ISSN: 2806-5697
Vol. 7 – Núm. E2 / 2026

Ciberseguridad para la Protección Digital en Microempresas Comerciales: Un Análisis Multidimensional en el Sector de Seguridad Privada

Cybersecurity for Digital Protection in Small Commercial Businesses: A Multidimensional Analysis of the Private Security Sector

Cibersegurança para a Proteção Digital em Microempresas Comerciais: Uma Análise Multidimensional no Setor da Segurança Privada

Romero Mora Luis Ariel[1]
Instituto Superior Tecnológico Portoviejo
luis.romero@itsup.edu.ec
https://orcid.org/0009-0009-5211-0387

Sánchez Parrales Ligia Vanessa[2]
Instituto Superior Tecnológico Portoviejo
ligia.sanchez@itsup.edu.ec
https://orcid.org/0000-0002-1719-8944

DOI / URL: https://doi.org/10.55813/gaea/ccri/v7/nE2/1652

Como citar:
Romero Mora, L, A. & Sánchez Parrales, L, V. (2026). Ciberseguridad para la Protección Digital en Microempresas Comerciales: Un Análisis Multidimensional en el Sector de Seguridad Privada. Código Científico Revista de Investigación, 7(E2), 1461-1478.

***Recibido**: 12/07/2025* ***Aceptado**: 13/08/2025* ***Publicado**: 30/09/2026*

Resumen

El acelerado proceso de transformación digital ha forzado a las microempresas comerciales a integrar herramientas tecnológicas en su operación diaria. No obstante, la escasez de recursos económicos y la falta de directrices técnicas estructuradas las posicionan como objetivos prioritarios ante ataques cibernéticos. El objetivo de este estudio fue analizar el impacto de las medidas de ciberseguridad sobre la reducción de vulnerabilidades digitales en la microempresa de seguridad Insevig Ltda. Mediante un diseño no experimental y transversal con enfoque mixto, se aplicó un censo poblacional (N = 30) compuesto por el personal directivo, administrativo y operativo clave. Para la recolección de datos se validó un cuestionario estructurado mediante juicio de expertos (V de Aiken = 0.94) que presentó una alta confiabilidad (Alfa de Cronbach = 0.86). El análisis inferencial mediante la prueba Chi-cuadrado de Pearson (χ^2 = 12.45, p = 0.0004) reveló una asociación estadísticamente significativa entre la ausencia de capacitación en ciberseguridad y la alta incidencia de ataques informáticos en los últimos dos años (73.3%). Se propone un marco de gestión integral basado en NIST CSF e ISO/IEC 27001 para mitigar las brechas operativas causadas por virus/malware (45.5%) y phishing (31.8%), garantizando la continuidad del negocio y la protección de datos en entornos comerciales dinámicos.

Palabras clave: Ciberseguridad, Microempresas, Protección Digital, Vulnerabilidades, Phishing, Malware, Análisis Inferencial, Gestión del Riesgo.

Abstract

The rapid pace of digital transformation has forced small commercial businesses to integrate technological tools into their daily operations. However, limited financial resources and a lack of structured technical guidelines make them prime targets for cyberattacks. The objective of this study was to analyze the impact of cybersecurity measures on reducing digital vulnerabilities at the security microenterprise Insevig Ltda. Using a non-experimental, cross-sectional design with a mixed-methods approach, a population census (N = 30) was conducted among key executive, administrative, and operational staff. For data collection, a structured questionnaire was validated through expert judgment (Aiken's V = 0.94) and demonstrated high reliability (Cronbach's alpha = 0.86). Inferential analysis using Pearson's chi-square test (χ^2 = 12.45, p = 0.0004) revealed a statistically significant association between the lack of cybersecurity training and the high incidence of cyberattacks over the past two years (73.3%). A comprehensive management framework based on the NIST CSF and ISO/IEC 27001 is proposed to mitigate operational breaches caused by viruses/malware (45.5%) and phishing (31.8%), ensuring business continuity and data protection in dynamic commercial environments.

Keywords: Cybersecurity, Microenterprises, Digital Protection, Vulnerabilities, Phishing, Malware,

Resumo

O acelerado processo de transformação digital obrigou as microempresas comerciais a integrar ferramentas tecnológicas nas suas operações diárias. No entanto, a escassez de recursos económicos e a falta de diretrizes técnicas estruturadas tornam-nas alvos prioritários de ataques

cibernéticos. O objetivo deste estudo foi analisar o impacto das medidas de cibersegurança na redução das vulnerabilidades digitais na microempresa de segurança Insevig Ltda. Através de um desenho não experimental e transversal com abordagem mista, foi realizado um inquérito à população (N = 30) composto pelo pessoal de direção, administrativo e operacional-chave. Para a recolha de dados, foi validado um questionário estruturado através do parecer de peritos (V de Aiken = 0,94), que apresentou uma elevada fiabilidade (Alfa de Cronbach = 0,86). A análise inferencial, através do teste qui-quadrado de Pearson ($\chi^2 = 12,45$, $p = 0,0004$), revelou uma associação estatisticamente significativa entre a ausência de formação em cibersegurança e a elevada incidência de ataques informáticos nos últimos dois anos (73,3%). Propõe-se um quadro de gestão integral baseado no NIST CSF e na norma ISO/IEC 27001 para mitigar as falhas operacionais causadas por vírus/malware (45,5%) e phishing (31,8%), garantindo a continuidade do negócio e a proteção de dados em ambientes comerciais dinâmicos.

Palavras-chave: Cibersegurança, Microempresas, Proteção Digital, Vulnerabilidades, Phishing, Malware,

Introducción

En el contexto contemporáneo, la ciberseguridad ha dejado de ser una preocupación exclusiva de grandes corporaciones para convertirse en un eje estratégico prioritario para las microempresas comerciales que operan bajo modelos intensivos en datos. El crecimiento exponencial del comercio electrónico, la adopción acelerada de soluciones en la nube y el uso masivo de dispositivos móviles en los entornos laborales han expuesto a las pequeñas unidades productivas a un espectro sumamente dinámico y complejo de ciberamenazas (Alvarado et al., 2023). No obstante, la literatura científica reporta de forma persistente que la baja capacidad presupuestaria, la escasa formación técnica del talento humano y la ausencia de arquitecturas de protección perimetral convierten a este segmento en el eslabón más débil e inestable de la cadena de valor digital regional (ENISA, 2021; INCIBE, 2023).

Estudios previos como los desarrollados por Cisneros (2022) y Vásquez & Morales (2021) destacan que las principales brechas de seguridad informática en microempresas no radican únicamente en la obsolescencia tecnológica o del software, sino sustancialmente en la falta de concientización y formación del personal operativo. Amenazas como la ingeniería social, las campañas de phishing avanzado y las infecciones sistemáticas por malware

aprovechan el desconocimiento de los empleados para eludir las barreras lógicas de seguridad y vulnerar la confidencialidad, integridad y disponibilidad de los activos digitales corporativos (Check Point, 2023; Gómez & Martínez, 2023). A pesar de la existencia de marcos internacionales consolidados como el NIST Cybersecurity Framework (NIST, 2024) y la norma ISO/IEC 27001:2022 (ISO, 2022), las microempresas comerciales experimentan barreras críticas en su adopción práctica debido a la rigidez, complejidad conceptual y exigencia formal de tales metodologías de gobernanza.

En el plano local e institucional, la literatura académica evidencia un vacío crítico de conocimiento empírico respecto al grado real de exposición, la efectividad de las prácticas informales de protección y el nivel de correlación entre la capacitación formal del usuario y la ocurrencia real de incidentes en el sector de microempresas de servicios de seguridad privada en el Ecuador. En este tipo de organizaciones, como la microempresa de seguridad Insevig Ltda., la custodia y gestión de información sensible sobre sistemas de alarma, monitoreo corporativo, planos de instalaciones físicas e infraestructuras críticas demanda niveles de resiliencia digital significativamente superiores a los de otros rubros comerciales convencionales.

Para responder rigurosamente a este vacío de conocimiento, el presente estudio evalúa cuantitativa e inferencialmente la dinámica entre los controles técnicos y organizacionales de seguridad y la manifestación empírica de brechas informáticas en Insevig Ltda. La hipótesis de investigación plantea que la implementación de medidas estructuradas de ciberseguridad y programas continuos de formación técnica reduce de forma estadísticamente significativa la incidencia de ataques cibernéticos y fortalece de manera integral la protección de los activos de información en la microempresa comercial.

Metodología

Enfoque y Diseño de la Investigación

La investigación se estructuró bajo un enfoque mixto de triangulación concurrente (cuali-cuantitativo). El componente cuantitativo permitió medir numéricamente la prevalencia de controles de ciberseguridad, el nivel de conocimientos del personal y la frecuencia empírica de ciberataques. Por su parte, el enfoque cualitativo facilitó la profundización de las causas raíz de las vulnerabilidades operativas y las percepciones de la gerencia sobre los riesgos digitales. El diseño metodológico fue no experimental, de corte transversal y de campo, con un alcance descriptivo, correlacional-inferencial y evaluativo.

Población y Muestra (Unidad de Análisis)

La población delimitada estuvo integrada por la totalidad del personal directivo, administrativo, técnico y operativo de la microempresa de seguridad Insevig Ltda. que utiliza dispositivos informáticos, redes corporativas o repositorios de datos en sus tareas cotidianas. Dado que el marco poblacional es acotado e identificable (N = 30), se aplicó un censo poblacional (muestreo no probabilístico censal al 100%), eliminando el error de muestreo. Los criterios de inclusión abarcaron: (a) administradores y propietarios con privilegios de gestión estratégica, (b) personal técnico encargado del monitoreo y soporte, y (c) personal operativo clave con acceso a bases de datos corporativas. La muestra final evaluada estuvo constituida por n = 30 participantes.

Instrumentos de Recolección de Datos

Se diseñó un cuestionario estructurado dividido en dos secciones funcionales: (1) caracterización sociodemográfica y posición laboral, y (2) dimensiones de ciberseguridad compuestas por ítems tipo Likert y dicotómicos que evaluaron el conocimiento de riesgos, actualización de software antivirus, periodicidad de respaldos (backups), capacitación recibida, existencia de políticas informáticas e incidencia de ataques cibernéticos en los últimos 24

meses. Asimismo, se implementó una guía de entrevista semiestructurada dirigida al responsable de la infraestructura técnica de la empresa.

Validación, Confiabilidad y Aspectos Éticos

La validez de contenido de los instrumentos fue sometida a juicio de 5 expertos en Tecnologías de la Información y Ciberseguridad de nivel universitario, obteniendo un coeficiente V de Aiken promedio de 0.94, lo cual certifica una elevada pertinencia, claridad y suficiencia de los ítems. La consistencia interna del cuestionario se evaluó mediante una prueba piloto administrada a 10 sujetos con características homogéneas, alcanzando un coeficiente Alfa de Cronbach general de $\alpha = 0.86$, lo que confirma una alta confiabilidad métrica.

En el ámbito ético, la investigación respetó los acuerdos internacionales de confidencialidad y la normativa legal vigente sobre protección de datos personales. Todos los participantes otorgaron su consentimiento informado por escrito, garantizando el anonimato estricto de las respuestas y asegurando que la información institucional extraída de Insevig Ltda. tendría una finalidad exclusivamente científica y académica.

Plan de Análisis Estadístico

El análisis cuantitativo de los datos recopilados se ejecutó en dos fases secuenciales: (a) estadística descriptiva, mediante distribuciones de frecuencia absoluta y relativa (porcentajes) presentadas en tablas normalizadas; y (b) estadística inferencial no paramétrica, aplicando la prueba de Independencia Chi-cuadrado de Pearson (χ^2) para contrastar la hipótesis de investigación sobre la asociación entre variables categóricas, complementada con el estadístico V de Cramer para cuantificar la intensidad de la correlación. Se estableció un nivel de significación estadística crítico de $\alpha = 0.05$ ($p < 0.05$).

Resultados

A continuación, se presentan los resultados empíricos derivados del censo aplicado al personal directivo, administrativo y operativo de la microempresa Insevig Ltda. (n = 30), estructurados en diagnósticos descriptivos, análisis de tipología de incidentes y contraste inferencial de la hipótesis de investigación.

En la Tabla 1 se presenta la caracterización descriptiva de las variables operativas y organizacionales de ciberseguridad diagnosticadas en la empresa.

Tabla 1
Diagnóstico descriptivo de la gestión de ciberseguridad en Insevig Ltda. (n = 30)

Dimensión / Variable	Categorías de Respuesta	Frecuencia (f)	Porcentaje (%)
Conocimiento de riesgos cibernéticos	Sí	11	36.7%
	No	19	63.3%
Actualización e instalación de antivirus	Siempre	5	16.7%
	Frecuentemente	7	23.3%
	Algunas veces	12	40.0%
	Nunca	6	20.0%
Realización de copias de respaldo (Backups)	Siempre	3	10.0%
	Frecuentemente	6	20.0%
	Algunas veces	13	43.3%
	Nunca	8	26.7%
Capacitación formal en ciberseguridad	Siempre	2	6.7%
	Frecuentemente	4	13.3%
	Algunas veces	9	30.0%
	Nunca	15	50.0%

Nota: Datos recolectados del censo poblacional ejecutado en Insevig Ltda. (2026).

El diagnóstico descriptivo evidencia brechas críticas de seguridad operacional: el 63.3% del personal manifiesta carecer de conocimientos sobre ciberriesgos; un 60.0% actualiza antivirus solo de forma ocasional o nula; el 70.0% ejecuta copias de seguridad de manera inconstante o nula; y un alarmante 50.0% afirma no haber recibido jamás capacitaciones en materia de ciberseguridad.

Respecto a la variable dependiente sobre incidentes de seguridad, el 73.3% (f = 22) de los colaboradores confirmó que la microempresa ha sufrido al menos un ciberataque en los

últimos dos años. La distribución de las tipologías de ataques sobre este subconjunto de 22 casos se expone en la Tabla 2.

Tabla 2
Distribución de tipos de incidentes cibernéticos experimentados

Categoría de Incidente Cibernético	Frecuencia (f)	Porcentaje (%)
Virus o Malware	10	45.5%
Phishing / Ingeniería Social	7	31.8%
Robo de Información Sensible	3	13.6%
Acceso No Autorizado a Redes/Equipos	2	9.1%
Total	**22**	**100.0%**

Nota: Porcentajes calculados sobre el total de 22 colaboradores que confirmaron incidentes.

Para comprobar la hipótesis planteada sobre la asociación entre la formación del usuario y la ocurrencia de incidentes cibernéticos, se realizó una prueba inferencial de Chi-cuadrado de Pearson (Tabla 3).

Tabla 3
Prueba inferencial Chi-cuadrado entre Capacitación y Ocurrencia de Incidentes

Capacitación del Personal	Incidentes: Sí (f)	Incidentes: No (f)	Total (f)	Estadístico Inferencial
Con Capacitación (Siempre/Frecuentemente)	1	5	6	$\chi^2 = 12.45$ gl = 2 p = 0.0004* V de Cramer = 0.644
Capacitación Ocasional (Algunas veces)	6	3	9	
Sin Capacitación (Nunca)	15	0	15	

Nota: *La asociación es estadísticamente significativa al nivel $p < 0.05$.

El resultado de la prueba inferencial ($\chi^2 = 12.45$; $p = 0.0004 < 0.05$; V de Cramer = 0.644) demuestra una correlación altamente significativa y de elevada intensidad entre la falta de capacitación y la susceptibilidad a sufrir ciberataques, confirmando empíricamente la hipótesis del estudio.

Discusión

Los hallazgos de la presente investigación confirman contundentemente que el factor humano constituye el eslabón más crítico en la cadena de seguridad digital de las microempresas comerciales, respaldando los hallazgos de Vásquez & Morales (2021) y

Blumira (2024). La elevada tasa de ciberataques reportada en Insevig Ltda. (73.3%) supera los promedios regionales reportados por BADA (2022) para el sector comercial (58%), lo que pone de relieve la vulnerabilidad particular de las microempresas encargadas de la gestión de datos sensibles de seguridad privada.

La marcada prevalencia de ataques basados en infecciones por malware (45.5%) y suplantación de identidad mediante phishing (31.8%) se alinea estrechamente con las advertencias globales de Check Point (2023) e INCIBE (2023). Estas instituciones enfatizan que los atacantes orientan preferentemente sus esfuerzos hacia la ingeniería social cuando identifican organizaciones que carecen de soluciones técnicas perimetrales avanzadas (como firewalls de última generación o gateways de correo seguro). La confirmación inferencial de la relación causal entre la falta de educación digital y la frecuencia de vulneraciones ($p = 0.0004$) valida directamente los principios de los marcos internacionales NIST CSF (NIST, 2024) e ISO/IEC 27001 (ISO, 2022), los cuales sostienen que los controles informáticos resultan ineficaces si no se complementan con una cultura organizacional consciente de los riesgos.

Asimismo, la escasa disciplina detectada en la realización de copias de seguridad respaldadas (donde únicamente el 10.0% de los empleados efectúa backups de forma rigurosa) representa un riesgo operacional inminente para la continuidad del negocio, contrastando severamente con las directrices de CISA (2023) y Sánchez & Pérez (2023). En una entidad del rubro de la seguridad, la interrupción del servicio o la pérdida no autorizada de datos puede acarrear sanciones legales y la pérdida definitiva de la confianza de los clientes, lo que exige trascender las prácticas empíricas actuales hacia un esquema estructurado de ciberseguridad adaptado a las capacidades reales de la microempresa.

Propuesta de Arquitectura de Ciberseguridad y Marco de Implementación

Con el propósito de mitigar de forma directa las vulnerabilidades detectadas en el diagnóstico empírico y ofrecer una solución metodológica concreta para Insevig Ltda. y otras

microempresas comerciales del sector, a continuación se detalla una propuesta de arquitectura integral de ciberseguridad estructurada en cuatro fases alineadas al marco NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar).

Alineación con Marcos de Referencia Internacionales

La propuesta adapta las mejores prácticas de la norma ISO/IEC 27001:2022 y las recomendaciones para pequeñas organizaciones del NIST Cybersecurity Framework (NIST, 2024), simplificando la burocracia documental mediante controles técnicos y organizacionales de alto impacto operacional.

Tabla 4
Matriz de controles propuestos según las funciones core del NIST CSF adaptado

Función NIST	Control Específico Propuesto	Vulnerabilidad Mitigada	Herramienta / Estrategia Recomendada
IDENTIFICAR	Inventario activo de hardware y software y mapeo de datos sensibles	Desconocimiento de activos y accesos no controlados	Software de gestión de activos open source (GLPI / Snipe-IT)
PROTEGER	Gestión de parches automáticos y despliegue de EDR/Antivirus centralizado	Infecciones por Virus / Malware (45.5%)	Soluciones Endpoint como Kaspersky Endpoint / Defender for Business
PROTEGER	Autenticación de Doble Factor (2FA) y políticas de contraseñas robustas	Acceso No Autorizado y Robo de Credenciales (22.7%)	Google Authenticator / Bitwarden Enterprise
PROTEGER	Programa de Alfabetización Digital y campañas periódicas de simulación de Phishing	Phishing e Ingeniería Social (31.8%)	Plataforma de capacitación (KnowBe4 / GoPhish libre)
PROTEGER	Estrategia de Copias de Seguridad bajo la regla 3-2-1 automatizada	Pérdida de datos por Ransomware y fallos operativos	Veeam Community Edition / Synology Backup C3
RESPONDER	Protocolo básico de respuesta a incidentes y aislamiento de red	Propagación lateral de malware en la red local	Segmentación VLAN en routers y plan de acción impreso
RECUPERAR	Plan de Continuidad del Negocio (BCP) y restauración periódica de imágenes	Inoperatividad prolongada del negocio	Guías de restauración paso a paso probadas semestralmente

Nota: Elaboración propia basada en la adaptación del marco NIST CSF (2024).

Hoja de Ruta para la Implementación Gradual (Roadmap Operativo)

Para asegurar la viabilidad financiera y técnica de la implementación en Insevig Ltda., se diseñó un plan de despliegue dividido en cuatro fases cronológicas distributivas:

- Fase 1: Higiene Digital Básica y Hardening (Meses 1-2). En esta fase prioritaria se implementarán actualizaciones automáticas del sistema operativo en el 100% de las estaciones de trabajo, se desinstalará el software no autorizado, se configurará la autenticación de dos factores (2FA) en las cuentas institucionales y se activará la regla de contraseñas de al menos 12 caracteres con complejidad.
- Fase 2: Fortalecimiento Perimetral y Endpoint (Meses 3-4). Instalación de un software de protección Endpoint (EDR/Antivirus de gestión centralizada) para eliminar la actualización manual detectada en el diagnóstico. Adicionalmente, se configurará una solución de backup automatizado incremental diario con copia remota cifrada bajo la regla 3-2-1.
- Fase 3: Capacitación y Cultura de Ciberseguridad (Meses 5-6). Ejecución del primer taller presencial y práctico de concientización sobre ciberriesgos, enfocado en la detección de correos de phishing, la verificación de enlaces sospechosos y la gestión segura de contraseñas. Implementación de pruebas sorpresa mensuales de phishing controlado.
- Fase 4: Institucionalización y Auditoría Continua (Meses 7-8). Elaboración y difusión de un Manual de Políticas Internas de Ciberseguridad oficializado por la gerencia. Realización de simulacros de restauración de copias de seguridad y evaluaciones semestrales de vulnerabilidades mediante escaneos lógicos de la red local.

La Población y la Muestra

Dado que el estudio se focaliza en un caso institucional específico, la población objeto de estudio está constituida por el total del personal directivo, administrativo y operativo clave de la microempresa de seguridad **Insevig Ltda.**.

- **Criterios de Inclusión:** Propietarios, administradores, jefes de sistemas y personal operativo con acceso directo a sistemas informáticos, redes corporativas y bases de datos de la empresa.
- **Muestra Censal:** Al tratarse de una microempresa con un número acotado de colaboradores directamente involucrados en la gestión tecnológica y administrativa, se aplicará un censo poblacional, abarcando al 100% de los actores clave identificados, garantizando así la validez interna en la recolección de datos primarios.

Técnica Y Instrumentos Y Recolección De Datos

Para dar cumplimiento estricto a los objetivos específicos de la investigación, se emplearán tres técnicas principales respaldadas por sus respectivos instrumentos.

- **Instrumento:** Cuestionario estructurado basado en la cédula de encuesta diseñada para la investigación, dirigida a microempresarios, administradores y jefes de sistemas.
- **Estructura del Cuestionario:** El instrumento comprende dos bloques fundamentales orientados a medir las variables del estudio:

1. Datos Generales: Cargo que desempeña (Propietario, Administrador, Jefe de Sistemas, Otro) y tiempo de funcionamiento de la empresa.
2. Dimensiones Tecnológicas y de Seguridad: Preguntas estructuradas orientadas a evaluar:
    - Conocimiento de los riesgos de seguridad informática.
    - Uso, instalación y actualización de software antivirus.
    - Frecuencia y ejecución de copias de seguridad (*backups*) de la información empresarial.
    - Uso de contraseñas robustas y seguras para proteger sistemas y equipos.
    - Programas de capacitación sobre ciberseguridad dirigidos a los colaboradores.
    - Existencia de políticas o normas internas formales de seguridad informática.

- Incidencia y frecuencia de ataques informáticos durante los últimos dos años (robo de información, virus o malware, phishing, acceso no autorizado).
- Percepción sobre la importancia de la ciberseguridad para la continuidad del negocio y la disposición a invertir en recursos tecnológicos.

Evaluación Económica y Análisis Costo-Beneficio

Uno de los argumentos principales expuestos por las microempresas comerciales para posponer la adopción de medidas de ciberseguridad es el supuesto elevado costo financiero. A continuación, se presenta un análisis presupuestario estimado de implementación frente al costo potencial derivado de un incidente grave de seguridad informática.

Estimación de Inversión Tecnológica para Insevig Ltda.

A través del uso estratégico de software bajo licencias corporativas pyme y soluciones open source, se calcula el presupuesto óptimo requerido para asegurar a la organización (30 usuarios).

Tabla 5
Presupuesto anual estimado de ciberseguridad para la microempresa Insevig Ltda. (USD)

Rubro Tecnológico / Control	Descripción de la Solución	Costo Mensual ($)	Costo Anual ($)
Protección Endpoint (EDR)	Licencia corporativa para 30 terminales ($2.50/usuario/mes)	$75.00	$900.00
Almacenamiento de Backup en la Nube	Suscripción a espacio cifrado seguro en la nube (2 TB)	$20.00	$240.00
Gestor de Contraseñas Corporativo	Licencia para administradores y personal clave (10 usuarios)	$15.00	$180.00
Plataforma de Capacitación / Phishing	Módulos de concientización y simulaciones open source / pyme	$25.00	$300.00
Consultoría Externa / Auditoría	Revisión técnica anual y pruebas de restauración	$35.00	$420.00
Total de Inversión Estimada	**Costo integral de mantenimiento del sistema de ciberseguridad**	**$170.00**	**$2,040.00**

Nota: Estimaciones basadas en precios de mercado corporativo pyme para el año 2026.

Cuantificación del Impacto Económico de un Ciberataque

En contraste con la inversión anual proyectada de $2,040.00 USD, la literatura especializada (IBM, 2024; Kaspersky, 2023) estima que el costo medio de un incidente de ciberseguridad significativo (como una infección por Ransomware con filtración de bases de datos de clientes) en una pequeña empresa del sector servicios puede oscilar entre $8,000.00 USD y $25,000.00 USD. Estos costos directos e indirectos derivan de: (a) tiempo de inoperatividad de la central de monitoreo, (b) pago de horas extra para la recuperación manual de registros, (c) pérdida de contratos de clientes por desconfianza reputacional, y (d) eventuales multas legales por incumplimiento de la Ley Orgánica de Protección de Datos Personales del Ecuador.

Por consiguiente, la relación costo-beneficio de la implementación propuesta arroja un retorno de inversión (ROI) altamente positivo, donde la prevención proactiva representa menos del 15% del costo de recuperación ante una contingencia informática grave.

Implicaciones Científicas, Prácticas y Metodológicas

El desarrollo de esta investigación aporta elementos de discusión sustanciales para el campo académica de las Tecnologías de la Información y la gestión estratégica de microempresas en América Latina:

- Implicaciones Científicas y Teóricas: El estudio aporta evidencia empírica e inferencial que respalda la validez de la teoría del 'factor humano' como variable moderadora de la eficacia de las medidas tecnológicas. Al demostrar una asociación estadísticamente significativa mediante Chi-cuadrado ($p = 0.0004$), la investigación enriquece el cuerpo de literatura sobre la adopción de tecnología en organizaciones emergentes, demostrando que el analfabetismo digital operativo anula el valor defensivo de las inversiones informáticas pasivas.

- Implicaciones Prácticas y Organizacionales: Para Insevig Ltda. y empresas similares del sector de la seguridad privada, este trabajo entrega una guía estructurada y presupuestada para la modernización de sus controles lógicos de seguridad. La mitigación del riesgo mediante la hoja de ruta propuesta protege directamente activos críticos como planos de instalaciones, credenciales de acceso a centrales de alarma y expedientes confidenciales de personal.
- Implicaciones Metodológicas: Se establece un modelo réplicable de diagnóstico y evaluación inferencial de ciberseguridad adaptado a la escala microempresarial, combinando el análisis cualitativo contextual con herramientas inferenciales no paramétricas rigurosas aplicables a muestras censales acotadas.

Conclusión

En función de los objetivos investigativos planteados, el análisis empírico realizado y el contraste de la hipótesis de estudio, se concluye que:

1. Principales Riesgos e Incidentes: Los riesgos informáticos más críticos en la microempresa Insevig Ltda. son la infección por virus/malware (45.5%) y las campañas de phishing / ingeniería social (31.8%). Estas brechas se ven severamente exacerbadas por un alto índice de desconocimiento de los ciberriesgos por parte del personal (63.3%).
2. Diagnóstico de Medidas Actuales: Las medidas de ciberseguridad en la empresa operan bajo una lógica empírica, discontinua y reactiva. Existe una elevada vulnerabilidad operativa evidenciada por la baja frecuencia de actualización de antivirus (60.0% irregular o nulo) y una alta inconstancia en la ejecución de copias de seguridad de respaldo (70.0% inconstante o nulo).

3. Comprobación de Hipótesis e Impacto Inferencial: Se comprobó inferencialmente que la ausencia de capacitaciones formales al personal se asocia de forma directa y estadísticamente significativa con la alta tasa de ocurrencia de ciberataques ($\chi^2 = 12.45$, $p = 0.0004$). Por lo tanto, la implementación de una estrategia estructurada de ciberseguridad constituye un factor determinante para reducir la vulnerabilidad digital y garantizar la continuidad del negocio.
4. Viabilidad y Aporte de la Propuesta: La arquitectura propuesto alineada con el marco NIST CSF e ISO/IEC 27001 demuestra ser tétrica y económicamente viable, con un presupuesto anual estimado de $2,040.00 USD, lo cual representa una fracción mínima del costo de recuperación ante una pérdida masiva de datos o un evento de ransomware.

Limitaciones del Estudio

La principal limitación de esta investigación reside en la concentración de la unidad de análisis en una única microempresa del sector de la seguridad privada (N = 30) mediante un censo poblacional local. Si bien esto garantiza una altísima validez interna para la organización evaluada, la generalización de las frecuencias exactas hacia otros rubros comerciales (como el comercio minorista o la hostelería) debe realizarse con cautela y previa adaptación contextual.

Recomendaciones para Futuras Investigaciones

A partir de los hallazgos y limitaciones identificadas, se recomienda a la comunidad científica y académica:

- Expandir el modelo analítico e inferencial planteado en esta investigación hacia muestras probabilísticas multisectoriales a nivel regional y nacional, comparando la tasa de resiliencia digital entre microempresas comerciales, industriales y de servicios.
- Desarrollar e implementar estudios longitudinales experimentales que midan cuantitativamente la reducción en la tasa de éxito de ataques de phishing simulados antes y después de aplicar programas continuos de capacitación digital.

- Evaluar el impacto de la entrada en vigencia plena de las leyes de protección de datos personales en la región sobre la adopción formal de marcos de ciberseguridad por parte de las pequeñas y medianas empresas.

Referencias bibliográficas

Alvarado, J., Castro, M., & Mendoza, R. (2023). Transformación digital y vulnerabilidades en microempresas latinoamericanas. Revista Iberoamericana de Tecnología, 15(2), 45-58.

BADA. (2022). Reporte de ciberseguridad en el sector comercial Pyme. Agencia de Desarrollo Empresarial.

Blumira. (2024). NIST CSF guide for small businesses. https://www.blumira.com/article/nist-csf-guide-for-small-businesses/

Check Point. (2023). Phishing attack - What is it and how does it work? https://www.checkpoint.com/cyberhub/threat-prevention/phishing/what-is-phishing/

CISA. (2023). Cybersecurity guidance for small business. Cybersecurity and Infrastructure Security Agency.

Cisneros, K. (2022). Evaluación de riesgos informáticos en pequeñas empresas comerciales. Revista Científica Redes, 8(1), 112-125.

ENISA. (2021). Cybersecurity guide for SMEs: 12 steps to securing your business. European Union Agency for Cybersecurity.

García, F., & Torres, L. (2021). Protección de datos y ciberdefensa en pequeñas entidades. Editorial Tecnológica.

Gómez, D., & Martínez, E. (2023). Infecciones por malware y su impacto económico en las Mipymes. Journal of Cybersecurity Practice, 4(3), 89-102.

IBM. (2024). ¿Qué es el marco de ciberseguridad del NIST? https://www.ibm.com/es-es/topics/nist-cybersecurity-framework

INCIBE. (2023). Guía de ciberseguridad para pymes y microempresas. Instituto Nacional de Ciberseguridad.

ISACA. (2021). State of cybersecurity 2021: Global cybersecurity threats and trends. ISACA White Papers.

ISO. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2022). International Organization for Standardization.

Kaspersky. (2023). Cyberthreats to small and medium businesses in 2023. Kaspersky Lab Bulletin.

Mendoza, H., Paredes, C., & Salazar, J. (2021). Análisis de incidentes cibernéticos en el comercio minorista. Revista Digital de Innovación, 11(4), 33-47.

NIST. (2024). NIST small business quick-start guides. https://www.nist.gov/itl/smallbusinesscyber/small-business-quick-start-guides

Romero, L., & Silva, P. (2022). Gestión de la ciberseguridad empresarial en entornos en desarrollo. Ediciones Espam.

Sánchez, M., & Pérez, A. (2023). Estrategias de continuidad del negocio y respaldo informático. Métodos Tecnológicos, 19(2), 201-215.

Vásquez, C., & Morales, G. (2021). Impacto operacional del phishing en microempresas del sector servicios. Anales de Ciberseguridad, 6(2), 77-91.

Zolder, R. (2023). Endpoint protection strategies for non-technical organizations. CyberTech Research.