de capacitar en el contexto de los riesgos de la ciberseguridad para de esta forma tener el conocimiento sobre las amenazas. En cuanto el criterio de medidas de ciberseguridad, se encontró que el 69% se limitan a la instalación de antivirus y carecen de conocimiento sobre las medidas de ciberseguridad, mientras que solo el 4% tiene un entendimiento sobre políticas (Figura 6).

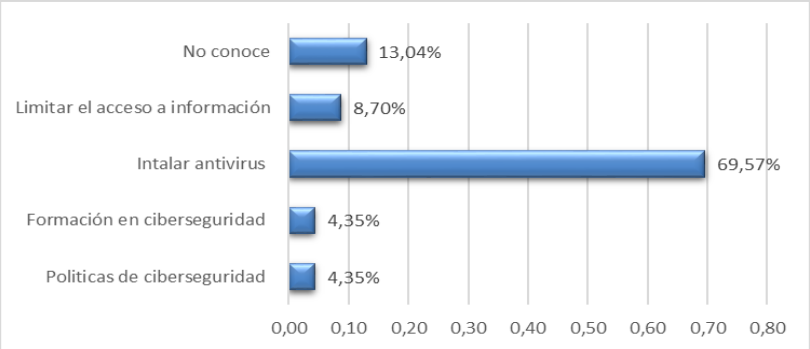

Figura 6. Medidas de ciberseguridad aplican en la Pymes.
Elaboración: Los autores.

En el ámbito de actualización de la plataforma de sistema operativo se determinó que el 54% de los equipos no realizan el proceso de actualización automática del sistema. Sin embargo, es preocupante el 21% ejecuta actualizaciones automáticas mediante licenciamiento debido a que tienen conocimiento, la falta de conciencia sobre los riesgos asociados con un sistema desactualizado y la importancia de instalar los últimos parches de seguridad (8%) (Figura 4). Para la ejecución de las pruebas de penetración se requieren múltiples recursos, herramientas, scripts, escáner de red (Coronel y Quirumbay, 2022).

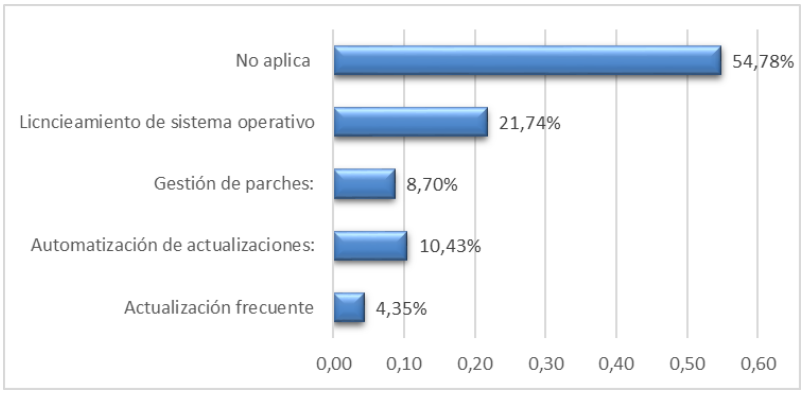

Figura 7. Proceso de actualización de plataforma de sistemas operativos.
Elaboración: Los autores.

En este orden de ideas, se observa que, si bien la mayoría de las empresas reconocen la

importancia de mantener actualizados sus sistemas operativos y software de seguridad, todavía hay una proporción significativa que no realiza actualizaciones periódicas. Esto indica una brecha en la implementación de prácticas básicas de ciberseguridad, lo que deja a esta vulnerable a posibles ataques.

En cuanto a la incidencia de ciberataques, el hecho de que aproximadamente tres cuartas partes de los empleados han experimentado algún tipo de ataque destaca la magnitud del problema. Es importante que comprendan que el riesgo siempre está presente y que deben tomar medidas proactivas para protegerse. En consecuencia, es evidente que la PYMEs necesite mejorar su postura de seguridad cibernética. Esto implica no solo aumentar el conocimiento y la conciencia sobre las amenazas cibernéticas, sino también implementar medidas preventivas adecuadas, como actualizaciones regulares de software, capacitación del personal en ciberseguridad y la elaboración de planes de contingencia ante posibles ataques. A pesar de esto, con el auge del comercio electrónico, cada vez más empresas confían en estos medios digitales para interactuar con sus clientes y realizar transacciones comerciales. Sin embargo, también es cierto que estos canales digitales presentan vulnerabilidades (Lecca Rengifo et al., 2023).

PROPUESTA

La Ferretería "Las Fuentes" es una pequeña empresa ubicada en la zona urbana de una ciudad Ibarra, lo que le ha permitido tener acceso a una base de clientes diversificada que incluye tanto consumidores individuales como pequeñas empresas locales y contratistas. El modelo de negocio está centrado en ofrecer una amplia gama de productos, herramientas, materiales de construcción, productos de plomería, electricidad, jardinería y ferretería en general. La Ferretería "Las Fuentes" cuenta con una infraestructura tecnológica que facilita las operaciones diarias mediante un sistema de punto de venta que permite gestionar las transacciones diarias y el inventario de manera eficiente. Además, tiene un sitio web que permite a los clientes realizar pedidos en línea y programar entregas

a domicilio, expandiendo así su alcance y clientes. Las operaciones administrativas y financieras se gestionan mediante software de contabilidad, lo que asegura una administración eficiente y precisa de las finanzas del negocio.

Evaluación de riesgos de ciberseguridad

La evaluación de riesgos de ciberseguridad es fundamental para la operación de las PYMEs debido a que estas dependen de tecnología para operar y almacenar información del modelo de negocio. Por lo tanto, el proceso de evaluación de los riesgos facilito identificar las amenazas potenciales, evaluar la probabilidad de que ocurran y determinar el impacto que tendrían en los activos de la organización. A continuación, se detalla los pasos involucrados en este proceso: El proceso de análisis de riesgos se inició con la identificación de los activos de información y de los recursos de TI, que forman parte del modelo de gestión de la información.

Del análisis de la seguridad de la ferretería enfrenta una serie de desafíos. Las amenazas a la seguridad que se analizaron en el estudio de caso provienen de diversos orígenes:

- Malware y virus.
- Phishing.
- Ataques de denegación de servicio (DDoS).
- Ingeniería social.
- Robo de datos.
- Dispositivos perdidos o robados.
- Acceso no autorizado.
- Fallas en la seguridad física.

Las amenazas identificadas pueden causar daños significativos por lo que fundamental analizar el riesgo, evaluar el impacto y tratar los riegos mediante controles de seguridad

para mitigar estas amenazas y proteger los activos.

Frente a los riesgos detectados se han definido las medidas de mitigación que sean efectivas, enfocadas a la mitigación tanto en la probabilidad de ocurrencia como en el impacto de cada riesgo. A continuación, se presentan las medidas específicas para cada tipo de alerta, priorizando aquellas con alta probabilidad y alto impacto (Tablas 1 a 8).

Tabla 1.
Ingeniería social.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	26.7%	2.55
Capacitación y Concienciación:	Realizar programas de formación regulares para que los empleados puedan reconocer intentos de ingeniería social.	
Simulaciones de Ingeniería Social:	Ejecutar simulaciones periódicas de ataques de ingeniería social para evaluar y mejorar la respuesta de los empleados.	
Protocolos de Verificación:	Implementar procedimientos estrictos de verificación de identidad antes de compartir información sensible o ejecutar transacciones.	

Elaboración: Los autores.

Tabla 2.
Acceso no autorizado.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	20.0%	1.75
Autenticación Multifactor (MFA):	Implementar MFA para todas las cuentas de usuario, especialmente para accesos a sistemas críticos.	
Revisión de Permisos	Realizar auditorías periódicas de los permisos de acceso para asegurar que solo los usuarios autorizados tengan acceso a los datos y sistemas necesarios	
Registro y Monitoreo de Accesos:	Implementar sistemas de registro y monitoreo para detectar y responder rápidamente a accesos no autorizados.	

Elaboración: Los autores.

Tabla 3.
Malware y virus.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	13.3%	6.83
Antivirus y Anti-Malware:	Mantener actualizado el software antivirus y anti-malware en todos los dispositivos de la organización	
Actualizaciones y Parches	Asegurar que todos los sistemas operativos y aplicaciones estén actualizados con los últimos parches de seguridad	
Educación de Usuarios:	Capacitar a los empleados sobre las mejores prácticas para evitar la descarga e instalación de software malicioso.	

Elaboración: Los autores.

Tabla 4.
Phishing.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	13.3%	6.5
Filtros de correo electrónico	Implementar soluciones avanzadas de filtrado de correo para detectar y bloquear correos electrónicos de phishing.	
Concienciación	Realizar campañas periódicas de concienciación sobre phishing y enseñar a los empleados a identificar y reportar correos sospechosos	
Simulaciones de Phishing	Llevar a cabo simulaciones de phishing para evaluar y mejorar la preparación de los empleados.	

Elaboración: Los autores.

Tabla 5.
Ataques de denegación de servicio (DDoS).

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	6.7%	7.5
Servicios de Mitigación DDoS	Contratar servicios de mitigación de DDoS de proveedores especializados para proteger la infraestructura.	
Monitoreo de Tráfico:	Implementar soluciones de monitoreo de tráfico para detectar patrones inusuales que puedan indicar un ataque DDoS.	
Planes de Respuesta	Desarrollar y probar planes de respuesta a incidentes DDoS para minimizar el impacto en caso de un ataque.	

Elaboración: Los autores.

Tabla 6.
Robo de datos.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	6.7%	3
Cifrado de Datos	Asegurar que todos los datos sensibles estén cifrados tanto en tránsito como en reposo.	
Controles de Acceso:	Implementar controles de acceso estrictos para limitar quién puede acceder a los datos sensibles.	
Auditorías de Seguridad:	Realizar auditorías de seguridad para identificar y corregir vulnerabilidades en los sistemas de almacenamiento de datos	

Elaboración: Los autores.

Tabla 7.
Dispositivos perdidos o robados.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	6.7%	2.75
Cifrado de Dispositivos	Implementar cifrado completo en todos los dispositivos móviles y portátiles	
Gestión de Dispositivos Móviles	Utilizar soluciones de MDM para monitorear, gestionar y, si es necesario, borrar remotamente los dispositivos perdidos o robados	
Políticas de Seguridad:	Establecer políticas claras para el manejo seguro de dispositivos y la respuesta ante pérdida o robo.	

Elaboración: Los autores.

Tabla 8.
Fallas en la seguridad física.

Medidas de Mitigación:	Probabilidad	Impacto Promedio
	6.7%	1
Controles de Acceso Físico	Implementar sistemas de control de acceso físico a cerraduras electrónicas, tarjetas de acceso y vigilancia por cámaras.	
Seguridad en el Sitio	Contratar personal de seguridad para monitorear y proteger las instalaciones.	
Evaluaciones de Seguridad:	Realizar evaluaciones periódicas de la seguridad física para identificar y corregir debilidades.	

Elaboración: Los autores.

La evaluación de riesgos y la implementación de medidas de mitigación son procesos continuos que deben adaptarse a medida que evolucionan las amenazas. La Ferretería "Las Fuentes" por lo que las medidas propuestas deben priorizar los esfuerzos de seguridad en función de la probabilidad y el impacto de los riesgos identificados. Al abordar los riesgos de mayor prioridad, el modelo de negocio puede fortalecer su infraestructura frente al tema de la ciberseguridad y proteger los activos de manera efectiva. La importancia de una estrategia de ciberseguridad integral que considere tanto la frecuencia como la gravedad de los riesgos potenciales, así como la capacitación constante, la implementación de tecnologías avanzadas y la adopción de políticas y procedimientos robustos son esenciales para mitigar los riesgos y mantener la seguridad de la organización.

CONCLUSIONES

Es fundamental implementar actualizaciones periódicas de software, incluyendo sistemas operativos y software de seguridad, para protegerse contra las vulnerabilidades conocidas y los últimos vectores de ataque. Las empresas deben invertir en soluciones de seguridad robustas y confiables, como antivirus con licencia, para garantizar una protección efectiva contra las amenazas cibernéticas. En este orden, se debe promover el uso de herramientas de seguridad avanzadas, como la autenticación de dos factores y el cifrado de datos, para fortalecer la protección de la información sensible.

Las PYMEs deben priorizar la capacitación y concientización del personal en ciberseguridad para aumentar la comprensión de las amenazas y fomentar una cultura de seguridad cibernética en toda la organización.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A las instituciones universitarias, por el apoyo prestado en el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Aguilar Antonio, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. [Cybersecurity challenges and opportunities in Latin America in the face of Latin America in the global context of cyber threats to national security and foreign policy security and foreign policy]. *Estudios internacionales (Santiago)*, *53*(198), 169-197. https://doi.org/10.5354/0719-3769.2021.57067

Bustamante García, S., Valles Coral, M., y Levano Rodríguez, D. (2020). Factores que contribuyen en la pérdida de información en las organizaciones. [Factors contributing to information loss in organizations]. *Revista Cubana de Ciencias Informáticas*, *14*(3), 148-164. https://n9.cl/665z3

Cando Segovia, M. R., y Medina Chicaiza, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3C TIC. [Cybersecurity prevention: focused on technological infrastructure processes. 3C ICT]. *Cuadernos de desarrollo aplicados a las TIC*, *10*(1), 17-41. https://doi.org/10.17993/3ctic.2021.101.17-41

Coronel, I., y Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. [IT security, methodologies, standards and management framework in a web application approach]. *Revista Científica y Tecnológica UPSE,* 9(2), 97-108 https://doi.org/10.26423/rctu.v9i2.672

Estrada Esponda, R., Unás Gómez, J., y Flórez Rincón, O. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. [Information security practices in times of pandemic. The case of the University of Valle, Tuluá campus]. *Revista Logos Ciencia & Tecnología*, *13*(3), 98-110. https://doi.org/10.22335/rlct.v13i3.1446

Hernández, R., Fernández, C., y Baptista, M. (2014). Metodología de la Investigación

[Investigation Methodology] (6ta. ed.). México: McGraw-Hill. https://n9.cl/t6g8vh

Hirare, C. (2017). Ciberseguridad. Presentación del dossier. [Cybersecurity. Presentation of the dossier]. *URVIO Revista Latinoamericana de Estudios de Seguridad,* (20), 8-15. https://doi.org/10.17141/urvio.20.2017.2859

Lecca Rengifo, L., Paz Medrano, H., y Mendoza de los Santos, A. (2023). Medidas de control interno para preservar la seguridad de los datos dentro de las empresas e-commerce: Una revisión sistemática. [Internal control measures for preserving data security within e-commerce companies: A systematic review]. *Revista Ciencia, Tecnología e Innovación*, *21*(27), 23-34. https://doi.org/10.56469/rcti.v21i27.881

Márquez Díaz, J. (2019). Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. [Risks and vulnerabilities of distributed denial of service in the internet of things]. *Revista de Bioética y Derecho*, (46), 85-100. https://n9.cl/lx5ic

Ospina Díaz, M., y Sanabria Rangel, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. [National challenges to cybersecurity on the global stage: an analysis for Colombia]. *Revista Criminalidad*, *62*(2), 199-217. https://n9.cl/z67mv

Peñafiel Lucuy, K. (2021). Factores que determinan la Vulneración Informática y el Desarrollo de una aplicación móvil para concientizar sobre los Impactos en los Activos. [Factors Determining Computer Vulnerability and the Development of a Mobile Application to Raise Awareness of Asset Impacts]. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, *21*(21), 143-172. https://n9.cl/hvwc0

Piñón, L., Sapién, A., y Gutiérrez, M. (2023). Capacitación en ciberseguridad en una empresa mexicana. [Cybersecurity training in a Mexican Company]. *Información tecnológica*, *34*(6), 43-52. https://dx.doi.org/10.4067/S0718-07642023000600043

Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. [Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cybersecurity]. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Sánchez Sánchez, P., García González, J., Triana, A., y Pérez Coronell, L. (2021). Medida

del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. [Measuring the level of IT security of small and medium-sized enterprises (SMEs) in Colombia]. *Información tecnológica*, *32*(5), 121-128. https://dx.doi.org/10.4067/S0718-07642021000500121

Zuña Macancela, E. R., Arce Ramírez, Á., A., Romero Berrones, W. J., y Soledispa Baque, C. J. (2019). Análisis de la seguridad de la información en las Pymes de la ciudad de Milagro. [Analysis of information security in SMEs in the city of Milagro]. *Universidad y Sociedad,* 11(4), 487-492. https://n9.cl/7qqf1