European Public & Social Innovation Review

ISSN 2529-9824

Artículo de Investigación

Estrategias de ciberseguridad para MiPymes del sector terciario

Cybersecurity Strategies for SMEs in the Tertiary Sector

Alexander Gordillo-Gaitán: Corporación Universitaria Minuto de Dios - UNIMINUTO, Colombia.
alexander.gordillo.g@uniminuto.edu

Fecha de Recepción: 06/06/2024

Fecha de Aceptación: 03/07/2024

Fecha de Publicación: 09/07/2024

Cómo citar el artículo (APA 7ª):

Gordillo-Gaitán, A. (2024). Estrategias de ciberseguridad para MiPymes del sector terciario [Cybersecurity Strategies for SMEs in the Tertiary Sector]. *European Public & Social Innovation Review*, 9, 01-19. https://doi.org/10.31637/epsir-2024-293

Resumen:
Introducción: Importancia de un Sistema de Vigilancia Tecnológica en ciberseguridad para MiPymes de Fusagasugá, dada la creciente transformación digital. **Metodología:** Evaluación del conocimiento en ciberseguridad y determinación de áreas vulnerables en hogares geriátricos, gastrobares y hoteles. **Resultados:** Identificación de riesgos y establecimiento de normas para anticipar y fortalecer la protección de información digital. **Discusión:** Análisis de vulnerabilidades específicas en MiPymes y la necesidad de priorizar medidas de protección. **Conclusiones:** Implementar normas y medidas específicas en ciberseguridad para proteger datos en MiPymes del sector terciario.

Palabras clave: MiPymes; ciberseguridad; estándares; superficies de ataque; estrategias de seguridad informática; transformación digital; industria 4.0; vigilancia tecnológica.

Abstract:
Introduction: Importance of a Cybersecurity Technology Watch System for MSMEs in Fusagasugá, given the increasing digital transformation. **Methodology:** Assessment of cybersecurity knowledge and determination of vulnerable areas in geriatric homes, gastrobars and hotels. **Results:** Identification of risks and establishment of standards to

anticipate and strengthen the protection of digital information. Discussion: Analysis of specific vulnerabilities in MSMEs and the need to prioritise protection measures. Conclusions: Implement specific cybersecurity standards and measures to protect data in MSMEs in the tertiary sector.

Keywords: SMEs; Cybersecurity; Standards; Attack surfaces; IT security strategies; Digital transformation; Industry 4.0; Technology surveillance.

1. Introducción

La transformación digital acoge a las MiPymes de Fusagasugá con la tecnología de la industria 4.0, y están cambiando la forma en la que las empresas producen y distribuyen sus productos, incorporando nuevas herramientas para agilizar sus operaciones como: el Internet de las Cosas (IoT), análisis y *cloud computing*, Inteligencia Artificial (IA) y *machine learning*, entre otras (IBM, 2022). Por ende, la ciberseguridad se ha convertido en un pilar fundamental para salvaguardar y proteger la información de las organizaciones, especialmente en aquellas que no posen sistemas tan complejos como lo son las micro, pequeñas y medianas empresas (MiPymes) (Sánchez-Sánchez *et al*., 2021). Estas empresas cumplen un papel importante en la generación de empleo, y poco a poco han comenzado a integrarse en esta transición digital para combatir los riesgos y vulnerabilidades que amenacen la información de sus recursos o datos de sus clientes que se encuentres almacenados digitalmente (Gamboa-Salinas *et al*., 2023a).

Por estas razones las MiPymes deben de empezar a implementar sistemas de gestión de seguridad de la información utilizando metodologías, herramientas de software, hardware e infraestructura que puedan impedir la vulnerabilidad de la información, y también aplicando vulnerabilidad o protocolos los cuales puedan salvaguardar los datos personales como los procesos de transacciones tanto de los clientes como de las empresas (Aguilar-Campoverde *et al*., 2017; Albarracín *et al*., 2014; Jones *et al*., 2016). Para ello, en el siguiente documento se realizará una vigilancia tecnológica pasiva con el objetivo de identificar las distintas normativas, *framework* y protocolos de seguridad informática que existen para empresas y que estrategias se pueden utilizar para construir un marco de ciberseguridad para las MiPymes del sector terciario de Fusagasugá con base en los criterios que tiene este sector.

En el estudio realizado por Coronel-Ayala y López-Sevilla en 2023, se diseñó una herramienta para recopilar datos claves sobre la seguridad informática y ciberseguridad de las organizaciones en proceso de transformación digital. La herramienta de captura de información cuantitativa se basó en dos preguntas fundamentales: ¿Cuáles son los principales riesgos de ciberseguridad que enfrenta su organización? y ¿Cuáles son las expectativas en materia de seguridad de datos? (Coronel-Ayala y López-Sevilla, 2023).

En este estudio también se tuvieron en cuenta las distintas opiniones que tienen los diferentes establecimientos del sector terciario por medio de una encuesta cuantitativa, de esta forma se evaluó el nivel de conocimiento sobre ciberseguridad en estas empresas, y a partir de esto, poder brindarles recomendaciones que fortalezcan sus entornos de información digital. Además, se pudo determinar cuál de los tres sectores que se estudiaron (hogares geriátricos, gastrobares y hoteles) presentan cada día más vulnerabilidades, con el objetivo de determinar que superficies de ataque requieren una mayor atención en términos de ciberseguridad.

Por último, se realizó un cuadro en donde se caracterizan los estándares internacionales más importantes para la industria con respecto a la seguridad de la información, las superficies de ataque que se vinculan con las empresas del sector terciario y su comercio electrónico. El análisis de los instrumentos de encuesta con el fin de impactar positivamente las MiPymes que se encuentran en proceso de una transición digital visibilizando la relevancia que tiene la información digital sobre sus datos y tomen medidas preventivas ante un ciberataque (Gamboa-Salinas *et al*., 2023b).

La ciberseguridad es una competencia que las empresas progresivamente han estado utilizando para la protección de la información y de sus activos. Las MiPymes se han visto preocupadas por los crecientes casos de amenazas y ciberataques (Díaz-Piraquive *et al*., 2023; Mertens, 2010; Permatasari *et al*., 2024), los cuales conllevan a que dichas organizaciones empiecen a tomar las medidas necesarias para evitar que se presenten este tipo de problemas.

Según estadísticas hasta el tercer trimestre del 2023 el CSIRT de Gobierno (Centro de Respuesta a Incidentes de Ciberseguridad), se registraron en Colombia 29.000 ciberataques a infraestructuras empresariales, que afectaron la continuidad de las operaciones a través de fraudes financieros y suplantación de identidad digital (Roldan, 2023).

Bustillos y Rojas (2023) en su artículo titulado *Cómo promueven los estados la ciberseguridad de las Pymes*, se resalta que, en los primeros ocho meses de 2021, en América Latina se produjeron 728 millones de intentos de ataques cibernéticos, lo que equivale a un promedio de 35 ataques por segundo. Esto representó un aumento del 24% en comparación con el mismo período del año anterior. Se estima que alrededor del 40% de los ataques exitosos que causan daños significativos se dirigen a las pequeñas y medianas empresas (Pymes), causando consecuencias tan graves que en muchos casos estas empresas no tienen una recuperación económica, de información y reputación (Bustillos y Rojas, 2022; Ortega y Segura, 2023).

Mediante un informe de Ciberseguridad de la Cámara Colombiana de Informática y Telecomunicaciones, CCIT (Misión PYME, 2023). Se demostró que durante el 2022 varios sectores se vieron afectados por los ciberataques, entre ellos, las empresas y entidades del sector público y privado, registrando un porcentaje mayor de un 67% del total de las denuncias, presentado. Esto como consecuencia llevó a que Colombia se ubicara como el tercer país con mayor cantidad de intentos de ciberataques en América Latina.

Por ello es importante conocer las medidas necesarias que se deben tomar al momento de presentarse ciberataques a este sector económico. Se realizó un análisis bibliográfico sobre los distintos modelos y protocolos que están gestionando las MiPymes en distintas partes del mundo, y como logran reaccionar ante las vulnerabilidades, amenazas y ataques a sus sistemas de información. establecerá partir de las superficies de ataque de las empresas tipo hoteles, gastrobares y centros geriátricos; a partir de resultados de una encuesta a las MiPymes del sector terciario de Fusagasugá que implementan acciones limitadas ante estos ciberataques y las herramientas tienen a su disposición para evitar ser afectadas por estos problemas.

El avance de las Tecnologías de la Información y las Comunicaciones (TIC), junto con la computación en la nube y la llegada de innovadores sistemas de telecomunicaciones como el 5G, ha dado lugar a la idea de una conectividad omnipresente y un amplio conjunto de recursos, almacenamiento y servicios. Esta enorme transformación ha generado nuevos tipos de amenazas a la seguridad, principalmente debido al notable incremento de las superficies

de ataque, que ahora puede ser aprovechada por usuarios malintencionados. Aunque los ataques maliciosos se vuelven cada vez más complejos, las MiPymes y las organizaciones públicas siguen mostrando demoras y limitaciones a invertir en ciberseguridad (Tselios *et al*., 2022).

Debido a que las MiPymes no disponen de la misma cantidad de recursos que pueden tener las empresas de mayor tamaño, van a requerir de herramientas y métodos de protección diferentes (Cyber Readiness Institute, 2021). Por lo tanto, los gobiernos pueden generar espacios, directrices y normativas para que las empresas logren tener un referente de cómo gestionar estrategias que permitan evaluar los riesgos y amenazas (Guevara-Vega *et al*., 2023; Ospina-Díaz Sanabria-Rangel, 2020).

Así mismo, las MiPymes deben entender la importancia y el impacto que tendrá el uso de las TIC, las cuales pueden llegar a mostrar una mejora no solo en la seguridad, sino también en el desempeño financiero, operacional y comunicación de relaciones entre cliente y proveedor, si se utilizan adecuadamente; generando contribuciones importantes para las empresas como: Mayor visibilidad, procesar más información y facilitar el intercambio de comunicación y transacciones financieras (Buenrostro-Mercado *et al*., 2019; Cuevas-Vargas *et al*., 2016; Núñez, 2020).

En cualquier caso, las MiPymes deben conocer cual son las modalidades que utilizan los ciberdelincuentes con más frecuencia, de modo que con ayuda de los recursos y las herramientas dispuestas puedan combatir estos riesgos especialmente para hoteles y empresas con atención al cliente (Cabezas-Azuero, 2023; Gómez-Córdoba *et al*., 2020; Lechuga-Cardozo *et al*., 2022; López-Rojas, 2022). Las modalidades van desde *Skimming* hasta la *estafa cibernética*, también se encuentra la denominada *carta nigeriana*, el *Vishing* y el *malware* o software malicioso mediante correos, mensajes y otras modalidades de ingeniería social con información sensible o llamativa (Rosas-Prado, 2022).

La investigación de Arroyabe M.F *et al*. explora en cómo las pequeñas y medianas empresas (Pymes) que abarcan la industria 4.0 perciben el temor a la ciberdelincuencia, entendiendo este miedo como la preocupación por los riesgos asociados al cibercrimen y sus potenciales repercusiones. Después de una exploración de una base de datos de la Unión Europea que incluye a 12.863 Pymes de los países miembros, el estudio contribuye al desarrollar una taxonomía fundamentada en las percepciones de las pymes respecto al miedo de ciberataques (Arroyabe *et al*., 2024).

La captura de datos a MiPymes del sector terciario de Fusagasugá realizado por Hernández-Lozano y Gordillo-Gaitán (2023) implementaron un instrumento basado en una encuesta que capturaba datos relacionados con la gestión de seguridad de la información y retos específicos de estas organizaciones. El instrumento diseñado plantea preguntas de ciberseguridad en procedimientos de negocios y otros temas relevantes. Después de recopilar la información, realizaron en análisis sistemático para la identificación comunes entre las MiPymes encuestadas (Lozano-Hernández y Gordillo-Gaitán, 2023).

Por lo anterior, las MiPymes deben de analizar y comprender como funciona cada modalidad y que áreas de la empresa se verían afectadas, con el fin de aplicar las medidas puntuales ante las vulnerabilidades que se presenten (Alahmari y Duncan, 2020). Por consiguiente, las empresas podrían aplicar distintos métodos de protección como: autenticación multifactorial, controles de acceso sólidos, compromiso de seguridad a terceros, capacitar a los empleados sobre seguridad, generar copias de seguridad, conocer las actualizaciones de los softwares empresariales e instalar firewalls y antivirus en los equipos

de la empresa (Cámara de Comercio de Bogotá, 2023). Seguidamente, se recomienda realizar la implementación de la norma ISO/IEC 27701 la cual es una extensión de la ISO/IEC 27001 y los controles de seguridad ISO/IEC 27002 (Rosas-Prado, 2022).

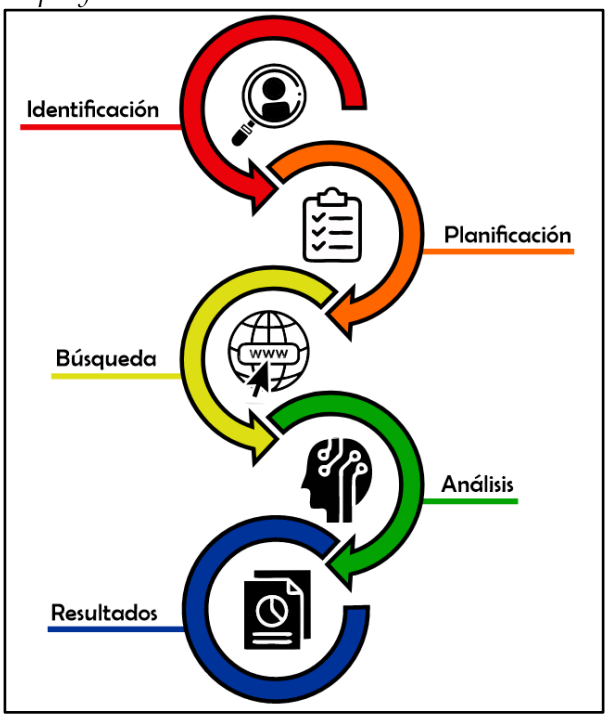
2. Metodología

La ciberseguridad es un área de la tecnología que en la última década ha tomado una enorme importancia para la protección de la información y los sistemas de cualquier organización, y las pequeñas y medianas empresas no son la excepción. Por esta razón, se desarrolló del proyecto: "Marco de gestión de ciberseguridad para las MiPymes del sector terciario del municipio de Fusagasugá", Cundinamarca, con el propósito de establecer medidas efectivas para enfrentar y prevenir los riesgos de ciberataques aplicando el proceso de Vigilancia e Inteligencia de la norma UNE 166006. Para ello, el proyecto se divide en cinco fases (ver Figura 1):

Fase 1 - Identificación de fuentes y recursos de información: La primera etapa se identificaron las fuentes y recursos de información externas e internas disponibles tomando en cuenta bases de datos académicas como la IEEE, *Scopus* y *Web of Science*. Se realizó la extracción de información científica, técnica y tecnológica no mayor a 5 años de antigüedad. Se desarrollan los instrumentos de captura de información cuantitativa para las organizaciones.

Figura 1

Etapas de la metodología del proyecto



Fuente: UNE 166006:2018 Gestión de La I+D+i: Sistema de Vigilancia e inteligencia, 2018

Fase 2 - Planificación de la vigilancia tecnológica: La segunda etapa se realizó la planificación de la ejecución del proceso de vigilancia e inteligencia basados en la norma UNE 166006 (Lambide-Heziketa, 2019). Se identificaron los criterios de la fórmula para las búsquedas en las fuentes de información.

Fase 3 – Búsqueda y validación de la información: La tercera etapa se recopiló la información, se discriminó por año, y se correlacionó con las MiPymes del sector terciario de Fusagasugá – Colombia y se validó cual es la que satisface los criterios planificados.
Fase 4 – Análisis estadístico: La cuarta etapa se realizó un tratamiento estadístico descriptivo a los resultados de las encuestas realizadas a las organizaciones y se extraen datos relevantes para identificar relaciones y características de los contenidos para que puedan ser procesados.
Fase 5 – Resultados a partir de la interpretación y estrategias: Finalmente, en la en la quinta etapa, se realizó la interpretación de la información para determinar las estrategias relevantes para la toma de decisiones en la construcción de un Framework de protección digital y ciberseguridad para MiPymes de Fusagasugá.

3. Resultados

Las MiPymes del sector terciario de Fusagasugá desconocen los controles y estrategias de protección que pueden implementar ante los ciberataques que afectan factores como la integridad, confidencialidad y disponibilidad de su información digital, además de los datos (De Jesús y Barraza, 2019). Y de qué manera están impulsando la concientización de la importancia de la ciberseguridad.

Por lo tanto, se realizó un trabajo de campo implementando un instrumento tipo encuesta en la cual se pretende evaluar cual es el concepto que tienen estas empresas sobre la protección de sus datos de los sectores más vulnerable ante los ciberataques. Como resultado del 100% de las MiPymes encuestadas el 11,53% corresponde al sector de los hogares geriátricos, el 69,23% corresponde a gastrobares y finalmente el 19,23% corresponde al sector de hotelería (ver Figura 2).

Figura 2

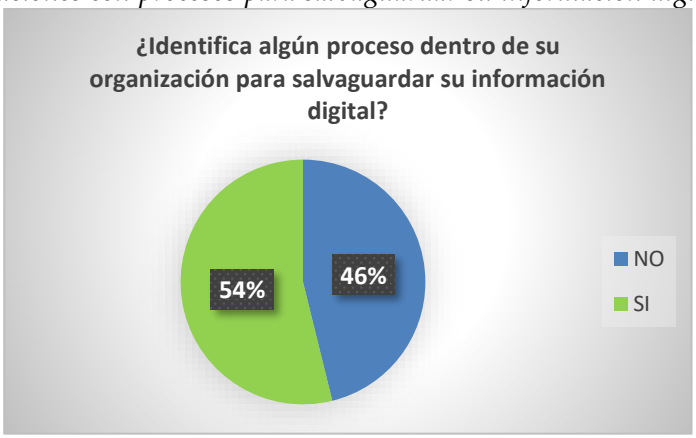
Resultados de la encuesta sobre la percepción de Ciberseguridad que tienen las MiPymes del sector terciario de Fusagasugá

Fuente: Elaboración propia (2023)
Nota. Las preguntas realizadas se centraron en la implementación y percepción de seguridad informática de las MiPymes del sector terciario de Fusagasugá

Para analizar los resultados que se obtuvieron a partir de las preguntas centradas en la seguridad informática, se realizó un desglose de los resultados con el objetivo de identificar las tendencias y patrones que podrían estar presentando en los determinados sectores. Por lo tanto, se observa lo siguiente:

Figura 3

Porcentaje de organizaciones con procesos para salvaguardar su información digital



Fuente: Elaboración propia (2023)

Nota. Adicionalmente indica el conocimiento básico sobre seguridad informática de la MiPyme entrevistada

Se logra visualizar que más de la mitad de las organizaciones encuestadas tienen medidas o protocolos para proteger su información digital, lo cual demuestra el interés y la importancia que tienen sobre la seguridad de la información tanto de sus clientes como la de sus activos. Sin embargo, hay que considerar de la Figura 3 el otro 46% debido a que este porcentaje representa la mitad de las organizaciones de los establecimientos que no tienen un proceso para salvaguardar su información digital.

Figura 4

Porcentaje de los sectores con procesos para salvaguardar su información digital

Fuente: Elaboración propia (2023)

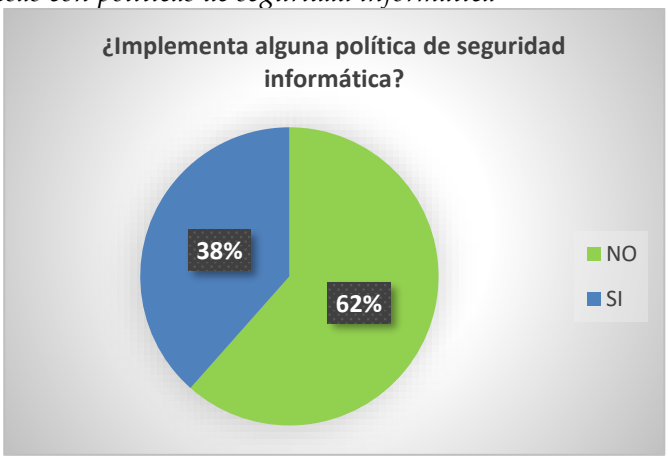
Nota. Adicionalmente se analizó el lenguaje utilizado y la facilidad de identificar controles de seguridad informática para indicar un conocimiento básico-medio.

Se identifica en la Figura 4 un porcentaje considerable con respecto al proceso para la seguridad de la información digital por parte del sector de los hogares geriátricos,

representando un porcentaje del 7,7%. El sector de hoteles también representa una cifra alta de un 15,4% con respecto a los establecimientos que declaran tener un proceso para salvaguardar su información digital, siendo una cifra considerable teniendo en cuenta la cantidad de datos de clientes que registra este sector. Por otra parte, se evidencia que existe una brecha significativa en el sector de los gastrobares, debido a que la proporción que no identifica procesos es alta, representando un 38,30% con respecto a los demás sectores, esto indica que se deben tomar medidas para promover la implementación de procesos y controles adecuados para proteger la información digital en el sector de los gastrobares.

Figura 5

Porcentaje de las empresas con políticas de seguridad informática

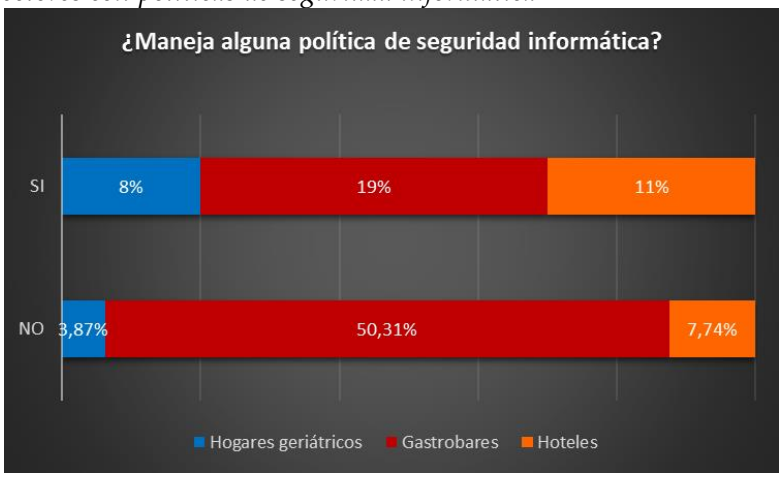


Fuente: Elaboración propia (2023)

Los resultados de la Figura 5 indican una cifra relevante del 62%, la cual demuestra que un alto porcentaje de los establecimientos encuestados no tiene políticas de seguridad informática. Esto puede representar una gran preocupación, debido a que una política de seguridad informática sólida es fundamental para proteger los activos digitales y la información confidencial de una organización.

Figura 6

Porcentaje de los sectores con políticas de seguridad informática



Fuente: Elaboración propia (2023)

Es importante señalar que la mayoría de los establecimientos encuestados en el sector de los gastrobares no cuentan con políticas de seguridad informática, representando el porcentaje más alto con un 50,31% en comparación con otros sectores (Ver Figura 6). A diferencia de los otros dos sectores que muestran porcentajes bajos: un 3,87% para los hogares geriátricos y un 7,74% para los hoteles, los cuales no han implementado políticas de seguridad de información. Esto nos da a entender la importancia que tienen estos sectores por proteger la información de sus clientes, debido a que en estos sectores manejan mucha información sensible (López-Rojas, 2022; Niño-García, 2022).
Por lo tanto, es fundamental promover la adopción de políticas de seguridad informática en el sector de los gastrobares debido a que ellos también manejan datos importantes por medio de sus transacciones las cuales involucran información financiera y personal que requieren protección especial (PCI Security Standards Council, 2021).

Figura 7

Porcentaje del nivel de importancia que tienen los establecimientos con respecto a la información de sus clientes y proveedores

Fuente: Elaboración propia (2023)

Los resultados indican que existe solo un pequeño porcentaje que califica como indiferente (7,7%) o de baja relevancia (7,7%) a la información de sus clientes y proveedores (Figura 7). Esto demuestra que en general, las empresas u organizaciones encuestadas valoran la información de clientes y proveedores deseando mantener un perfil confiable con relación a sus clientes y proveedores para que se sientan seguros al momento de adquirir algún producto o servicio.

Figura 8

Porcentaje del nivel de importancia que tienen los establecimientos con respecto a la información de sus clientes y proveedores

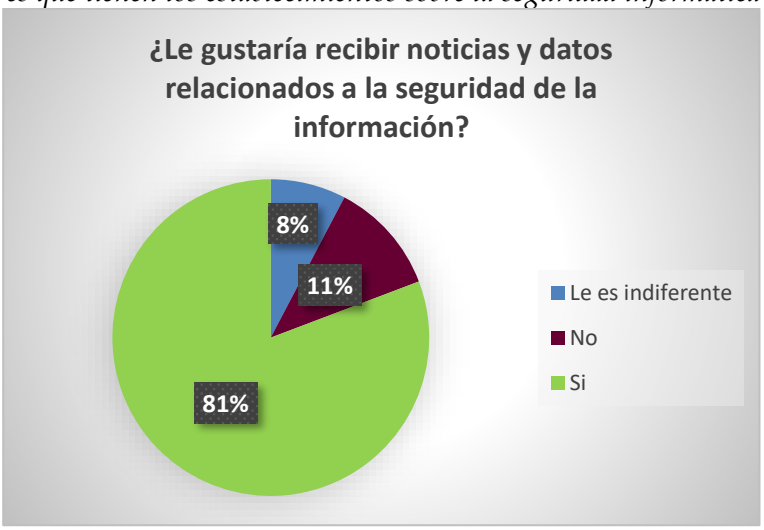
Fuente: Elaboración propia (2023)

Se visualiza en la Figura 8 que en el sector de gastrobares están con un compromiso de priorizar los datos de clientes y proveedores con un 34,65%, mientras que los hogares geriátricos, existe una división más equitativa con un 3,8% de participación en cada uno de los niveles de valoración; por último, el sector hotelero con un 15,4% de participación considera que esta información es de importancia para su empresa u organización.

Las diferentes opiniones que presentan los distintos sectores pueden ser debido a forma en la que abordan la seguridad de la información y las políticas de protección de datos, debido a que no todas manejar la misma información de sus clientes o proveedores. Sin embargo, es importante adaptar las medidas de seguridad y privacidad de los datos de acuerdo con el nivel de importancia la información en cada sector.

Figura 9

Porcentaje del interés que tienen los establecimientos sobre la seguridad informática

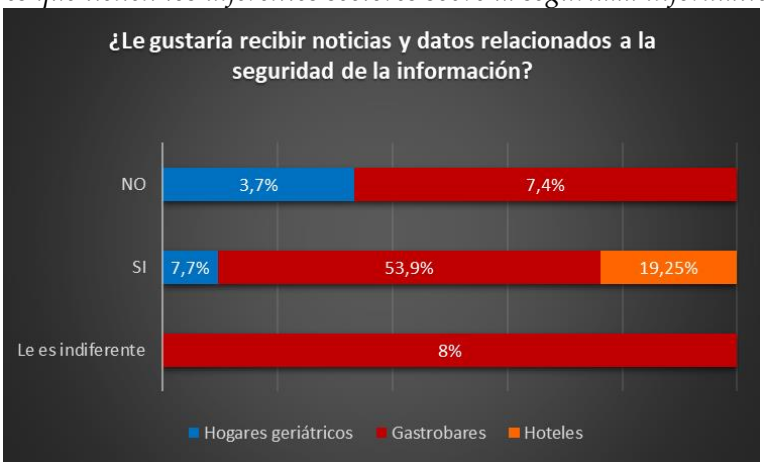


Fuente: Elaboración propia (2023)
Nota. El 81% de las organizaciones dan oportunidad de avanzar en la promoción de la seguridad informática en las MiPymes de Fusagasugá

Este último análisis de la Figura 9, la gran mayoría de los encuestados representando el 81% expresó un alto interés en recibir noticias y datos relacionados con la seguridad de la información, lo cual demuestra la preocupación que tienen las empresas por la protección y gestión adecuada de la información que manejan. De esta forma, las empresas podrán dejarse asesorar de manera más fácil para la implementación de mejoras que ayuden a proteger sus datos contra posibles ciberataques (Aguilar-Campoverde *et al*., 2017; David-Díaz *et al*., 2023; PCI Security Standards Council, 2021).

Figura 10

Porcentaje del interés que tienen los diferentes sectores sobre la seguridad informática



Fuente: Elaboración propia (2023)

Los resultados de la Figura 10 muestran que en general los tres sectores tienen un alto interés por conocer más sobre la seguridad de la información. Sin embargo, existe una minoría: un 3,7% para los hogares geriátricos y un 7,4% para los gastrobares, los cuales presentan un desinterés sobre las noticias, últimas tendencias, amenazas y buenas prácticas en ciberseguridad. Esto podría requerir mejores estrategias para concientizar a este sector minoritario sobre los beneficios que podrían tener sus establecimientos al implementar métodos para asegurar su información digital tanto a nivel personal como organizacional (Lechuga-Cardozo *et al*., 2022).

Después de analizar los distintos puntos de vista que tienen las MiPymes con respecto al manejo de sus datos y la seguridad informática, se puede concluir que la mayoría, aunque conocen la importancia que tienen la información de sus activos y clientes, no poseen o están utilizando de manera adecuada los protocolos de ciberseguridad para salvaguardar la información digital (David-Díaz *et al*., 2023; Lechuga-Cardozo *et al*., 2022).

Sin embargo, proponen iniciativa e interés por entender los procesos relacionados con la seguridad informática, por lo tanto, se realizó una caracterización de cuáles son las superficies de ataque que tienen una mayor probabilidad de vulnerabilidad en cada sector de las MiPymes encuestada, y también se darán a conocer los protocolos o estándares necesarios que se deben aplicar en cada superficie que puede ser atacada teniendo en cuenta el nivel de importancia de la información que se maneje (Tabla 1).

Tabla 1
Framework de Ciberseguridad para las MiPymes del sector terciario de Fusagasugá

Superficie de ataque	Sector	Control o acción de ciberdefensa	Norma
Transacciones	Hogares Geriátricos Gastrobares Hoteles	Protección de transacciones de los servicios de las aplicaciones	ISO/IEC 27001 (Objetivo 14.1.3)
		Autenticación y manejo de identidades	NIST 800-63
		Firewalls, encriptación, políticas de contraseñas seguras, monitoreo de la red.	PCI DSS
Página Web	Hogares Geriátricos Gastrobares Hoteles	Restricción de acceso a la información	ISO/IEC 27001 (Objetivo 9.4.1)
		Procedimiento de ingreso seguro	ISO/IEC 27001 (Objetivo 9.4.2)
		Sistema de gestión de contraseñas	ISO/IEC 27001 (Objetivo 9.4.3)
		Uso de programas utilitarios privilegiados	ISO/IEC 27001 (Objetivo 9.4.4)
		Control de acceso a códigos fuente de programas	ISO/IEC 27001 (Objetivo 9.4.5)
		Autenticación y manejo de identidades	NIST 800-63
		Controles de la información en la nube	ISO/IEC 27017
		Protocolos de correo electrónico	NIST 800-177
		Seguridad en aplicaciones informáticas	ISO/IEC 27034
		Prevención y el manejo de incidentes de *malware*	NIST 800-83
Redes Inalámbricas	Hoteles	Controles de red	ISO/IEC 27001 (Objetivo 13.1.1)
		Seguridad de los servicios de red	ISO/IEC 27001 (Objetivo 13.1.2)
		Separación en las redes	ISO/IEC 27001 (Objetivo 13.1.3)

Superficie de ataque	Sector	Control o acción de ciberdefensa	Norma
		Diseño e implementación de seguridad en redes	ISO/IEC 27033
		Aseguramiento de las comunicaciones entre redes mediante gateways de seguridad	
		Aseguramiento de comunicaciones mediante VPNs	
		Securización de redes IP wireless	
		Directrices sobre firewall y política de firewall	NIST 800-41
		Implementaciones de seguridad de la capa de transporte (TLS)	NIST 800-52
Sistemas de vigilancia	Gastrobares Hoteles	Disponibilidad de instalaciones de procesamiento de información.	ISO/IEC 27002 (Objetivo 17.2)
		Controles de la información en la nube	ISO/IEC 27017
		Aseguramiento de las comunicaciones entre redes mediante gateways de seguridad	ISO/IEC 27033-4
		Seguridad de los sistemas de control industrial (ICS)	NIST 800-82

Fuente: Elaboración propia (2023)

4. Discusión

La identificación de múltiples marcos normativos, controles y estrategias de seguridad informática permite construir un *framework* para la protección de la información digital adaptado a las características de las MiPymes del sector terciario de Fusagasugá. Este sector que poco a poco implementa servicios basados en tecnología como es el *e-commerce* y los pagos sin contacto, asumen retos de ciberseguridad que en experiencias de grandes empresas no siempre son aplicables o escalables para las MiPymes debido a diferencias en recursos, conocimiento técnico y riesgos específicos. En contraste La guía de ciberseguridad

lanzada por la Cámara de Comercio de Bogotá (CCB) que proporciona un ejemplo práctico de cómo adaptar estrategias de ciberseguridad a las necesidades y capacidades de las pequeñas empresas.

Además, la tendencia de publicaciones normativas para organizaciones se desafía debido a que sugieren una adopción uniforme de normativas y *frameworks* de ciberseguridad sin considerar el contexto específico de cada sector. Los resultados de exploración de metodologías de gestión sugieren que la efectividad de las políticas de ciberseguridad está influenciada por el contexto organizacional y sectorial. Este estudio refuerza esa noción al demostrar que un *framework* de ciberseguridad debe ser flexible y adaptarse a las características únicas de las MiPymes del sector terciario.

Desde una perspectiva práctica, La investigación lidera el fortalecimiento de la postura de ciberseguridad de las MiPymes tiene efectos positivos en la resiliencia y conocimiento preventivo de toda la comunidad empresarial de hotelería, geriátricos y gastrobares que también contribuyen a la estabilidad y seguridad del ecosistema empresarial más amplio en Fusagasugá. A pesar de los aportes significativos, este estudio literario presenta varias limitaciones para las MiPymes. En primer lugar, las organizaciones pueden no acceder a todas las normativas relevantes, especialmente aquellas que no están ampliamente publicadas o su acceso es únicamente de pago. Esto puede limitar la implementación autónoma del *framework* de ciberseguridad propuesto.

Además, la falta de datos técnicos específicos de las MiPymes de Fusagasugá puede afectar la aplicabilidad y precisión de las recomendaciones. La investigación futura debería considerar la realización de casos de implementación y encuestas a otros sectores de MiPymes para fortalecer nuevas superficies de ataque. La evaluación de las prácticas actuales de ciberseguridad en estas empresas y la identificación de áreas vulnerables en hogares geriátricos, gastrobares y hoteles proporcionarán una base empírica más sólida para la construcción de estrategias efectivas de ciberseguridad.

5. Conclusiones

El *framework* creado para la protección digital de las MiPymes se basa en la integración de enfoques interdisciplinarios que combinen ciencias de la gestión de seguridad de la información, seguridad informática y estudios sectoriales específicos para proporcionar una perspectiva más holística y robusta. Este enfoque permite desarrollar estrategias de ciberseguridad que no solo sean efectivas, sino también sostenibles y adaptables a futuros cambios tecnológicos y regulatorios.

De los resultado del análisis estadístico de las encuestas se resalta que las MiPymes del sector terciario de Fusagasugá deben empezar a evaluar los sistemas que están implementando actualmente para el almacenamiento de los datos de sus clientes y proveedores, asegurándose que las herramientas que estas utilizando para salvaguardar esta información tengan o cumplan los requisitos para responder ante los ciberataques, porque no basta con solo conocer cómo funciona la ciberseguridad sino también saber implementar una estrategia puntual para combatir un riesgo o vulnerabilidad en específico. Así mismo, deben empezar a conocer los programas que ofrece la alcaldía de Fusagasugá para las MiPymes en el tema de ciberseguridad, puesto que estas instituciones brindan distintos asesoramientos e incentiva mediante campañas sobre la importancia que tiene la ciberseguridad y la preparación cibernética en sus empresas.

Además, las empresas no deben subestimar los ataques o vulnerabilidades de ciberseguridad que podrían estar enfrentando. Por ello, es fundamental adquirir experiencia y certificaciones en este ámbito. En caso de sufrir un ataque, no deben dar por sentado que será algo temporal, ya que estos ataques pueden llegar a intensificarse y llegar a ser cada vez más repentinos.

6. Referencias

Aguilar-Campoverde, B. G., Valverde-Jaramillo, J. G. y Alvarado-Camacho, P. E. (2017). Gestión de la relación con clientes a través del uso de las tecnologías de la información y la comunicación en las Mipymes del Ecuador. *Iberian Conference on Information Systems and Technologies, CISTI*. https://doi.org/10.23919/CISTI.2017.7976031

Alahmari, A. y Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CYBERSA49311.2020.9139638

Albarracín, E. J. G., Erazo, S. C. R. y Palacios, F. C. (2014). Influence of information and communication technology on the performance of Colombian micro, small and medium enterprises. *Estudios Gerenciales*, *30*(133), 355–364. https://doi.org/10.1016/J.ESTGER.2014.06.006

Arroyabe, M. F., Arranz, C. F., De-Arroyabe, I. F. y De-Arroyabe, J. C. F. (2024). Revealing the Realities of Cybercrime in Small and Medium Enterprises: Understanding Fear and Taxonomic Perspectives. *Computers & Security*, 141, 103826. https://doi.org/10.1016/j.cose.2024.103826

Buenrostro-Mercado, H. E. y Hernández-Eguiarte, M. (2019). La incorporación de las TIC en las empresas. Factores de la brecha digital en las Mipymes de Aguascalientes. *Economía: Teoría y Práctica*, *27*(50), 101–124. https://doi.org/10.24275/ETYPUAM/NE/502019/BUENROSTRO

Bustillos, O. y Rojas, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases*, 016, 168–186. https://doi.org/10.26439/INTERFASES2022.N016.6021

Cabezas-Azuero, J. S. (2023). Tratamiento de datos personales y compliance en Colombia. *Revista de La Facultad de Derecho y Ciencias Políticas*, *53*(138), 1-25. https://doi.org/10.18566/rfdcp.v53n138.a2

Cámara de Comercio de Bogotá. (2023, septiembre 20). *La Cámara de Comercio de Bogotá lanza Guía de Ciberseguridad para pymes y fortalece su portafolio de soluciones*. https://acortar.link/UbLNnm

Coronel-Ayala, F. M. y López-Sevilla, G. M. (2023). Mapeo del panorama actual de la ciberseguridad en la era moderna digital. *Análisis del comportamiento de las líneas de crédito a través de la corporación financiera nacional y su aporte al desarrollo de las PYMES en Guayaquil 2011-2015*, *7*(2), 441–452. https://doi.org/10.26820/recimundo/7.(2).jun.2023.441-452

Cuevas-Vargas, H., Aguilera-Enríquez, L., López-Torres, G. C. y González-Adame, M. (2016). La relación entre el uso de las TICs y la innovación de las MiPymes Mexicanas. Evidencia empírica del estado de Guanajuato, México. | Cairn.info. *Recherches En Sciences de Gestion*, 1, 39–58. https://acortar.link/sOTz4f

Cyber Readiness Institute. (2021, July 20). *Fortalecimiento de la postura de ciberseguridad de la comunidad de pequeñas empresas de Estados Unidos*. https://acortar.link/OZnnnR

David-Díaz Jiménez, E., Ariza-Rodríguez, M. Y., Ruiz-Moncada, C. y Giussepe-Rodríguez, W. (2023). *La Ciberseguridad en las Pymes*. Escuela de Administración de Negocios.

De Jesús, A. y Barraza, C. (2019). *Modelo de implementación de ciberseguridad para sistemas IoT en el marco de redes 5g* [Universidad Tecnológica de Pereira]. https://hdl.handle.net/11059/12043

Díaz-Piraquive, F. N., de Jesús Muriel-Perea, Y. y González-Crespo, R. (2023). Cybersecurity Management in Micro, Small, and Medium Enterprises in Colombia. *Communications in Computer and Information Science*, 1825 CCIS, 74–85. https://doi.org/10.1007/978-3-031-34045-1_8

Gamboa-Salinas, J. M., Mancheno-Saá, M. J. y Hurtado-Yugcha, J. D. P. (2023a). Management skills and digital transition for Mipymes Zone 3-Ecuador. *Revista Venezolana de Gerencia*, *28*(101), 297–315. https://doi.org/10.52080/RVGLUZ.28.101.19

Gamboa-Salinas, J. M., Mancheno-Saá, M. J. y Hurtado-Yugcha, J. D. P. (2023b). Management skills and digital transition for Mipymes Zone 3-Ecuador. *Revista Venezolana de Gerencia*, *28*(101), 297–315. https://doi.org/10.52080/RVGLUZ.28.101.19

Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D. y Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, 1. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017

Guevara-Vega, E. M. D., Delgado-Deza, J. R. y Mendoza-de-los-Santos, A. C. (2023). Vulnerabilities and threats in information assets: a systematic review. *Revista Científica de Sistemas e Informática*, *3*(1), e461–e461. https://doi.org/10.51252/RCSI.V3I1.461

Hernández-Lozano, M. A. y Gordillo-Gaitán, A. (2023). Aplicación web que analiza y valida la seguridad y confiabilidad de los enlaces de e-commerce de las MiPymes del sector terciario de Fusagasugá - Cundinamarca. *Encuentro Internacional De Educación En Ingeniería*. https://doi.org/10.26507/paper.2873

IBM. (2022). *¿Qué es la Industria 4.0 y cómo funciona? | IBM*. https://acortar.link/AmLrmj

Jones, C., Motta, J. y Alderete, M. V. (2016). Strategic management of information and communication technologies and electronic commerce adoption in MSME from Córdoba, Argentine. *Estudios Gerenciales*, *32*(138), 4–13. https://doi.org/10.1016/J.ESTGER.2015.12.003

Lambide-Heziketa, E. (2019). *Nueva norma UNE 166006 de Vigilancia e Inteligencia*. https://acortar.link/KXJVYJ

Lechuga-Cardozo, J. I., Uran, A. U., Pérez, C. C., Ayola, M. P., Cadena, R. R. y Quintero, K. P. (2022). Acercamiento a la transformación digital en un grupo de hoteles Mipymes del caribe colombiano. *Ad-Gnosis*, *11*(11), 1–12. https://doi.org/10.21803/ADGNOSIS.11.11.532

López-Rojas, E. M. (2022). *Análisis de la seguridad para protección de pérdida de datos en las plataformas e-commerce utilizadas por las MiPymes en tiempo de pandemia* [Universidad Nacional Abierta y a Distancia UNAD]. https://repository.unad.edu.co/handle/10596/51476

Mertens, D. M. (2010). Transformative mixed methods research. *Qualitative Inquiry*, *16*(6), 469–474. https://doi.org/10.1177/1077800410364612

Misión PYME. (2023, June 12). *Pymes, las más afectadas por los ciberataques*. https://acortar.link/Bs4Gan

Niño-García, D. Y. (2022). Los datos personales y sus riesgos jurídicos a partir de la transformación digital en el comercio electrónico. *Revista CES Derecho*, *13*(1), 70–89. https://doi.org/10.21615/CESDER.6386

Núñez F., J. E. (2020). The role of information and communication technologies in micro, small and medium enterprise (MSME). Methodological approach. *Daena: International Journal of Good Conscience*, 15, 1–13.

Ortega, O. B. y Segura, J. R. (2023). Cómo promueven los Estados la ciberseguridad de las pymes. *Interfases*, 017, 21–37. https://doi.org/10.26439/INTERFASES2023.N017.6246

Ospina-Díaz, M. R. y Sanabria-Rangel, P. E. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, *62*(2). https://acortar.link/hcyELc

PCI Security Standards Council. (2021). *Protect Payment Data with Industry-driven Security Standards, Training, and Programs*. https://www.pcisecuritystandards.org/about_us/

Permatasari, D., Mohammed, N. F. y Shafie, N. A. (2024). Exploring Factors Influencing the Adoption of Cloud Accounting Systems in Indonesian Micro Small and Medium Enterprises: A Unified Theory of Acceptance and Use of Technology Based Analysis. *Management and Accounting Review*, *23*(1), 195–229.

Roldán, M. J. M. (2023, verano 10). *'Ciberseguridad a la medida' para todas las empresas de Colombia*. Portafolio.co. https://acortar.link/EYcpmc

Rosas-Prado, A. F. (2022). *El cibercrimen en Colombia y su evolución en los últimos dos años (2020-2021)* [Universidad Militar Nueva Granada]. https://repository.unimilitar.edu.co/handle/10654/43617

Sánchez-Sánchez, P. A., García-González, J. R., Triana, A. y Perez-Coronell, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Tecnológica*, *32*(5), 121–128. https://acortar.link/ltnzUk

Tselios, C., Politis, I. y Xenakis, C. (2022). *Improving Network, Data and Application Security for SMEs*. Proceedings Of The 17th International Conference on Availability, Reliability And Security. https://doi.org/10.1145/3538969.3544426

UNE 166006:2018 Gestión de La I+D+i: Sistema de Vigilancia e inteligencia, Pub. L. No. UNE 166006:2018 (2018). https://acortar.link/Jg31Bu

CONTRIBUCIONES DE AUTORES/AS, FINANCIACIÓN Y AGRADECIMIENTOS

Contribuciones de los/as autores/as:

Conceptualización: Gordillo-Gaitán, Alexander; **Validación:** Gordillo-Gaitán, Alexander**;** Herrera-Ladino, Jose Alexander**;** Martinez-Jiménez, Geovanny; **Análisis formal:** Gordillo-Gaitán, Alexander; **Curación de datos:** Herrera-Ladino, Jose Alexander**;** Martinez-Jiménez, Geovanny; **Redacción-Preparación del borrador original:** Gordillo-Gaitán, Alexander **Redacción-Re- visión y Edición:** Gordillo-Gaitán, Alexander **Visualización:** Gordillo-Gaitán, Alexander **Supervisión:** Gordillo-Gaitán, Alexander **Administración de proyectos:** Gordillo-Gaitán, Alexander **Todos los/as autores/as han leído y aceptado la versión publicada del manuscrito:** Gordillo-Gaitán, Alexander.

Financiación: Esta investigación recibió financiamiento de la Corporación Universitaria Minuto de Dios - UNIMINUTO.

AUTOR/ES:

Alexander Gordillo-Gaitán:
Corporación Universitaria Minuto de Dios – UNIMINUTO.
Ingeniero electrónico, Magister en Ingeniería Electrónica con énfasis en Telecomunicaciones, con experiencia de 6 años como docente e investigador líder en proyectos de educación, ciberseguridad y seguridad informática en la Corporación Universitaria Minuto de Dios – UNIMINUTO y la Universidad de Cundinamarca, certificado como implementador y auditor de ISO/IEC 27001, Ethical Hacking Certified Associate (EHCA).
alexander.gordillo.g@uniminuto.edu