Ciberseguridad en PYMES del sector digital y publicitario en Colombia: guía práctica para mitigar riesgos compartidos entre empresas que contratan o prestan servicios digitales

Luis Eduardo Gomez Guevara

Director

Alexander Larrahondo Núñez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Agradecimientos

Agradezco a mi esposa, mi compañera inquebrantable, quien siempre estuvo a mi lado de manera incondicional en cada trasnocho, cada fin de semana que cedió con amor, paciencia y comprensión a mi desarrollo profesional, Me apoyaste día a día en cada reto que se me presentó en este proceso de crecimiento. Fuiste, eres y seguirás siendo mi mayor motivación.

A la Universidad Nacional Abierta y a Distancia, a los docentes los cuales me formaron durante este programa. Considero que su compromiso y dedicación han fomentado una verdadera equidad para este país por medio del conocimiento. Este logro también es de ustedes, a través de mi proceso formativo e igual al de muchas personas que como yo, buscan ser y aportar a esta sociedad.

A cada persona que directa o indirectamente fue participe en este proceso, con un poco de conocimiento, un consejo o un apoyo incondicional, este logro también es de ustedes.

Dedicatoria

Aunque son demasiadas mis gratitudes, el más grande de todos se lo debo a Dios por haber sido mi guía y darme fortaleza para seguir adelante, su presencia ha sido crucial para poder logra sembrar en mí todas esas semillas en la necesidad para crecer como profesional.

A mis padres que a través de su esfuerzo y dedicación me inculcaron los valores y la disciplina que fueron claves para llegar a este punto.

Este trabajo es el resultado de mi compromiso por aprender, crecer y seguir, con constancia y pasión, profesionalmente.

Resumen

La creciente dependencia tecnológica en las pequeñas y medianas empresas del sector servicios digitales y publicidad en Colombia ha incrementado su vulnerabilidad ante las amenazas cibernéticas, mientras que pocas de estas organizaciones cuentan actualmente con planes de protección óptimos. Este artículo analiza la situación actual de ciberseguridad en dichas compañías, identificando vacíos habituales como el empleo de contraseñas débiles, la falta de capacitación al personal y la ausencia de protocolos de respuesta ante incidentes.

A través de un examen documental, se evaluaron estrategias básicas de ciberseguridad reconocidas a nivel internacional, por ejemplo, la autenticación multifactor, la utilización de herramientas de código abierto para supervisión, y la implementación de copias de seguridad encriptadas. Asimismo, se diseñó una propuesta simple de programa de capacitación interna, pensada para PYMES con recursos limitados. El objetivo final es aportar una guía práctica que les permita fortalecer su protección digital sin necesidad de grandes inversiones, adaptándose al contexto colombiano.

Palabras Clave: Ciberseguridad, PYMES, Servicios digitales, Publicidad digital, Brechas de seguridad, Protección de datos, Capacitación en seguridad, Herramientas de código abierto, Autenticación multifactor, Estrategias de seguridad

Abstract

The growing technological dependence of small and medium-sized enterprises (SMEs) in Colombia's digital services and advertising sector has increased their vulnerability to cyber threats, while few of these organizations currently have effective protection plans in place. This paper analyzes the current state of cybersecurity in such companies, identifying common gaps such as the use of weak passwords, lack of staff training, and the absence of incident response protocols.

Through a documentary analysis, basic internationally recognized cybersecurity strategies were evaluated, including multi-factor authentication, the use of open-source monitoring tools, and the implementation of encrypted backups. In addition, a simple internal training program was designed, tailored to SMEs with limited resources. The ultimate goal is to offer a practical guide that helps strengthen their digital protection without requiring significant investments, while remaining adapted to the Colombian context.

Keywords: Ciberseguridad, PYMES, Servicios digitales, Publicidad digital, Brechas de seguridad, Protección de datos, Capacitación en seguridad, Herramientas de código abierto, Autenticación multifactor, Estrategias de seguridad

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En un entorno donde la transformación digital avanza rápidamente, las pequeñas y medianas empresas (PYMES) del sector digital y publicitario en Colombia enfrentan crecientes desafíos relacionados con la seguridad de la información. Estas organizaciones, caracterizadas por operar con recursos limitados y una alta dependencia tecnológica, se han convertido en blancos frecuentes de ciberataques, principalmente por no contar con políticas estructuradas de ciberseguridad ni con personal especializado.

Esta monografía surge como respuesta a esa vulnerabilidad latente. Su propósito es diseñar una guía práctica y realista que permita a las PYMES fortalecer su postura de seguridad sin que el factor económico sea una barrera insalvable. A través de un enfoque documental y aplicado, se analizan las brechas más comunes en este tipo de empresas, se evalúan estrategias básicas de protección basadas en estándares reconocidos, y se plantea una propuesta formativa orientada a construir una cultura organizacional más consciente y resiliente frente a las amenazas digitales.

Este documento no solo pretende ser un aporte académico, sino también una herramienta útil para empresarios, agencias digitales y profesionales del sector que buscan implementar medidas efectivas de ciberseguridad en contextos reales y con recursos limitados.

Planteamiento del Problema

Muchas PYMES siguen sin darle la atención necesaria a la seguridad cibernética, lo cual las deja en una posición vulnerable frente a posibles ciberataques. Esto suele deberse a una percepción equivocada: al ser empresas pequeñas, piensan que no son objetivos atractivos para los ciberdelincuentes (López-Anchala & Ordóñez-Parra, 2024). Este enfoque despreocupado, sin embargo, incrementa significativamente el riesgo al que están expuestas.

Según el informe de Marsh (2024), el 60% de las PYMES en Colombia reportaron al menos un incidente de seguridad cibernética en el último año, lo que evidencia la urgencia de medidas preventivas para evitar pérdidas económicas y reputacionales.

Esta situación resulta particularmente crítica en las pequeñas y medianas empresas del sector de servicios digitales y publicidad en Colombia. Muchas de estas organizaciones no gestionan directamente toda su operación tecnológica, sino que subcontratan servicios como diseño web, campañas digitales o manejo de plataformas, delegando así funciones clave a terceros. Esta práctica genera lo que se conoce como riesgos compartidos: brechas de seguridad que surgen cuando una empresa entrega acceso o información sensible a un proveedor, sin validar si este cumple con medidas mínimas de ciberseguridad.

Según Mitratech (2024), el 61% de las organizaciones ha sufrido brechas de seguridad ocasionadas por terceros, y un porcentaje considerable no gestiona de forma activa estos riesgos en sus contratos o acuerdos. En las PYMES del sector digital, esta confianza sin verificación suele ser la norma, y ante un incidente, tanto la agencia como la empresa cliente pueden verse comprometidas. A medida que este sector crece, se vuelve urgente generar conciencia sobre la corresponsabilidad en la protección de la información, promoviendo una cultura de seguridad más madura, incluso en entornos con recursos limitados (PwC, 2024; Latin Lawyer, 2024).

Esto plantea un reto claro ¿cómo lograr que las estrategias básicas de ciberseguridad mitiguen los riesgos y fortalezcan la postura de seguridad en organizaciones con recursos limitados?

Una de las fallas más comunes es la falta de auditorías de seguridad regulares, que son clave para evaluar continuamente las medidas de protección y mejorar la postura de seguridad. Sin este proceso, no solo las brechas siguen existiendo, sino que el personal y la dirección permanecen sin la conciencia adecuada sobre los riesgos (López-Anchala & Ordóñez-Parra, 2024).

El problema de la ciberseguridad en las PYMES no se limita a la tecnología, también implica la falta de formación en el personal. Aunque algunos empleados creen que tienen el conocimiento necesario para enfrentar amenazas cibernéticas, la realidad es que, sin una capacitación adecuada y continua, estos conocimientos suelen ser insuficientes (Piñon et al., 2023). Aquí es donde el hacking ético puede jugar un papel importante, ya que no solo permite identificar puntos débiles, sino que también ayuda a concienciar al personal sobre las amenazas reales que podrían enfrentar (Jimenez Calderón et al., 2024).

Otro desafío evidente para las PYMES es el tema económico. Muchas no pueden costear soluciones de seguridad avanzadas, pero existen alternativas viables como los dispositivos de bajo costo para implementar sistemas de detección de intrusos (IDS), lo cual es una manera efectiva de comenzar a protegerse sin requerir grandes inversiones (Lopez Rojas y otros, 2023).

Si las PYMES que ofrecen servicios digitales y publicidad en Colombia no abordan estos problemas, las consecuencias pueden ser críticas. Estarán más expuestas a ataques como el ransomware, que se aprovechan de la falta de preparación y concientización del personal (Flórez Rojas & León Rubio, 2024). Este tipo de ataques no solo puede afectar las operaciones de la

empresa, sino también su reputación y, en última instancia, llevar al cierre del negocio. Por eso, la capacitación del personal y la concientización se convierten en la primera línea de defensa.

En definitiva, esta monografía propone desarrollar una guía práctica que no solo se base en la implementación de herramientas tecnológicas, sino también en la creación de una cultura de seguridad sólida que abarque a todos los niveles de la organización. Capacitar al personal y generar conciencia son pasos fundamentales para mejorar la seguridad sin necesidad de grandes recursos.

Justificación

Las pequeñas y medianas empresas del sector de servicios digitales y publicidad en Colombia se han convertido en actores clave dentro de la economía digital. Su crecimiento y dinamismo también las expone a nuevas amenazas cibernéticas, especialmente cuando gran parte de su operación tecnológica se delega a terceros. En estos escenarios, la seguridad de la información ya no depende únicamente de medidas internas, sino que se convierte en una responsabilidad compartida entre quien presta el servicio digital y quien lo contrata. Esta relación abre la puerta a lo que se conoce como riesgos compartidos, es decir, vulnerabilidades que se trasladan de un actor a otro en ausencia de controles o verificaciones mínimas.

Justificar una intervención en este tipo de empresas resulta clave, no solo porque manejan datos sensibles y canales digitales de comunicación con sus clientes, sino porque la mayoría no cuenta con una estructura formal de ciberseguridad. Las decisiones relacionadas con la seguridad tienden a ser reactivas y, muchas veces, superficiales. De acuerdo con el Banco Interamericano de Desarrollo (2017), las organizaciones deben adoptar una visión compartida de la seguridad, entendiendo que cualquier eslabón débil incluso externo, puede comprometer toda la cadena digital. Esta perspectiva cobra mayor relevancia cuando se considera que en muchas PYMES ni siquiera existe claridad sobre las obligaciones de seguridad cuando se trabaja con terceros.

La monografía propone desarrollar una guía de estrategias básicas, accesibles y realistas, que permita a las empresas ya sea que presten o contraten servicios digitales, mitigar riesgos sin requerir grandes inversiones. Esta propuesta cobra especial relevancia cuando se considera que muchas PYMES ni siquiera cuentan con personal dedicado a la seguridad de la información, y que tanto el conocimiento como los recursos financieros son limitados (Serna et al., 2024; López Rojas y otros, 2023).

Además, la falta de formación al interior de estas empresas es una de las principales causas de su vulnerabilidad. Como señalan Piñon et al. (2023), sin programas de capacitación que enseñen a identificar y responder a incidentes cibernéticos, incluso las herramientas más avanzadas pueden resultar ineficaces. En este sentido, una guía práctica también puede servir como base para fortalecer la cultura de seguridad y orientar buenas prácticas, tanto para el personal interno como para las agencias externas involucradas.

Por lo tanto, esta propuesta se justifica no solo por el aumento de ciberataques en el país y la región, sino también por la necesidad de brindar soluciones específicas y contextualizadas a un sector que suele quedar fuera de los grandes marcos regulatorios y normativos. El objetivo es cerrar esas brechas sin exigir recursos que las empresas no tienen, pero sí generando conciencia, compromiso y corresponsabilidad.

Objetivos

Objetivo General

Diseñar una guía práctica de estrategias básicas de ciberseguridad para PYMES del sector de servicios digitales y publicidad en Colombia, orientada a fortalecer la protección de la información y la conciencia sobre riesgos compartidos en entornos tercerizados.

Objetivos Específicos

Analizar las medidas actuales de seguridad cibernética en las PYMES mediante un diagnóstico detallado, para identificar las brechas y necesidades en la protección de la información.

Evaluar estrategias básicas de ciberseguridad reconocidas a nivel internacional, que sean aplicables al contexto de las PYMES colombianas del sector digital y publicitario.

Diseñar una propuesta básica de un programa de capacitación interna en seguridad de la información, dirigida a empleados de PYMES del sector digital, que promueva prácticas seguras frente a amenazas internas y riesgos compartidos asociados a la tercerización de servicios digitales.

Marco Referencial

Antecedentes

En los últimos años se han desarrollado múltiples estudios relacionados con la ciberseguridad en organizaciones colombianas, así como propuestas para implementar estrategias de protección de la información en contextos de recursos limitados. A continuación, se presentan algunos trabajos relevantes que han servido de base para el desarrollo de esta monografía.

- Gil Arenas et al. (2025)

En su estudio sobre la gestión del riesgo y la evaluación de controles en empresas de servicios públicos en Antioquía, los autores resaltan la importancia de identificar brechas mediante diagnósticos específicos y proponen evaluaciones periódicas para fortalecer los sistemas existentes. Aunque el contexto es diferente al de las PYMES digitales, los hallazgos permiten comprender cómo aplicar modelos de mejora gradual en entornos organizacionales complejos.

- Serna, Villamizar y Vallejo (2024)

Este trabajo propone un modelo económico para la implementación de marcos de seguridad de la información en organizaciones colombianas. La investigación destaca que la percepción del alto costo de la seguridad es una de las principales barreras, y propone alternativas de bajo presupuesto. Sus conclusiones coinciden con la línea de esta monografía, al defender que la seguridad es una inversión necesaria, incluso para empresas pequeñas.

- LinkTIC (2024)

El informe “Ciberseguridad en Colombia: panorama completo de su estado en 2023” revela que los incidentes de ciberseguridad han aumentado un 35% en el último año, afectando tanto a grandes como pequeñas organizaciones. Se destaca la falta de preparación de las PYMES,

así como la ausencia de protocolos internos y estrategias de capacitación. Esta fuente fue clave para contextualizar la problemática y justificar la propuesta de estrategias básicas en este proyecto.

- UNAD (2025)

El artículo "Ciberseguridad en Colombia: integrando blockchain e inteligencia artificial para fortalecer la protección digital" resalta la necesidad de combinar herramientas tecnológicas con procesos de formación y cultura organizacional. Aunque su enfoque se orienta a soluciones avanzadas, refuerza la idea de que la seguridad digital no se debe abordar solo como un tema exclusivamente técnico, sino que también es de carácter humano y organizacional, lo cual es transversal al planteamiento de esta monografía.

Estos antecedentes permiten establecer un marco de análisis sólido y evidencian que, aunque existen múltiples esfuerzos por abordar la ciberseguridad en Colombia, aún hay un vacío práctico en cuanto a estrategias simples y realistas para PYMES del sector digital. Este trabajo busca contribuir en ese sentido, priorizando soluciones que puedan ser adoptadas sin requerir grandes estructuras técnicas ni presupuestos elevados.

Marco Conceptual

Para el desarrollo del presente trabajo, se establecieron una serie de conceptos clave que permiten delimitar el alcance del análisis y dar claridad sobre los términos que se emplean a lo largo del documento. Estos conceptos han sido definidos de forma operativa, es decir, con un enfoque práctico y aplicado al contexto de las PYMES del sector digital en Colombia.

Ciberseguridad

Conjunto de prácticas, herramientas y políticas orientadas a proteger los sistemas informáticos, redes, dispositivos y datos frente a accesos no autorizados, alteraciones o

destrucción. En este trabajo, se entiende como un conjunto mínimo de medidas que las PYMES pueden adoptar para reducir riesgos comunes y fortalecer su infraestructura digital.

Brechas de seguridad

Son los vacíos o deficiencias que existen en la protección de los activos digitales. Pueden estar relacionadas con la falta de herramientas técnicas, desconocimiento del personal, ausencia de políticas internas o exposición a amenazas externas. Identificarlas es clave para diseñar estrategias de mejora realistas y priorizadas.

PYMES del Sector Digital y Publicitario

Empresas pequeñas o medianas que ofrecen servicios relacionados con marketing, publicidad y comunicación digital, incluyendo SEO, campañas en redes sociales, diseño web, automatización, entre otros. Suelen operar con equipos reducidos, presupuestos ajustados y alta dependencia de recursos tecnológicos.

Cultura de Seguridad

Hace referencia a la conciencia, comportamiento y compromiso de todos los miembros de una organización frente a la protección de la información. Va más allá del uso de herramientas, e implica la integración de la seguridad como parte de la dinámica empresarial diaria.

Capacitación en Ciberseguridad

Proceso mediante el cual los empleados reciben formación sobre riesgos digitales, buenas prácticas y protocolos de respuesta ante incidentes. En este trabajo, se considera una de las estrategias más efectivas y económicas para reducir vulnerabilidades, especialmente en el caso del phishing o errores humanos.

Tabla 1

Variables Clave

Variable clave	Definición operativa	Justificación
Nivel de implementación de medidas de ciberseguridad	Grado en que una empresa ha adoptado herramientas, políticas y prácticas para proteger sus sistemas y datos.	Permite medir el estado actual de protección y priorizar acciones de mejora.
Capacitación interna en seguridad de la información	Existencia de procesos formales o informales de formación a empleados sobre riesgos cibernéticos y buenas prácticas.	Ayuda a reducir vulnerabilidades humanas y prevenir ataques como el phishing.
Disponibilidad de recursos tecnológicos y financieros	Capacidad de la empresa para invertir en tecnologías, herramientas y servicios relacionados con la ciberseguridad.	Facilita propuestas adaptadas a las condiciones reales de las PYMES.
Conciencia organizacional sobre la ciberseguridad	Nivel de importancia que la dirección de la empresa le asigna a la protección de la información, evidenciado en políticas y decisiones.	Determina si la seguridad es parte activa de la cultura organizacional o solo una obligación técnica.

Nota. Elaboración propia basada en el análisis conceptual del proyecto.

Análisis Documental

Metodología empleada para revisar, organizar y analizar información proveniente de fuentes secundarias (artículos científicos, normas técnicas, informes institucionales, etc.).

Permite obtener conclusiones a partir del conocimiento ya disponible, sin necesidad de realizar recolección directa de datos.

Variables clave del Proyecto

Con el fin de estructurar y orientar el análisis del problema identificado en este trabajo, se presentan a continuación cuatro variables clave del proyecto. Estas variables permiten establecer un marco de interpretación claro y coherente, alineado con los objetivos específicos y el contexto de las PYMES del sector digital y publicitario en Colombia. En la tabla 1 se resume la definición operativa y la justificación de su inclusión en el estudio.

Marco Teórico

El presente marco conceptual y teórico tiene como objetivo proporcionar una base sólida para entender y justificar la investigación sobre la implementación de estrategias de ciberseguridad en PYMES. A continuación, se definen y se explican los principales conceptos que estructuran la investigación y se relacionan con teorías y estudios relevantes del campo.

Seguridad Cibernética y PYMES

La seguridad cibernética se refiere al conjunto de prácticas, políticas y tecnologías diseñadas para proteger los sistemas, redes y datos frente a ataques cibernéticos. En el contexto de las PYMES, la seguridad cibernética se enfrenta a desafíos específicos relacionados con la falta de recursos y de concienciación. Las PYMES representan una parte vital de la economía, particularmente en países como Colombia, donde contribuyen de manera significativa al empleo y al desarrollo local. Sin embargo, debido a su tamaño y limitaciones de presupuesto, muchas PYMES creen erróneamente que no son objetivos atractivos para los ciberdelincuentes, lo cual las deja en una posición vulnerable (López-Anchala y otros, 2024).

Cultura De Seguridad y Concientización

Uno de los problemas fundamentales que enfrentan las PYMES es la falta de cultura de seguridad. La cultura de seguridad se refiere a las creencias, actitudes y comportamientos en una organización orientados a la protección de la información y la prevención de riesgos. Para crear una cultura de seguridad sólida, es crucial involucrar a todos los niveles de la empresa en la implementación y comprensión de las medidas de seguridad. Sin embargo, muchas PYMES carecen de esta cultura debido a la falta de recursos para capacitar a su personal, lo cual incrementa la vulnerabilidad ante amenazas como el ransomware y el phishing (Piñon y otros, 2023).

El éxito de la implementación de medidas de seguridad depende en gran parte de la concientización del personal. Según Flórez Rojas y León Rubio (2024), el ransomware se aprovecha principalmente de la falta de preparación de los empleados. La capacitación en ciberseguridad no es solo un complemento, sino una parte esencial para garantizar que el personal pueda identificar, prevenir y reaccionar ante incidentes cibernéticos. Sin una preparación adecuada, cualquier medida técnica que se implemente podría ser insuficiente.

Hacking Ético y su Rol en la Concientización

El hacking ético se presenta como una herramienta poderosa no solo para identificar vulnerabilidades en los sistemas, sino también para generar conciencia sobre los riesgos. A través de pruebas de penetración, los empleados pueden ver en la práctica cómo sus sistemas y datos pueden ser atacados, lo cual crea una sensación inmediata de relevancia sobre la necesidad de mantener la seguridad (Jimenez Calderón y otros, 2024). Además, el hacking ético promueve la adopción de un enfoque preventivo, ayudando a las PYMES a identificar áreas de mejora antes de que se produzcan incidentes reales.

Gestión de Recursos y Alternativas Económicas

Otro de los desafíos importantes es la falta de recursos económicos. Para muchas PYMES, invertir en tecnologías de ciberseguridad avanzadas no es una opción viable. Sin embargo, existen alternativas más asequibles que permiten a estas empresas fortalecer su seguridad sin necesidad de realizar grandes inversiones. Lopez Rojas y otros (2023) sugieren el uso de dispositivos de bajo costo para implementar sistemas de detección de intrusos (IDS), lo cual puede ser un buen primer paso para aquellas PYMES que quieren comenzar a protegerse, pero cuentan con recursos limitados. Estas alternativas ofrecen una forma práctica y económica de mitigar riesgos.

Estrategias De Seguridad y su Impacto

La implementación de estrategias de seguridad adecuadas no solo ayuda a mitigar riesgos, sino que también mejora la confianza de los clientes y la sostenibilidad de la empresa. En un mercado competitivo, las PYMES que logran demostrar un compromiso serio con la seguridad cibernética están en una mejor posición para establecer relaciones comerciales sólidas y ganar contratos importantes. Además, como argumenta Dorairajan (2024), la ciberseguridad bien implementada tiene un impacto positivo en el rendimiento general de la organización, al reducir las interrupciones causadas por incidentes y permitir una operación más eficiente.

Conclusiones del Marco Conceptual y Teórico

En resumen, la seguridad cibernética en PYMES debe ser entendida desde un enfoque integral que no solo considere la implementación de herramientas tecnológicas, sino que también promueva la creación de una cultura de seguridad y la capacitación continua del personal. La investigación demuestra que las PYMES pueden mejorar su postura de seguridad incluso con recursos limitados, siempre y cuando se adopten medidas prácticas como la capacitación, el uso

de dispositivos económicos y la concientización del personal. Esta combinación de elementos permite a las PYMES no solo reducir sus vulnerabilidades, sino también fortalecer su competitividad y garantizar la continuidad del negocio frente a las crecientes amenazas cibernéticas.

Marco Legal

En Colombia, el marco normativo relacionado con la seguridad de la información y la protección de datos ha avanzado en los últimos años, con el propósito de brindar un entorno regulado para las organizaciones que manejan datos personales y sistemas de información críticos. Para el desarrollo de este documento considera las siguientes normas y leyes relevantes para el contexto de las PYMES del sector digital:

Ley 1581 de 2012 – Protección de Datos Personales

Establece disposiciones generales para la protección de datos personales en Colombia. Esta norma exige a las empresas adoptar medidas para garantizar la confidencialidad, integridad y disponibilidad de la información de sus usuarios y clientes.

Decreto 1377 de 2013

Complementa la Ley 1581, regulando el manejo y tratamiento de datos recolectados antes de su entrada en vigor. Además, establece las obligaciones de los responsables del tratamiento de datos en cuanto a autorización y seguridad.

Ley 1266 de 2008 – Habeas Data financiero

Si bien está orientada principalmente al manejo de información financiera, también impone obligaciones de seguridad sobre el uso de datos sensibles, aplicable a algunas operaciones realizadas por empresas del sector digital.

ISO/IEC 27001:2022 (adoptada en Colombia como NTC-ISO/IEC 27001)

Aunque no es de carácter obligatorio, esta norma internacional sirve como guía para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Su adopción por parte de empresas colombianas es voluntaria, pero altamente recomendable.

Ley 1273 de 2009 – Delitos Informáticos

Modifica el Código Penal colombiano para incluir delitos informáticos y contra la protección de datos. Establece sanciones para actos como acceso no autorizado, daño informático, interceptación de datos y sabotaje a sistemas.

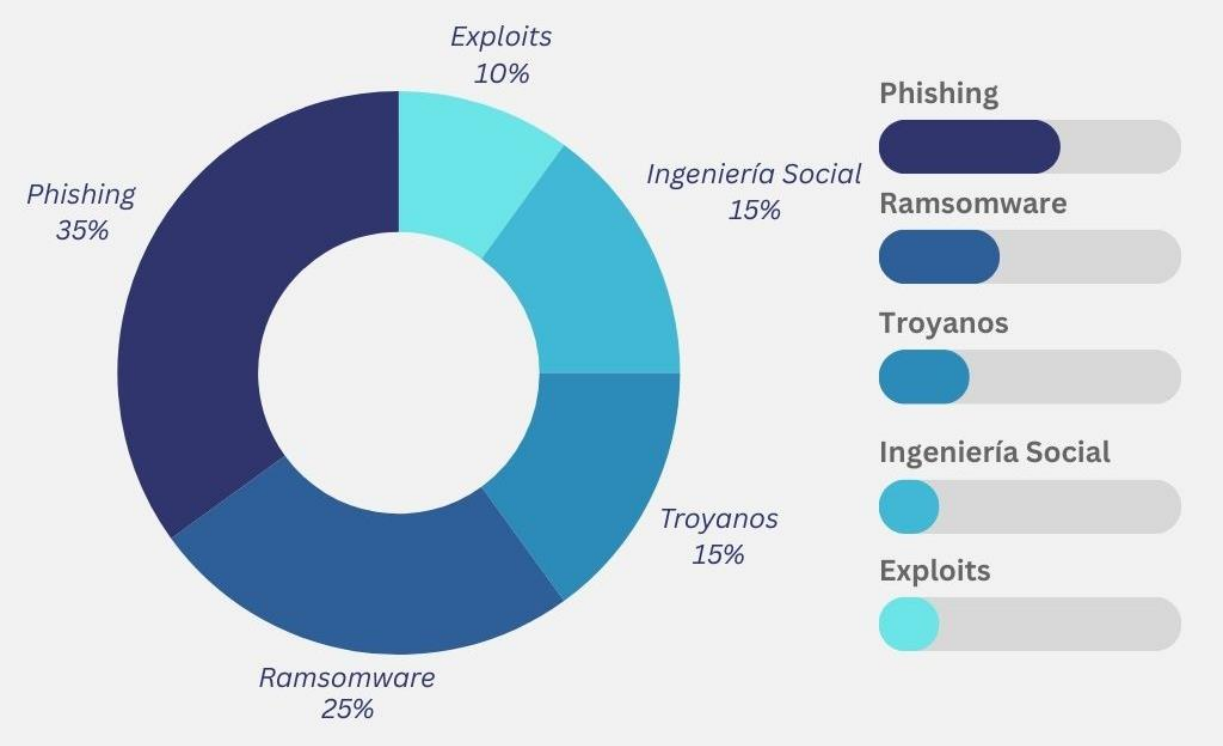
Este marco legal establece una base normativa sólida sobre la cual las PYMES deben construir sus políticas y prácticas de ciberseguridad, incluso si no están obligadas a certificarse. La falta de cumplimiento puede representar riesgos legales, económicos y reputacionales que afectan directamente la sostenibilidad del negocio.

Marco Contextual

El crecimiento acelerado de las pequeñas y medianas empresas (PYMES) del sector digital y publicitario en Colombia ha estado acompañado por un aumento exponencial en su exposición a ciberamenazas. Estas empresas suelen operar con estructuras reducidas, dependencia tecnológica alta y manejo constante de datos sensibles de clientes, campañas, accesos a plataformas y activos digitales. Sin embargo, la falta de inversión en seguridad y el bajo nivel de cultura organizacional en ciberseguridad las convierte en objetivos atractivos para ciberdelincuentes.

Figura 1

Tipos de Ciberataques más Comunes en Latinoamérica (2023–2024)



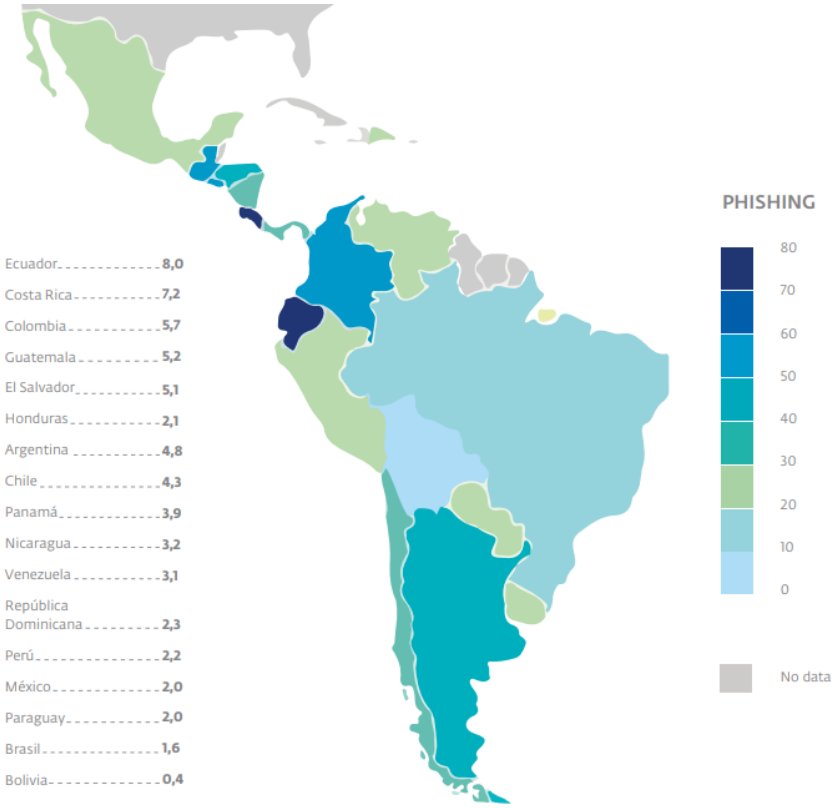
Nota. Elaboración propia con base en tendencias regionales reportadas por Hackmetrix, Check Point LATAM y ESET Security Report 2024.

Tal como se ilustra en la Figura 1, se presentan estimaciones propias elaboradas con base en tendencias descritas por ESET, Check Point y Hackmetrix sobre los tipos de ataques más frecuentes en la región.

Por su parte, Check Point señala que el “malvertising” ha incrementado en la región, afectando especialmente a empresas que compran y venden espacios publicitarios en línea. Estos ataques permiten distribuir malware mediante anuncios legítimos, comprometiendo la reputación y los recursos de plataformas que gestionan campañas digitales (Figura 2).

Figura 2

Porcentaje de Detecciones de Phishing en América Latina (2022)



Nota. Detección de phising en Latam (2023). Tomado de. ESET Security Report 2023. https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

En cuanto al entorno empresarial, datos de Statista (2024) muestran que el gasto en publicidad digital en América Latina superó los 13.000 millones de dólares en 2023, con una proyección de crecimiento anual del 8,2%. Este auge ha venido acompañado de una adopción masiva de servicios automatizados, publicidad programática y gestión de datos en la nube, aumentando el número de vectores de ataque para agencias y proveedores de servicios digitales.

Aunque los informes de ciberseguridad no siempre desglosan específicamente al sector publicitario, los estudios de ESET, PwC y Check Point identifican consistentemente a sectores como finanzas, tecnología, salud y educación entre los más atacados en América Latina. En este grupo de alta exposición también se encuentran empresas del sector servicios, dentro del cual pueden ubicarse muchas PYMES dedicadas al marketing digital, la publicidad y la gestión de plataformas en línea.

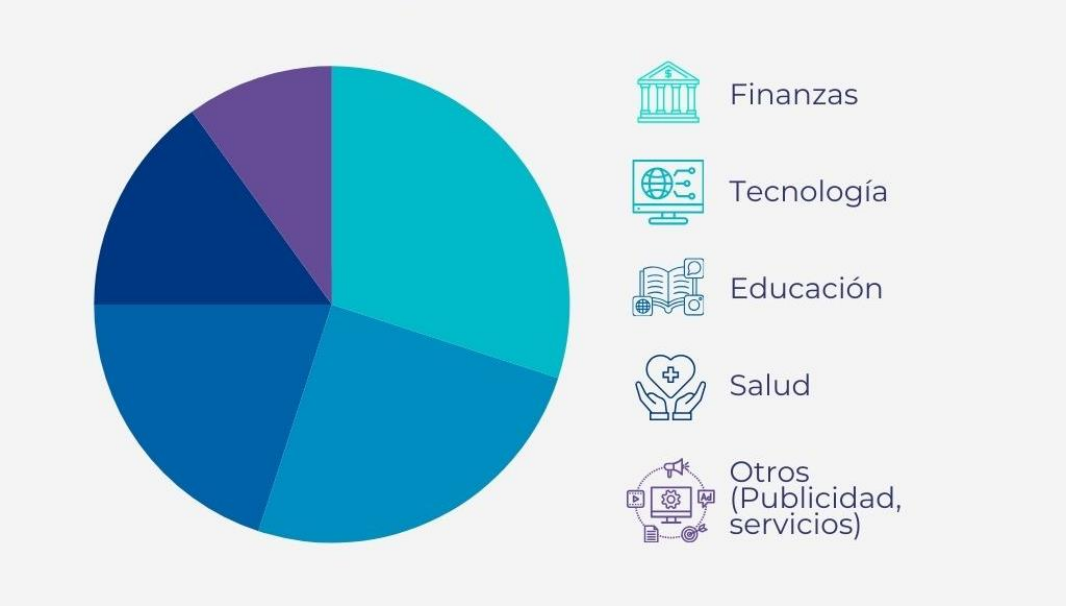
La Figura 3 muestra una síntesis visual basada en la identificación de sectores más vulnerables reportados por ESET y PwC. Aunque el sector publicitario no se muestra explícitamente, se estima que puede ubicarse dentro del grupo de servicios altamente expuestos.

Un caso paradigmático, fue el ataque en 2017 al grupo WPP, uno de los conglomerados publicitarios más grandes del mundo, en cual afectó agencias como Ogilvy y Young & Rubicam con el ransomware “Petya” (BBC, 2017). Esto demostró que las agencias creativas no solo son vulnerables, sino también estratégicamente atractivas para los atacantes debido a la cantidad de credenciales, bases de datos y sistemas que gestionan.

En este contexto, es posible inferir que muchas PYMES publicitarias, aunque no figuren directamente en estadísticas nacionales comparten el mismo nivel de exposición que sus pares de otros sectores. De hecho, informes como los de Hackmetrix (2024) destacan que el 67% de las empresas latinoamericanas aumentaron su inversión en marketing digital entre 2023 y 2024, lo que eleva proporcionalmente el riesgo de ataques si no se acompaña de medidas de protección.

Figura 3

Sectores Económicos Más Afectados por Ciberataques en Latinoamérica (2023–2024)



Nota. Elaboración propia a partir de los sectores vulnerables identificados por ESET y PwC en informes regionales de ciberseguridad.

Por todo lo anterior, la presente monografía se centra en brindar una respuesta concreta a ese vacío: una guía práctica de ciberseguridad enfocada en las PYMES que prestan o contratan servicios digitales en Colombia, con especial atención a los riesgos compartidos que surgen al tercerizar servicios tecnológicos. Esta propuesta busca fortalecer su postura de seguridad digital sin requerir grandes inversiones, priorizando estrategias realistas, escalables y adaptadas a su entorno.

Diseño Metodológico

Este trabajo adopta un enfoque metodológico de tipo documental y analítico, fundamentado en la revisión de literatura especializada, informes de organismos oficiales, estudios de caso y marcos normativos nacionales e internacionales relacionados con la ciberseguridad en PYMES. El propósito fue identificar las principales brechas de seguridad y proponer estrategias accesibles y contextualizadas para su mitigación.

La unidad de análisis corresponde a PYMES colombianas del sector de servicios digitales y publicidad, con énfasis en aquellas que prestan o contratan servicios tecnológicos con terceros, como agencias digitales, desarrolladores externos o proveedores de hosting. Esta delimitación responde a la necesidad de comprender los desafíos que enfrentan estas empresas no solo desde sus capacidades internas, sino también desde la gestión de riesgos compartidos derivados de relaciones de tercerización tecnológica.

El método aplicado se centró en el análisis comparativo de buenas prácticas descritas por marcos como ISO/IEC 27001 y NIST CSF, así como en el contraste con estudios recientes sobre vulnerabilidades específicas en organizaciones pequeñas, incluyendo aquellas generadas por proveedores externos. Fuentes como PwC (2024) y Mitratech (2024) permitieron identificar la frecuencia de brechas asociadas a terceros, lo que complementa la caracterización del problema más allá del entorno interno de las PYMES.

En esta metodología se integró un análisis de variables claves las cuales se describieron dentro del marco conceptual y que sirvieron de base para estructurar la guía propuesta, diferenciando medidas aplicables al contexto interno de las PYMES y recomendaciones mínimas para su interacción con agencias o servicios digitalmente subcontratados. De este modo, el diseño metodológico permitió articular un diagnóstico realista con recomendaciones prácticas,

considerando tanto la capacidad operativa de las empresas como los riesgos a los que se exponen al depender de terceros.

Análisis de las Medidas Actuales de Seguridad Cibernética en las PYMES Mediante Un Diagnóstico Detallado, Para Identificar Las Brechas Y Necesidades en la Protección de la Información

Este capítulo presenta un análisis del estado actual de la seguridad cibernética en PYMES del sector digital y publicitario en Colombia, con el propósito de identificar brechas comunes y prácticas deficientes. A partir de una revisión documental, se examinan los principales riesgos, la infraestructura básica con la que cuentan estas empresas y los desafíos que enfrentan al operar en entornos expuestos a ciberamenazas.

En la economía digital, las PYME's del sector de servicios digitales y publicitarios en Colombia juegan un papel muy importante. Pero, también se han convertido en blancos notorios para el cibercrimen: la dependencia de tecnologías y la gestión de datos sensibles aumentan su riesgo de sufrir ataques como phishing, ransomware y fugas de información. La realidad es que muchas de ellas no cuentan con medidas de seguridad suficientes y sólo se apoyan en soluciones básicas como el uso de antivirus y cortafuegos tradicionales.

Dentro del panorama de la ciberseguridad en Colombia, hemos observado cómo los incidentes de seguridad han ido aumentando en los últimos años y se evidencia que es una tendencia que viene en aumento. En una publicación de la empresa LinkTIC (2024) evidencio el incremento de hasta un 79% en ataques a empresas de todos los tamaños. Como he abordado anteriormente, aunque se suele pensar que los cibercriminales sólo atacan a las grandes corporaciones, no debemos olvidar que esas pequeñas y medianas empresas también pueden sufrir. Justamente el hecho de tener menos protección las deja en una situación de riesgo considerable.

Así, muchas de estas empresas aún usan passwords básicos que comparten con otros empleados y empresas externas, realizan copias de seguridad cada tres meses más o menos, en algunos casos simplemente no se realizan. Y si a esto se le suma que no cuentan con un plan de respuesta para casos de emergencia. También son muy frágiles a los ataques de ingeniería social si se las compara con marcos como ISO 27001 o NIST; hay muchas brechas por rellenar.

Un ejemplo sencillo, si bien estos estándares sugieren el uso de la autenticación multifactor de contraseñas y el cifrado de información vital, sobre todo en el almacenamiento; La mayor parte de las empresas pequeñas y medianas se sigue refugiando en simples formas de acceso e informática sin protección. Tampoco efectúan auditorías de seguridad en forma periódica, con lo cual les resultará difícil detectar alguna vulnerabilidad a tiempo (Gil Arenas et al., 2025).

Si bien, aunque los ciberdelincuentes suelen atacar a los empleados porque ellos son el punto más débil, también aprovechan otros puntos de entrada como el corrompimiento de contraseñas en el propio servicio. Las compañías están sumamente expuestas a riesgos críticos por ataques de phishing dirigidos a empleados, ransomware de información crítica y ataques de DDoS (LinkTIC, 2024). Un punto crucial es que muchas PYMES piensan que es costoso implementar una medida de seguridad, cuando en realidad existen soluciones asequibles como software de código abierto, almacenamiento en la nube con cifrado y educación interna que se puede manejar sin necesidad de que sea proporcionada por especialistas externos (Serna et al., 2024).

Es precisamente el estudio de Serna et al. (2024) sobre el impacto económico de la seguridad en las organizaciones colombianas confirma esta idea, demostrando que es posible reforzar protección sin dañar exageradamente al presupuesto general. No sólo se trata de

implementar herramientas tecnológicas, sino también se debe crear conciencia desde el nivel de dirección hasta el más bajo escalón de toda empresa sobre la importancia de la seguridad en nuestra era.

En general el análisis revela que las PYMES del sector digital son inseguras. Dependen más de medidas reactivas que de una estrategia proactiva. Las empresas que descuidan su seguridad en línea ponen en peligro su reputación y pueden afectarse gravemente por la pérdida de confianza y de operaciones. Hace falta cambiar de mentalidad para que la seguridad se perciba como una inversión y no como un gasto sin razón.

Para identificar las principales brechas en la implementación de medidas de seguridad en las PYMES del sector digital y publicitario, se presenta a continuación una tabla comparativa que confronta las prácticas más comunes observadas en este tipo de empresas con las buenas prácticas recomendadas por marcos de referencia como ISO 27001, NIST CSF y los controles CIS.

En conclusión, el diagnóstico muestra que muchas PYMES del sector digital y publicitario continúan dependiendo de medidas reactivas y soluciones básicas que no se alinean con las buenas prácticas internacionales. Estas debilidades, sumadas a la tercerización de servicios tecnológicos sin controles adecuados, aumentan el nivel de exposición ante amenazas digitales. Este panorama justifica la necesidad de evaluar estrategias accesibles y adaptables, lo cual se abordará en el siguiente capítulo.

Tabla 2

Comparación Entre Prácticas Comunes y Buenas Prácticas de Seguridad de la Información

Área de Seguridad	Práctica común en PYMES	Buena práctica recomendada
Autenticación	Uso de contraseñas débiles y compartidas	Autenticación multifactor (MFA) y gestores de contraseñas
Protección de datos	Copias de seguridad locales, sin cifrado ni redundancia	Backups cifrados, automáticos y en la nube
Capacitación del personal	Poca o nula formación en ciberseguridad	Capacitación periódica y simulacros de phishing
Monitoreo y respuesta a incidentes	Ausencia de monitoreo o protocolos de respuesta	Uso de SIEM, IDS/IPS como Snort o Suricata
Control de accesos	Permisos generales sin segmentación	Roles definidos y control estricto sobre accesos

Nota. Elaboración propia basada en las recomendaciones de ISO/IEC 27001:2022, NIST CSF, CIS Controls.

Evaluación de Estrategias Básicas de Ciberseguridad Aplicables A PYMES del Sector Digital, con Base en Buenas Prácticas Reconocidas a Nivel Internacional

Una vez identificado el diagnóstico, se procede a evaluar estrategias básicas de ciberseguridad que respondan a las brechas detectadas en las PYMES del sector

En el contexto colombiano, muchas pequeñas y medianas empresas del sector digital y publicitario reconocen la necesidad de proteger su información, pero pocas cuentan con estrategias definidas, estructuradas y sostenibles. Por eso, este capítulo se enfoca en evaluar un conjunto de estrategias básicas de ciberseguridad, seleccionadas por su aplicabilidad, bajo costo y alineación con buenas prácticas recomendadas por estándares internacionales como ISO 27001, NIST CSF y los controles CIS.

Estas estrategias no pretenden reemplazar una gestión formal del riesgo o la implementación de un SGSI completo, sino ofrecer soluciones iniciales, prácticas y realistas para empresas con recursos limitados.

Estrategias seleccionadas para la evaluación

A continuación, se presentan las estrategias básicas consideradas más relevantes para el sector objetivo. Estas fueron elegidas con base en estudios recientes, guías internacionales y herramientas de código abierto recomendadas por la comunidad de seguridad informática.

1. Gestión de contraseñas y autenticación segura

- Implementación de autenticación multifactor (MFA).
- Uso de gestores de contraseñas (por ejemplo, Bitwarden o KeePass).
- Reglas mínimas de complejidad y cambio periódico.

2. Copias de seguridad automatizadas y cifradas

- Programación de backups locales y en la nube.

- Uso de herramientas gratuitas como Duplicati.
- Almacenamiento cifrado con control de acceso.

3. Capacitación básica y campañas de concienciación

- Simulacros de phishing.
- Políticas internas claras y comprensibles.
- Cursos en línea gratuitos sobre seguridad básica (como los de Cisco Networking Academy o Google Activate).

4. Uso de herramientas de código abierto para monitoreo

- Snort y Suricata para detección de intrusiones.
- Security Onion como plataforma completa de análisis de seguridad.
- Implementación de registros (logs) y alertas mínimas.

5. Segmentación de red y control de acceso

- Separación de la red administrativa y la red de producción.
- Creación de perfiles de usuarios con permisos específicos.
- Desactivación de servicios innecesarios.

Evaluación de Aplicabilidad

La evaluación de estas estrategias se realiza considerando los siguientes criterios:

- Costo de implementación: ¿Es viable con recursos limitados?
- Facilidad de adopción: ¿Requiere alta especialización o puede aplicarse con personal básico?
- Impacto en la reducción de riesgos: ¿Mitiga amenazas críticas como ransomware o fuga de datos?

Esta evaluación permitió identificar que las estrategias relacionadas con gestión de contraseñas, backups cifrados y capacitación básica son las más viables de implementar en el corto plazo, con un alto retorno en reducción de riesgos. En contraste, herramientas como Security Onion ofrecen gran capacidad de análisis, pero requieren mayor conocimiento técnico, lo que puede dificultar su adopción inicial.

Tabla 3

Comparativa de Estrategias de Ciberseguridad

Estratégia básica	Costo de Implementación	Facilidad en su adopción	Impacto en la reducción
Gestión de contraseñas y autenticación segura	Bajo	Alto	Alto
Copias de seguridad automatizadas y cifradas	Bajo	Alto	Alto
Capacitación básica y campañas de concienciación	Muy bajo	Alto	Medio
Uso de herramientas de código abierto para monitoreo	Medio	Medio	Alto
Segmentación de red y control de acceso	Bajo	Medio	Medio

Nota: Elaboración propia con base en evaluación comparativa de estrategias documentadas en estudios de Serna et al. (2024), LinkTIC (2024) y buenas prácticas internacionales

En la tabla 2 se presenta una comparación entre las estrategias básicas de ciberseguridad evaluadas, considerando criterios como el costo de implementación, la facilidad de adopción y el impacto estimado en la reducción de riesgos. Esta comparación permite visualizar de forma clara cuáles podrían ser aplicadas prioritariamente por PYMES con recursos limitados.

Análisis crítico

Los estándares como ISO 27001 y NIST CSF promueven un enfoque estructurado, pero muchas PYMES no logran cumplir con estos marcos debido a su complejidad o costo. Sin embargo, adoptar estrategias básicas como las aquí evaluadas permite avanzar en la madurez de la seguridad organizacional, aunque sea en etapas.

Tal como lo menciona Serna et al. (2024), el costo no debe ser visto como una barrera absoluta, sino como un factor que obliga a seleccionar soluciones creativas, escalables y sostenibles en el tiempo.

Uso de Herramientas y Referentes Aplicados al Análisis

Para el desarrollo de este documento, se acudió a diversas herramientas y referentes del sector para comprender en profundidad el panorama actual de la ciberseguridad en las pequeñas y medianas empresas, y sobre todo, para identificar las estrategias que realmente pueden ser aplicables en compañías modestas con recursos limitados.

A lo largo del trabajo, se hizo uso de normativas como la ISO 27001, el marco NIST CSF y los Controles CIS, los cuales ayudaron a tener una guía clara sobre qué prácticas mínimas debe implementar una organización para salvaguardar su información. Aunque estos marcos pueden parecer enrevesados, fueron útiles como punto de comparación frente a lo que las PYMES verdaderamente están aplicando.

También se exploraron herramientas de código abierto que podrían ser aprovechadas por empresas pequeñas, sin necesidad de hacer grandes desembolsos. Entre ellas sobresalen:

Snort y Suricata, que son sistemas de detección de intrusiones.

Security Onion, que reúne varias herramientas en una sola plataforma para supervisión.

Duplicati, útil para programar copias de seguridad cifradas y automatizadas.

Bitwarden y KeePass, como alternativas gratuitas para administrar contraseñas de forma segura.

Adicionalmente, se trabajó con el desarrollo de unas tablas comparativas que facilitan el análisis, como la que muestra las diferencias entre las prácticas comunes en PYMES y las buenas prácticas recomendadas. Todo esto ayudó a evaluar el efecto y la viabilidad de aplicar ciertas estrategias de seguridad, de forma simple y realista.

Construcción de una Cultura de Seguridad Informada: Propuesta de Capacitación Interna en Ciberseguridad para Empleados de PYMES

Considerando las estrategias evaluadas previamente, se plantea ahora una propuesta formativa concreta orientada a fortalecer el factor humano dentro de la cultura de ciberseguridad organizacional.

La capacitación interna en seguridad de la información constituye uno de los pilares más relevantes en la construcción de una cultura organizacional resiliente frente a ciberamenazas. En las pequeñas y medianas empresas del sector digital y publicitario, este aspecto cobra mayor importancia debido a la alta rotación de personal, la tercerización de servicios tecnológicos y la escasa formalización de políticas internas. De acuerdo con Piñon et al. (2023), la falta de formación continua representa una de las principales causas de vulnerabilidad frente a incidentes como el phishing, la fuga de información o el uso indebido de credenciales.

En ese contexto, el presente capítulo desarrolla una propuesta básica pero estructurada de programa de capacitación en ciberseguridad para empleados de PYMES, orientado a fortalecer la conciencia sobre los riesgos compartidos que surgen cuando se contratan servicios digitales con terceros. El diseño se fundamenta en principios pedagógicos, buenas prácticas internacionales y herramientas de bajo costo, con el fin de facilitar su adopción incluso en empresas con recursos limitados.

La importancia Estratégica de la Capacitación en Seguridad de la Información

El factor humano continúa siendo una de las principales causas de incidentes cibernéticos. De acuerdo con el informe de Seguridad de IBM (2023), el 95% de las vulnerabilidades de seguridad tienen su origen en errores humanos, ya sea por desconocimiento, descuido o falta de preparación ante situaciones de riesgo. Esta realidad convierte a la formación

interna en un componente estratégico clave, no solo técnico, en la protección de los activos de información de una organización.

En el caso de las pymes, la situación es aún más crítica. Estas empresas suelen operar con recursos limitados, carecen de personal especializado en seguridad informática y tienden a subcontratar servicios tecnológicos sin contar con criterios claros de seguridad. Esto implica que los riesgos no solo se generan internamente, sino también desde terceros que intervienen en los procesos. Por lo tanto, la capacitación se convierte en una herramienta fundamental para reducir la exposición al riesgo en todos los niveles de la organización.

Además, capacitar al personal no solo mejora la postura de seguridad de la empresa, sino que también fortalece la confianza con sus clientes y aliados estratégicos. En sectores donde la reputación digital es clave, como el publicitario o el de servicios creativos, la percepción de control sobre la seguridad puede ser un diferenciador competitivo. Como señalan Medina y Tovar (2021), "la cultura de seguridad organizacional no se impone, se construye desde la conciencia colectiva y la responsabilidad compartida".

Por lo tanto, más allá del cumplimiento normativo o de las mejores prácticas, la capacitación constante en ciberseguridad debe entenderse como una inversión estratégica que impacta directamente en la sostenibilidad y competitividad de las pymes en entornos digitales cada vez más complejos y vulnerables.

Componentes Esenciales del Programa de Capacitación en Ciberseguridad

El diseño de un programa de capacitación efectivo en ciberseguridad para PYMES requiere considerar elementos que aseguren su pertinencia, escalabilidad y sostenibilidad. A diferencia de las grandes organizaciones, donde los programas suelen ser altamente estructurados

y sostenidos por recursos tecnológicos avanzados, las pequeñas empresas deben recurrir a estrategias más flexibles, pero no por ello menos rigurosas.

A continuación, se detallan los principales componentes que debe contemplar un programa formativo adaptado al contexto de las PYMES:

Diagnóstico Inicial de Capacidades. Antes de implementar cualquier iniciativa formativa, es indispensable evaluar el nivel de conocimiento, percepción del riesgo y hábitos digitales del personal. Este diagnóstico puede realizarse a través de encuestas breves, entrevistas o ejercicios de simulación de ataques comunes (como el phishing). Este insumo permite ajustar los contenidos y priorizar áreas críticas.

Definición de Objetivos de Aprendizaje. Los objetivos deben estar alineados con las necesidades reales de la organización y responder a preguntas como: ¿Qué comportamientos queremos cambiar? ¿Qué vulnerabilidades queremos reducir? ¿Qué procesos deben fortalecerse? Esta claridad evita programas genéricos que no generan impacto real.

Segmentación Por Roles y Niveles de Exposición. No todos los colaboradores enfrentan los mismos riesgos ni tienen el mismo nivel de acceso a la información. Por tanto, es recomendable diseñar contenidos diferenciados para roles administrativos, técnicos, operativos y directivos. Esta personalización mejora la retención del conocimiento y la aplicabilidad de lo aprendido.

Contenidos Temáticos Estratégicos. El programa debe abordar temáticas clave, tales como:

- Gestión de contraseñas y autenticación multifactor.
- Reconocimiento de correos fraudulentos y técnicas de ingeniería social.
- Uso seguro de dispositivos móviles y conexiones remotas.

- Protocolos de manejo de incidentes.
- Buenas prácticas en el uso de software y servicios en la nube.

Metodologías de Aprendizaje Activas. La capacitación no debe limitarse a sesiones informativas. La incorporación de casos reales, simulacros, ejercicios prácticos y contenidos multimedia favorece el aprendizaje significativo. Además, herramientas de gamificación pueden ser útiles para reforzar conceptos en contextos laborales informales o creativos.

Mecanismos de Evaluación y Retroalimentación. La medición del aprendizaje es esencial para verificar la efectividad del programa. Evaluaciones periódicas, pruebas de conocimientos y análisis de incidentes previos/posteriores a la capacitación son estrategias que permiten identificar mejoras o ajustes necesarios.

Esto justifica con claridad que un programa exitoso no depende del volumen de contenidos impartidos, sino de su alineación con los riesgos reales de la organización, la adaptación al perfil de los trabajadores y el seguimiento continuo.

Diseño instruccional Adaptado a los Roles y Niveles de Riesgo

Una característica clave en la efectividad de los programas de capacitación es su capacidad para adaptarse a los distintos perfiles laborales y a los riesgos específicos que enfrentan. En el contexto de una PYME del sector digital o publicitario, se pueden identificar al menos tres grupos funcionales que interactúan con sistemas de información: el personal operativo, el personal técnico y los cargos directivos o administrativos. Cada uno requiere un enfoque diferenciado de formación (Tabla 4).

Este enfoque instruccional permite priorizar esfuerzos, reducir carga operativa y ofrecer un modelo escalable que puede ajustarse a las capacidades de cada organización. Además, facilita la rendición de cuentas y el seguimiento de resultados por segmento de la empresa

Tabla 4

Propuesta Instruccional Diferenciada Por Rol y Riesgo

Perfil del colaborador	Tipo de acceso a información	Riesgos principales	Contenidos prioritarios	Metodología sugerida
Operativo	Aplicaciones de uso general, correo	Phishing, malas prácticas de navegación	Reconocimiento de amenazas, contraseñas seguras, navegación responsable	Talleres prácticos, simulaciones
Técnico / TI	Servidores, bases de datos, paneles de control	Gestión de credenciales, configuración insegura, escalamiento de privilegios	Políticas de acceso, hardening, gestión de logs	Cursos especializados, casos reales
Administrativo / Directivo	Datos sensibles, reportes, cuentas privilegiadas	Fuga de información, decisiones sin contexto técnico	Concientización sobre impacto organizacional, políticas de seguridad, cumplimiento normativo	Sesiones breves, cápsulas informativas

Nota. Elaboración propia con base en CIS Controls y NIST SP 800-50

Estrategia de Implementación del Programa de Capacitación

El éxito del programa de capacitación no depende únicamente de su diseño instruccional, sino también de una implementación planificada, progresiva y adaptada a la dinámica interna de la organización. En PYMES del sector digital, donde el ritmo operativo suele ser intenso y los

equipos son reducidos, es clave que el despliegue de las capacitaciones no interrumpa las labores diarias, pero sí logre una interiorización gradual de los conceptos de seguridad.

A continuación, se plantea una estrategia en cuatro fases que responde a criterios de eficacia, sostenibilidad y bajo costo:

Figura 4

Etapas de Implementación del Programa de Capacitación

Nota. Elaboración propia con base en el diseño instruccional propuesto en este capítulo

Fase 1. Sensibilización Inicial

Consiste en una intervención breve pero de alto impacto, como una charla motivacional o un video introductorio elaborado internamente, que logre captar la atención del personal sobre la importancia de la ciberseguridad. Puede reforzarse con materiales visuales (posters, mailing interno, infografías).

El objetivo de esta es despertar conciencia sobre riesgos comunes y su impacto directo en el negocio.

Fase 2. Capacitación por Perfil

Para proporcionar conocimientos y habilidades concretas, orientadas al rol funcional de cada colaborador. Se debe ejecutar el plan instruccional definido, diferenciando los contenidos por rol como se muestra en la tabla 4. Esta fase puede realizarse en sesiones grupales presenciales o virtuales, dependiendo del contexto de trabajo de la empresa (presencial, remoto o híbrido). Es clave asignar tiempos claros, con una agenda flexible y materiales preparados previamente.

Fase 3. Evaluación y Retroalimentación

Una vez finalizadas las sesiones formativas y con el fin de Medir el nivel de asimilación, identificar brechas y ajustar contenidos futuros, se deben aplicar mecanismos de evaluación como cuestionarios breves, análisis de casos o simulaciones. También es útil abrir un espacio para comentarios del personal sobre la utilidad percibida del programa.

Fase 4. Seguimiento Continuo

La ciberseguridad no puede tratarse como un evento único, por eso, en esta última fase se pretende mantener activa la cultura de seguridad, actualizando conocimientos según las amenazas emergentes. Es por ello que se recomienda institucionalizar acciones periódicas como:

- Boletines mensuales con noticias o tips.
- Simulacros semestrales de ataques comunes.
- Refuerzo de políticas y procedimientos internos.

Al final, con la realización de estas, se permite que la capacitación sea vista como un proceso continuo e integrado a la operación, no como una obligación puntual. También facilita su adaptación futura a nuevos requerimientos regulatorios, tecnológicos o comerciales.

Evaluación de la Efectividad del Programa de Capacitación

Medir la efectividad de un programa de capacitación en ciberseguridad es esencial para determinar si los objetivos de aprendizaje fueron alcanzados, si se ha logrado una reducción de los riesgos asociados al factor humano, y si la cultura organizacional ha incorporado prácticas seguras de manera sostenida. En el contexto de una PYME, donde los recursos para auditorías internas suelen ser limitados, se requieren instrumentos simples, pero funcionales, que permitan obtener retroalimentación accionable.

A continuación, se describen los mecanismos más relevantes para la evaluación continua del programa:

Tabla 5

Indicadores de Desempeño clave (KPIs)

Indicador	Descripción	Frecuencia sugerida
% de empleados capacitados	Proporción del personal que ha completado satisfactoriamente el programa	Trimestral o semestral
Nivel de retención del conocimiento	Resultados en pruebas o quizzes posteriores a las sesiones	Inmediatamente y a 3 meses

Indicador	Descripción	Frecuencia sugerida
Reducción de incidentes relacionados al error humano	Comparativa de incidentes antes y después de la capacitación	Semestral
Participación en simulacros	Número de usuarios que responden correctamente ante ataques simulados	Trimestral o anual
Satisfacción del usuario	Resultados de encuestas de percepción sobre la utilidad del programa	Tras cada sesión o módulo

Nota: Elaboración propia

Además de los indicadores cuantitativos previamente descritos, es recomendable incorporar algunas fuentes cualitativas que permitan obtener una visión más integral del impacto del programa. Estas herramientas complementarias ofrecen información contextual valiosa y ayudan a identificar patrones de comportamiento, percepciones del personal y oportunidades de mejora continua.

- Bitácoras de incidentes de seguridad: permiten identificar si persisten patrones de comportamiento riesgoso tras la capacitación.
- Observaciones cualitativas de líderes de área: útiles para detectar cambios en la actitud y apropiación de las políticas.
- Análisis de cumplimiento normativo: especialmente en empresas que aspiren a certificarse en ISO 27001 o similares.

La evaluación no debe limitarse a cumplir un requisito, sino que debe utilizarse para mejorar iterativamente el contenido, la metodología y la cobertura del programa. Así, la capacitación evoluciona con las amenazas y se convierte en un componente vivo dentro del

sistema de gestión de seguridad de la información (SGSI), aunque no se cuente aún con uno formalmente implementado.

Análisis crítico: Límites y Oportunidades del Programa Propuesto

Aunque el diseño del programa de capacitación presentado en este capítulo responde a criterios de pertinencia, viabilidad y escalabilidad, es necesario reconocer ciertos límites inherentes a su implementación en el contexto de las PYMES del sector digital y publicitario.

Uno de los principales desafíos radica en la resistencia al cambio organizacional, especialmente en entornos donde la seguridad informática no ha sido históricamente una prioridad. Sin el compromiso activo de los líderes, cualquier iniciativa formativa corre el riesgo de convertirse en una actividad aislada y simbólica, sin impacto real en la cultura corporativa.

Otro límite importante es la dificultad para medir el impacto de la capacitación en la reducción del riesgo, sobre todo cuando no existe un sistema estructurado de gestión de incidentes o cuando los registros de fallas no se documentan de forma rigurosa. En estos casos, se recomienda establecer indicadores simples pero constantes, como los simulacros de phishing o encuestas de validación de políticas internas.

Por otro lado, el programa representa una oportunidad valiosa para posicionar la ciberseguridad como un eje transversal dentro de la organización, incluso sin grandes inversiones. A través de herramientas gratuitas, materiales de acceso abierto y metodologías activas, es posible lograr una transformación progresiva en el comportamiento de los colaboradores.

Además, el enfoque por roles permite que cada área se sienta parte del proceso, y no como simple destinataria de instrucciones externas. Esto fortalece la noción de que la seguridad

no es responsabilidad exclusiva del área técnica, sino una responsabilidad compartida que requiere el compromiso de toda la organización.

Este programa de capacitación se articula como componente fundamental de la guía práctica de ciberseguridad propuesta, al fortalecer desde el factor humano la postura organizacional frente a los riesgos compartidos que caracterizan al entorno digital del sector publicitario.

En conclusión, la propuesta formativa aquí desarrollada no pretende reemplazar a un SGSI formal, pero sí actuar como catalizador para la construcción de una cultura organizacional más consciente, resiliente y preparada frente a un entorno digital en constante evolución.

Conclusiones

El presente trabajo permitió analizar, desde una perspectiva estratégica y técnica, los desafíos que enfrentan las pequeñas y medianas empresas del sector digital frente a la protección de la información, especialmente en contextos donde el trabajo con terceros es frecuente y las capacidades internas en ciberseguridad son limitadas.

A lo largo del documento se evidenció que, si bien existen marcos normativos y técnicos ampliamente reconocidos como la ISO/IEC 27001, NIST y los Controles CIS, su aplicación en las PYMES requiere adaptaciones específicas que contemplen tanto su capacidad operativa como su nivel de madurez tecnológica. No se trata de una mera implementación documental, sino de transformar la cultura organizacional hacia una visión proactiva de la seguridad como valor estratégico.

El análisis crítico realizado en el capítulo 2 permitió establecer que la combinación de lineamientos de diferentes marcos puede ofrecer una solución más integral para las PYMES, al permitir abordar desde la gestión de activos hasta el monitoreo continuo, pasando por la concienciación del personal y el cumplimiento regulatorio. Esto cobra aún más relevancia en sectores como el publicitario, donde la reputación digital es un activo clave y donde las operaciones suelen ser altamente expuestas al entorno digital.

Finalmente, el diseño del programa de capacitación interna presentado en el capítulo 3 refuerza la idea de que una cultura de seguridad no se impone, sino que se construye mediante procesos pedagógicos continuos, diferenciados por rol y orientados a reducir el riesgo desde la raíz: el comportamiento humano. La propuesta no solo es viable desde el punto de vista operativo, sino también sostenible en el tiempo, especialmente si se acompaña de mecanismos simples de evaluación y mejora.

Finalmente, este trabajo, contribuye a la reflexión sobre cómo aplicar estándares internacionales de seguridad en entornos locales con limitaciones reales, y ofrece una hoja de ruta práctica para avanzar hacia la madurez en ciberseguridad sin depender exclusivamente de infraestructura tecnológica o certificaciones formales.

Referencias Bibliográficas

Aguilar Antonio, Juan Manuel (2021). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior.* http://www.scielo.cl/scielo.php?script=sci_abstract&pid=S0719-37692021000100169&lng=es&nrm=iso&tlng=es

Almaraz Josue, Perez Diaz Jesus y otros (2022). *Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset.* https://www.researchgate.net/publication/364265728_LATAM-DDoS-IoT_Dataset

Banco Interamericano de Desarrollo (BID). (2017). Impact of Digital Security Incidents in Colombia. https://publications.iadb.org/publications/english/document/Impact-of-Digital-Security-Incidents-in-Colombia-2017.pdf

Bustillos Olda, Rojas Javier (2022). *Protocolo básico de ciberseguridad para pymes.* https://dialnet.unirioja.es/servlet/oaiart?codigo=9039514

Cano Jeimy. (2022). *Prospectiva de ciberseguridad nacional para Colombia a 2030.* https://research-ebsco-com.bibliotecavirtual.unad.edu.co/c/qcagk4/viewer/pdf/loliack6hf

Chaves Cepik, Marco Aurélio, Marcelino, Henriques Manuel. (2021). *Segurança cibernética em Moçambique: conceitos, infraestrutura e desafios de implementação.* https://research-ebsco-com.bibliotecavirtual.unad.edu.co/c/qcagk4/search/details/iiebj4seqv?q=incidentes%20seguridad%20infraestructuras%20criticas

Check Point Software. (2024). *Latin American Orgs See More Cyberattacks Than the Global Average. Dark Reading.* https://www.darkreading.com/cybersecurity-analytics/latin-american-orgs-more-cyberattacks-global-average

Delgado Renzo, Guerreo Milton y otros (2023) *Buenas prácticas para la adopción del marco de seguridad digital para sistemas de control industrial en activos críticos nacionales.* https://www.researchgate.net/publication/377302461_Buenas_practicas_para_la_adopcion_del_marco_de_seguridad_digital_para_sistemas_de_control_industrial_en_activos_criticos_nacionales

Diaz Jimenez, Cesar David; Ariza Rodriguez, Edgar y otros (2023). *La Ciberseguridad en las Pymes* http://hdl.handle.net/10882/12818

Dorairajan Veena S. *Cybersecurity and Organisational Performance –the Interplay (2024).* https://www.researchgate.net/publication/382019607_Cybersecurity_and_Organisational_Performance_-_the_Interplay

ESET. (2023). ESET Security Report 2023: *Panorama de ciberamenazas en América Latina.* https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

ESET. (2024). ESET Security Report 2024: *Informe de ciberseguridad en América Latina.* https://www.eset.com/py/security-report/

Especial Directivos (2021) *Cómo mejorar la ciberresiliencia de una empresa paraprotegerla de ciberataques.* https://research-ebsco-com.bibliotecavirtual.unad.edu.co/c/qcagk4/viewer/pdf/lg3zhgm6nb

Falconi Ayón, P. M., Briones García, S. S., Falconí Ayón, P. M., & Menéndez Macías, F. G. (2024). *Crimen organizado, una mirada reflexiva y análisis de estado actual. Revista científica arbitrada Múltidisciplinaria* PENTACIENCIAS, 6(1), 63–81. https://doi-org.bibliotecavirtual.unad.edu.co/10.59169/pentaciencias.v6i1.956

Flórez Rojas, Nicolas Felipe; León Rubio, Yohan Leon (2024). *El increíble impacto del ransomware en Colombia.* (2024) https://hdl.handle.net/20.500.12494/56308

García Arturo (2023). *La ciberresiliencia ante la inevitabilidad de los ciberataques* https://www.researchgate.net/publication/371925419_La_ciberresiliencia_ante_la_inevitabilidad_de_los_ciberataques

Gil Arenas, Diego Alonso., Alvarez Arboleda, Carlos Augusto., Trujillo-Vargas, Laura Marcela. (2025) Gestión del riesgo y evaluación de la eficacia de los controles de mitigación en las empresas de servicios públicos de Antioquía, Colombia. REDER, Revista de Estudios Latinoamericanos sobre Reduccion del Riesgo de Desastres. Volume 9, Páginas 67 – 79 Recuperado de https://doi.org/10.55467/reder.v9i1.178

Jiménez Calderón, Cristian David; Mendoza Tuay, Diego Albert. y otros (2024). *Hacking ético y cibercultura: impacto en el entorno laboral.* https://repository.libertadores.edu.co/bitstreams/8394711a-f1cf-4419-b510-92a6b8fe6b59/download

Kamlofsky Jorge, Gonzalez Gerardo, Trigo Santiago (2021) *Desarrollo de una guía para el abordaje de incidentes de ciberseguridad en infraestructuras críticas industriales.* https://www.researchgate.net/publication/351943535_Desarrollo_de_una_Guia_para_el_abordaje_de_Incidentes_de_Ciberseguridad_en_Infraestructuras_Criticas_Industriales

Kumar, S. (2024). *Colombia Cyber Security Market Size, Share, Growth & Demand. LinkedIn.* https://www.linkedin.com/pulse/colombia-cyber-security-market-size-share-growth-demand-satyam-kumar-luudc

Ladino Fernández, J. M., Briceño Barrero, D. L., & Rodríguez Rojas, L. A. (2022). *Industria 4.0: el reto para las pymes manufactureras de Bogotá, Colombia.* Revista Mutis, 12(1), 110–127. https://doi-org.bibliotecavirtual.unad.edu.co/10.21789/22561498.1784

Latin Lawyer. (2024). *Mitigating Risk: Data Breaches and Cyber Incidents Surge in Latin America.* https://latinlawyer.com/guide/the-guide-corporate-compliance/fifth-edition/article/mitigating-risk-data-breaches-and-cyber-incidents-surge-in-latin-america

López Rojas, Edgar Mauricio; Larrahondo Núñez, Alexander y otros. (2023). *Uso de dispositivos de bajo costo como alternativa para la implementación de IDS en las pymes* https://revista.uisrael.edu.ec/index.php/ro/article/view/918

López-Anchala, Karina Alejandra; Ordóñez-Parra, Yanice Licenia (2024). *Auditoría y ciberseguridad en el sector comercial: Evaluación de resiliencia ante amenazas digitales.* https://rperspectivasinvestigativas.org/index.php/multidiscipinaria/article/view/154

MARSH. (s.f) *Estado del riesgo cibernético en Latinoamérica en tiempos del COVID-19.* https://www.marsh.com/co/services/cyber-risk/insights/report-cyber-risk-in-latin-america-in-times-of-covid19.html

Martínez Vázquez, Francisco (2020). *Ciberseguridad y Estado autonómico: Cybersecurity and Autonomic State.* https://dialnet.unirioja.es/servlet/articulo?codigo=7474190

Mendoza José Eduardo, Larios Emigdio (2021). *Gestión de riesgos y continuidad del negocio sobre la seguridad informática en el sector retail en méxico.* https://research-ebsco-com.bibliotecavirtual.unad.edu.co/c/qcagk4/viewer/pdf/pxt4rwz44z

Mitratech. (2024). *2024 Third-Party Risk Management Study.* https://mitratech.com/resource-hub/blog/2024-third-party-risk-management-study/

Peña Martha del Pílar, Moreno Ana (2024) *Amenazas emergentes en la computación en la nube: desafíos de seguridad y respuesta.* https://research-ebsco-com.bibliotecavirtual.unad.edu.co/c/qcagk4/viewer/pdf/qiowls7x2b

Piñon, Laura C; Sapién, Alma L; Gutierrez, Maria del C. (2023). *Capacitación en ciberseguridad en una empresa mexicana.* https://www.scielo.cl/scielo.php?pid=S0718-07642023000600043&script=sci_arttext

PwC. (2024). *Vendor Cybersecurity Risk Management.* https://www.pwc.com/us/en/services/audit-assurance/digital-assurance-transparency/vendor-cybersecurity-risk.html

Santoro Javier, Rodríguez Ricardo. (2016). *Propuesta de adaptación del Framework de ciber seguridad de NIST a los sectores que soportan infraestructuras críticas en Colombia: enfoque sobre el sector de las telecomunicaciones.* https://repository.unipiloto.edu.co/handle/20.500.12277/2729

Serna, J. C., Villamizar-Jaimes, A. E., & Vallejo, S. L. (2024). Modelo Económico de implementación de un marco de seguridad de la información para las Organizaciones Colombianas. AiBi Revista De Investigación, Administración E Ingeniería, 12(2), 41–48. Recuperado de https://doi.org/10.15649/2346030X.3669

Signorino Barbat, A. (2022). *Los seguros cibernéticos: alcance frente a los ciber riesgos. Revista Ibero-Latinoamericana de seguros,* 31(57), 231–247. https://doi-org.bibliotecavirtual.unad.edu.co/10.11144/Javeriana.ris57.scaf

Urbanovics, Anna; Guajardo, Rodrigo. (2022). *Estrategias de ciberseguridad en los paises latinoamericanos – un análisis comparativo.* https://www.iskolakultura.hu/index.php/acthisp/article/view/43979

Apéndices

Apéndice A

Glosario

Autenticación multifactor (MFA)

Mecanismo de seguridad que requiere más de un método de verificación para permitir el acceso a un sistema, combinando al menos dos de los siguientes factores: algo que el usuario sabe (contraseña), algo que tiene (token) o algo que es (biometría).

Brecha de seguridad

Vulnerabilidad o falla que permite comprometer la confidencialidad, integridad o disponibilidad de la información, ya sea por errores humanos, fallas técnicas o ataques deliberados.

Ciberseguridad

Conjunto de prácticas, herramientas y políticas orientadas a proteger los sistemas informáticos, redes y datos frente a accesos no autorizados, alteraciones o destrucción.

Controles CIS (Center for Internet Security)

Conjunto de recomendaciones prácticas para proteger activos digitales, organizadas por niveles de priorización. Especialmente útiles para pequeñas y medianas empresas.

Gestión de Incidentes

Proceso estructurado para detectar, responder, registrar y aprender de eventos que comprometen o pueden comprometer la seguridad de la información.

ISO/IEC 27001:2022:

Norma internacional que establece requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización.

Malvertising

Se refiere a la práctica de insertar código o contenido malicioso en anuncios legítimos en línea. Los cuales se distribuyen posteriormente a través de redes o plataformas de publicidad en línea que muestran anuncios en diversos sitios web.

Phishing

Técnica de ingeniería social mediante la cual un atacante engaña a un usuario para que revele información confidencial (como contraseñas o datos bancarios) simulando ser una fuente confiable.

PYMES

Pequeñas y medianas empresas, caracterizadas por tener una estructura organizacional reducida, recursos limitados y operar principalmente en mercados locales o nichos específicos.

Riesgo Compartido

Situación en la que dos o más organizaciones comparten la responsabilidad por la seguridad de los datos o sistemas, común en relaciones de tercerización o subcontratación de servicios digitales.

Sistema de Gestión de Seguridad de la Información (SGSI)

Estructura organizativa que permite gestionar, monitorear y mejorar la seguridad de la información de manera sistemática, basándose en normas como ISO/IEC 27001.