

UNIVERSIDAD CATÓLICA DE CUENCA



Universidad
Católica
de Cuenca

Maestría en Ciberseguridad

**Informe de Investigación previo a la obtención del título de Magíster en
Ciberseguridad**

Tema: Desigualdad digital y ciberresiliencia: Un análisis de la vulnerabilidad de las PYMES desde la perspectiva de la ciberseguridad.

Autor: Ing. Danilo Gerardo Berrones Sares

Asesores: Ing. Miguel Andrade López. Mg

Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2024

Agradecimiento

Quiero expresar mi gratitud a mi madre y a mi esposa por su paciencia, amor y apoyo incondicional, han sido cruciales durante este camino. A mis amigos, cuya motivación y cercanía han sido vitales para mantener mi espíritu fuerte y enfrentar los desafíos con confianza y determinación. A mis compañeros y colegas que contribuyeron en este recorrido, este logro es un reflejo del esfuerzo y trabajo en equipo que hemos compartido.

Dedicatoria

Mi trabajo de investigación rinde honor a las figuras esenciales de mi vida, cuya presencia ha sido decisiva en mi periplo académico. A mi familia, cuyo respaldo incondicional ha sido la base de mi perseverancia y éxito. A mis amigos, verdaderas luces en los momentos más desafiantes, testimonio de la solidaridad y apoyo. A mis docentes cuyas enseñanzas han sido fundamentales en mi formación. A la institución educativa que me ha acogido, en especial a mis tutores, mi aprecio por su dedicación y apoyo. Esta investigación refleja la fortaleza de espíritu y ánimo que he recibido de todos Ustedes. Con un profundo sentido de gratitud y estima, les dedico este trabajo.

Resumen

Este informe de investigación analiza un problema crítico y progresivo de alcance global: la creciente desigualdad en ciberseguridad entre las grandes organizaciones y las PYMES que impacta profundamente en su capacidad de ciberresiliencia. Es oportuno examinar con ojo crítico los retos que enfrentan las PYMES para progresar en un mundo globalizado y cada vez más digitalizado. La metodología empleada incluye una minuciosa selección de estudios recientes y datos relevantes. Los resultados nos revelan el impacto desproporcionado que sufren las PYMES en ciberseguridad debido a sus recursos limitados, acceso restringido a tecnologías avanzadas y una creciente escasez de talento en ciberseguridad. Las consecuencias incluyen una mayor exposición a ciberataques con graves e incluso nefastas repercusiones económicas, sociales y reputacionales. Como conclusión se resalta la importancia de adoptar estrategias inclusivas y sostenibles para mejorar la ciberresiliencia de las PYMES, apelando a incrementar la inversión en ciberseguridad de los ecosistemas organizacionales, democratizar la formación en habilidades cibernéticas, facilitar el acceso a las tecnologías y colaborar activamente entre las diferentes organizaciones para reducir la brecha de ciberseguridad.

Palabras clave: ciberseguridad, ciberresiliencia, ciberataques, brecha, desigualdad, pymes, estrategias, talento

Abstract

This research report examines a critical and progressive issue of global scope: the growing cybersecurity inequality between large organizations and SMEs, which significantly impacts their cyber resilience capabilities. It is timely to critically examine the challenges SMEs face in progressing in a globalized and increasingly digitalized world. The methodology employed includes a careful selection of recent studies and relevant data. The results reveal the disproportionate impact suffered by SMEs in cybersecurity due to their limited resources, restricted access to advanced technologies, and a growing shortage of cybersecurity talent. The consequences include increased exposure to cyberattacks, with severe and even disastrous economic, social, and reputational repercussions. In conclusion, the importance of adopting inclusive and sustainable strategies to improve SMEs' cyber resilience is highlighted, appealing to increase investment in cybersecurity within organizational ecosystems, democratize training in cyber skills, facilitate access to technologies, and actively collaborate among different organizations to reduce the cybersecurity gap.

Keywords: cybersecurity, cyber resilience, cyberattacks, gap, inequity, SMEs, strategies, talent

Índice

Capítulo I. Introducción	1
1.1. Situación problemática	1
1.2. Problema científico	2
1.3. Línea de investigación	2
1.4. Objeto de estudio	3
1.5. Campo de acción	4
1.6. Objetivos	5
1.7. Problema científico – preguntas de investigación	6
1.8. Variables	6
1.9. Justificación – contribuciones de la investigación	7
1.10. Estado del arte o antecedentes	8
1.11. Marco teórico referencial	13
1.12. Diseño marco metodológico	19
1.13. Procedimientos éticos	22

Capítulo I. Introducción

1.1. Situación problemática

La ciberseguridad es un eje trascendental para las organizaciones de todo el planeta. Existe una creciente brecha en las capacidades cibernéticas de las organizaciones que afecta de forma desmedida a las PYMES, especialmente a las asentadas en los países en vías de desarrollo.

Entre los factores que originan esta brecha podemos destacar:

- Constante evolución de las amenazas cibernéticas, que implica una inversión constante de tiempo y recursos.
- Rápido avance de las tecnologías, que genera nuevos espacios de riesgo y oportunidades para los ciberatacantes, soluciones cada vez más complejas que dificultan la adquisición y operación especialmente para las PYMES.
- Creciente escasez de talento y habilidades cibernéticas, que dificulta a las organizaciones disponer del personal suficiente y adecuado.
- Inestabilidad geopolítica, económica y social, que crea un entorno propicio para ciberataques.

Los efectos de esta brecha de ciberseguridad son significativos. Las organizaciones que carecen de las capacidades cibernéticas adecuadas son más vulnerables a los ciberataques, pudiendo causar pérdidas financieras, daños a la reputación y graves problemas operativos. En el caso de las PYMES, que suelen tener menos recursos para invertir en ciberseguridad, y por lo general no cuentan con empleados debidamente capacitados, son más vulnerables a ciberataques cuyo impacto puede ser devastador.

1.2. Problema científico

La desigualdad en ciberseguridad entre las grandes organizaciones y las PYMES es un problema creciente que afecta a la capacidad de ciberresiliencia de las PYMES; es importante tomar en cuenta que sus consecuencias afectan a todo el ecosistema organizacional ya que las grandes organizaciones interactúan constantemente con las PYMES. Las PYMES que son víctimas de ciberataques pueden sufrir pérdidas económicas importantes, problemas de continuidad del negocio y daños a su reputación.

La pérdida de datos es una de las principales consecuencias de los ciberataques que pueden acarrear el pago de multas o indemnizaciones. Además, la pérdida de datos puede dañar la reputación de las PYMES, ya que los clientes o proveedores pueden perder la confianza en ellas.

La interrupción del negocio es para las PYMES otra consecuencia importante de los ciberataques. Un ciberataque que provoque la interrupción de los sistemas informáticos puede afectar su capacidad para operar, y dicha interrupción puede ocasionar pérdidas económicas al detener el flujo de ingresos o perder clientes.

1.3. Línea de investigación

Siendo la línea de investigación ciencia de los ordenadores, analítica de datos y algoritmos computacionales los estudios de informática, técnicas y herramientas para el análisis de datos y la resolución de problemas computacionales, este proyecto se relaciona estrechamente al analizar los datos sobre el acceso e inversión en ciberseguridad de las organizaciones, desagregando a las PYMES para comprender mejor las tendencias por sector,

los factores que contribuyen a la desigualdad en ciberseguridad y las consecuencias para todo el ecosistema global.

Líneas de investigación institucionales		Sub Línea
En desarrollo	Energía eléctrica y Tecnologías de la Información para la innovación y el desarrollo sostenible	Ciencia de los ordenadores, analítica de datos y algoritmos computacionales ☒
		Sistemas eléctricos de potencia, energía e iluminación ☐
		Modelado, automatización y control ☐

Fuente: Universidad Católica de Cuenca

El proyecto procura ayudar a comprender mejor un problema importante que afecta a las organizaciones en general y en especial a las PYMES, y precisar métodos y herramientas que permitan mejorar la ciberseguridad de estas organizaciones.

1.4. Objeto de estudio

La investigación se centra en un análisis de los siguientes elementos:

- Grandes organizaciones, son las que cuentan con al menos 200 empleados y un valor de activos y operaciones de cierto nivel, poseen una capacidad financiera robusta que les permite realizar inversiones significativas en ciberseguridad. Este músculo financiero facilita la implementación de medidas de seguridad de vanguardia, el uso de tecnologías actualizadas y la contratación de personal altamente calificado y experimentado en el campo de la ciberseguridad.

- Las PYMES, definidas como empresas con menos de 200 empleados y un nivel de ventas y operaciones más discreto, son organizaciones con limitaciones financieras que restringen su capacidad para invertir en ciberseguridad. Esta falta de recursos dificulta la implementación de medidas de seguridad al mismo nivel que las grandes organizaciones, generando una brecha en ciberseguridad que es nuestro principal objeto de análisis.
- La ciberseguridad, la definimos como el conjunto de estrategias y procedimientos destinados a salvaguardar los activos digitales de las organizaciones contra amenazas cibernéticas. La brecha entre las grandes organizaciones y PYMES en términos de ciberseguridad plantea desafíos significativos que afectan directamente la ciberresiliencia de las organizaciones.

1.5. Campo de acción

Esta investigación se centra en el análisis de la creciente inequidad en ciberseguridad y su injerencia directa en la capacidad de ciberresiliencia de las PYMES en particular, y del ecosistema organizacional en general, dentro de un contexto de las organizaciones de diferentes tamaños, sectores y países. Este campo no posee una única dimensión, abarca un espectro que comprende aspectos económicos, tecnológicos y sociales relacionados con la ciberseguridad y sus efectos.

En términos económicos, analizamos cómo la disponibilidad de recursos financieros y la inversión en ciberseguridad varían entre las grandes organizaciones y las PYMES, y cómo esta inequidad afecta sus capacidades de enfrentar y recuperarse de los ciberataques. Desde una mirada tecnológica, estudiamos cómo el acceso y la implementación de tecnologías de seguridad cibernética difieren entre las organizaciones; al igual que la adopción de

herramientas avanzadas para detección y prevención, así como el personal altamente calificado en materia de ciberseguridad.

Finalmente, en el ámbito social y reputacional, examinamos cómo la desigualdad en ciberseguridad puede afectar la percepción pública de las organizaciones, su confiabilidad y la confianza de los clientes y socios comerciales, y cómo los incidentes cibernéticos pueden afectar las relaciones en el ecosistema empresarial, especialmente entre grandes organizaciones y PYMES.

1.6. Objetivos

General

Identificar las causas y consecuencias de la desigualdad en ciberseguridad en la capacidad de ciberresiliencia de las PYMES.

Específicos

- Definir los factores que contribuyen al crecimiento constante de la brecha en ciberseguridad entre las grandes organizaciones y las PYMES.
- Determinar el impacto de la desigualdad en ciberseguridad en los ecosistemas de las organizaciones, en particular en las PYMES.
- Subrayar los resultados económicos, sociales y reputacionales adversos impulsados por la inequidad en ciberseguridad para las PYMES.

1.7. Problema científico – preguntas de investigación

Preguntas científicas

- ¿Cómo la desigualdad en ciberseguridad incide drásticamente en la capacidad de ciberresiliencia de las PYMES?
- ¿Qué factores fomentan la brecha en ciberseguridad entre las grandes organizaciones y las PYMES?
- ¿Cómo afecta esta inequidad a los ecosistemas de las organizaciones en general y en especial a las PYMES?
- ¿Cuáles son las consecuencias económicas, sociales y reputacionales de la desigualdad en ciberseguridad para las PYMES?

Hipótesis

La desigualdad en ciberseguridad incide drásticamente en la capacidad de ciberresiliencia de las PYMES, aumentando su exposición y vulnerabilidad a los ciberataques y sus repercusiones.

1.8. Variables

Variable independiente:

- Inversión en ciberseguridad

Variables dependientes:

- Número de incidencias reportadas
- Tiempo de recuperación luego de una incidencia
- Impacto económico de la incidencia

- Tiempo de duración de la interrupción de operaciones tras una incidencia

1.9. Justificación – contribuciones de la investigación

Esta investigación tiene relevancia en el campo de la ciberseguridad y la resiliencia empresarial, ya que aborda un problema crítico que afecta a las PYMES y al ecosistema organizacional en su conjunto. La creciente desigualdad en ciberseguridad entre las grandes organizaciones y las PYMES plantea desafíos sustanciales que deben ser analizados, entendidos y mitigados de manera efectiva.

La justificación de esta investigación radica en su capacidad para proporcionar una mirada clara y específica sobre los factores que fomentan la creciente brecha en ciberseguridad y cómo esta inequidad incide directamente en la capacidad de las PYMES para enfrentar las amenazas cibernéticas. Al analizar aspectos económicos, tecnológicos y sociales, esta investigación nos mostrará las áreas críticas que requieren atención.

Las contribuciones de esta investigación son múltiples:

- Ayudar a comprender mejor las dimensiones de la desigualdad en ciberseguridad y a tomar medidas para fortalecer sus capacidades de resiliencia cibernética.
- Proporcionar información valiosa para la adopción de medidas más efectivas para abordar este problema de alcance global.
- Aportar a la protección de la infraestructura organizacional y la mitigación de riesgos cibernéticos, promoviendo así el desarrollo y la innovación en un entorno digital cada vez más complejo.

1.10. Estado del arte o antecedentes

A lo largo de los años, el concepto de seguridad de la información ha evolucionado, en 1990, la Organización del Tratado del Atlántico Norte (OTAN) unificó las definiciones de seguridad de transmisión, seguridad de redes y seguridad de ordenadores en un único concepto denominado "seguridad de la información". Esta nueva concepción tenía como objetivo esencial proteger la información en sus tres dimensiones fundamentales: confidencialidad, integridad y disponibilidad (Candau, 2021).

Complementa Candau (2021) su explicación indicando que Estados Unidos en el año 2002 propuso una ampliación de este concepto al incorporar el término "aseguramiento de la información" (information assurance), se introdujeron dos nociones: autenticidad y no repudio, que se integraron en el ámbito de la "Seguridad de las Tecnologías de Información y Comunicaciones". Este enfoque ampliado tenía como propósito salvaguardar tanto la información como los sistemas encargados de su gestión en cinco dimensiones clave: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La Unión Europea (UE) manifestó su interés en la seguridad de los sistemas y la información, lo que innovó la terminología, pasando de "information assurance" a "ciberseguridad". En esta nueva concepción, la ciberseguridad se definió como la aplicación práctica del "information assurance", fundamentada en la responsabilidad compartida entre la autoridad encargada de autorizar el sistema para manejar información clasificada y la entidad responsable de su gestión.

La ciberseguridad incorporó conceptos adicionales, como la vigilancia y las respuestas a incidentes, la auditoría continua y la notificación de incidentes, todos ellos elementos cruciales para garantizar la integridad y seguridad de la información y los sistemas. En la actualidad, los sistemas de información basados en tecnología están presentes en todos los procesos de cualquier organización: desde la comunicación interna, la atención al cliente, producción, marketing, logística, selección y formación de personal, hasta la internacionalización y sobre todo innovación (Instituto Nacional de Ciberseguridad, 2017).

Las PYMES no están excluidas del ecosistema tecnológico, y aquellas que no son nativas digitales deben evolucionar para mantenerse competitivas y sobrevivir. La implementación de tecnologías en las PYMES puede aumentar la productividad, mejorar la capacitación de los empleados, conectar los equipos y mejorar la experiencia del cliente y usuario, entre otros beneficios.

1.10.1. Impacto de las nuevas tecnologías y la evolución de las amenazas

Con la transformación digital en pleno apogeo, impulsada forzosamente por la presencia del COVID-19, el avance de tecnologías como la inteligencia artificial, el internet de las cosas, la computación en la nube, han creado nuevas oportunidades para potenciar la eficiencia y la productividad, el trabajo remoto se ha establecido como una modalidad permanente pero también han dado origen a un prolífico campo de acción para nuevas vulnerabilidades y vectores de ataque. Los atacantes están desarrollando y perfeccionando sus tácticas, técnicas y procedimientos (TTP) para explotar estas vulnerabilidades, incorporando métodos más sofisticados y sigilosos para comprometer sistemas, robar datos e interrumpir operaciones.

La persistente transformación de las amenazas y defensas cibernéticas establecen una carrera tecnológica donde atacantes y defensores están en constante innovación y adaptación. La tecnología avanza a un ritmo sumamente acelerado, y con ella, las amenazas cibernéticas despliegan nuevos desafíos para que las organizaciones protejan sus activos digitales críticos, sobre todo las PYMES.

Computing Technology Industry Association (2023) señala en su reporte State of Cybersecurity 2024 que actualmente la ciberseguridad es una necesidad crítica en las organizaciones, es crucial examinar cada proceso para identificar posibles vulnerabilidades. Esta evaluación de riesgos orienta decisiones sobre flujos de trabajo, desarrollo de habilidades y uso de tecnología.

Debido a la constante evolución de las tendencias tecnológicas y los patrones de ataque, alcanzar el equilibrio es un gran desafío para una organización moderna. A medida que las empresas se digitalizan y vinculan la tecnología con su crecimiento y éxito, una ciberseguridad demasiado restrictiva puede frenar el avance; sin embargo, una ciberseguridad insuficiente puede causar incidentes serios, afectando negativamente el progreso (Computing Technology Industry Association, 2023).

Bueermann & Rohrs (2024) en su informe Global Security Outlook 2024 señala que las organizaciones, particularmente las PYMES, a menudo operan con recursos limitados, lo que puede restringir su capacidad para invertir en herramientas de ciberseguridad avanzadas y personal especializado. Estas limitaciones plantean desafíos significativos en la gestión de riesgos cibernéticos. Los defensores deben hacer más con menos, optimizando sus recursos y empleando estrategias creativas y efectivas para detectar, prevenir y responder a las

amenazas. La necesidad de formación continua, el desarrollo de habilidades y la implementación de soluciones de seguridad son obligatorias.

1.10.2. Escasez de talento en ciberseguridad

La brecha de habilidades en ciberseguridad es un problema global que afecta a todas las organizaciones pero tiene un impacto desproporcionado en las PYMES. La competencia por profesionales calificados en ciberseguridad es implacable, y las grandes organizaciones por lo general tienen la capacidad de ofrecer mejores condiciones laborales dejando a las PYMES en desventaja para atraer y retener talento. Sin embargo, redoblar esfuerzos en la educación de los colaboradores, la respuesta a incidentes y la mejora de procesos deberían ser objetivos prioritarios para avanzar en la ciberseguridad (Computing Technology Industry Association, 2023).

1.10.3. Influencia de la inestabilidad geopolítica, económica y social

La inestabilidad geopolítica, económica y social crea un entorno propicio para los ciberataques aumentando la incertidumbre y el riesgo en el ciberespacio. Las organizaciones deben estar preparadas para adaptarse a estas condiciones cambiantes, pero las PYMES a menudo carecen de la flexibilidad financiera para hacerlo de manera efectiva (Bueermann & Rohrs, 2024).

1.10.4. Ciberseguridad y responsabilidad corporativa

Actualmente se reconoce que la ciberseguridad no solo es un asunto tecnológico sino un aspecto integral de la responsabilidad corporativa. Las organizaciones están siendo

evaluadas cada vez de forma más minuciosa en su capacidad para proteger la información y los activos digitales, lo que afecta su reputación y su relación con clientes, socios y entes reguladores. Las PYMES enfrentan desafíos únicos en este ámbito, ya que la dificultad para acceder a los recursos necesarios puede limitar su capacidad para cumplir con estas expectativas y regulaciones de forma eficiente.

1.10.5. Resiliencia

Las organizaciones deben adoptar un enfoque proactivo para mantenerse protegidas y actualizadas con el actual panorama de amenazas en rápida evolución. Esto implica no solo la implementación de tecnologías de seguridad avanzadas sino también la promoción de una cultura de concienciación en ciberseguridad entre los empleados. Además, es crucial fomentar la resiliencia organizativa, preparando a las empresas para responder y recuperarse eficazmente de los incidentes cibernéticos. La adaptabilidad y la resiliencia se convierten en cualidades esenciales para sobrevivir y prosperar en el hostil y siempre cambiante mundo de la ciberseguridad.

En nuestro país, la percepción de la ciberseguridad como un gasto sin retorno económico (Return On Investment ROI) evidente ha sido un factor limitante en la cultura organizacional, particularmente en nuestro medio donde el soporte especializado en ciberseguridad es costoso y escaso. Sin embargo, es imperativo realinear este enfoque, considerando la ciberseguridad no solo como una inversión esencial, sino también en términos de su relación beneficio/costo.

Al invertir en ciberseguridad, las organizaciones no solo evitan ataques que pueden impactar severamente sus finanzas y reputación, sino que también fortalecen su posición

competitiva en el mercado. Aunque el costo inicial del soporte especializado en ciberseguridad puede ser elevado, los beneficios a mediano y largo plazo, como la protección contra interrupciones operativas y pérdidas de datos justifican claramente esta inversión.

Es crucial que las empresas ecuatorianas adopten un enfoque más estratégico hacia la ciberseguridad, considerándola como un elemento fundamental en la gestión de riesgos y la continuidad del negocio. Esta nueva perspectiva implica entender que una inversión adecuada en ciberseguridad no solo protege contra pérdidas potenciales, sino que también fortalece la confianza de clientes y socios, asegurando así una ventaja competitiva y sostenible en el mercado. Adoptar esta visión más integrada y proactiva es un paso fundamental hacia la mejora de la cultura organizacional en Ecuador en relación con la ciberseguridad.

1.11. Marco teórico referencial

1.11.1. Definiciones

Organización: “Asociación de personas reguladas por un conjunto de normas en función de determinados fines” (Real Academia Española, 2024).

Empresa: “Unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos” (Real Academia Española, 2024).

Grandes empresas.- En Ecuador se consideran grandes empresas a las que tienen al menos 200 trabajadores y un valor de ingresos brutos superior a 5 millones de dólares (Servicio Ecuatoriano de Normalización, 2024). Sin embargo estos umbrales varían según el país o región, la Comisión Europea considera dentro de las grandes empresas las que poseen al

menos 250 empleados, volumen de negocios de 50 millones de euros, y un balance general superior a 43 millones de euros (Comisión Europea, 2016).

PYMES/MIPYMES: Conocemos como PYME a la empresa que no supera cierto número de trabajadores y cierto volumen de facturación (Real Academia Española, 2024). En Ecuador, el concepto está ligado a MIPYMES (Micro, Pequeñas y medianas empresas) que son unidades productivas que pueden ser personas naturales o sociedades que están compuestas por entre 1 y 199 trabajadores, y sus ingresos brutos anuales no superan los 5 millones de dólares (Servicio Ecuatoriano de Normalización, 2024).

Filtración de información: también conocida comúnmente como fuga de datos, sucede cuando la confidencialidad de la información empresarial se ve comprometida. Esta información debería estar restringida a los usuarios autorizados dentro de la organización. El problema surge cuando, debido a un incidente de seguridad, dicha información se vuelve accesible para personas no autorizadas externas a la organización (Instituto Nacional de Ciberseguridad, 2020).

1.11.2. Relevancia de las PYMES a nivel nacional, regional y global

El Instituto Nacional de Estadísticas y Censos (2016) determinó que en Ecuador las PYMES representan el 99.5% de las empresas registradas. Según datos del Ministerio de Producción, Comercio Exterior, Inversiones y Pesca del Ecuador, las PYMES han experimentado un crecimiento promedio del 10% anual en los últimos cinco años y generan el 32.38% del empleo. Un estudio reciente realizado por la Cámara de Comercio de Quito revela que el 75% de las PYMES ecuatorianas han implementado nuevas tecnologías en sus operaciones, lo que les ha permitido mejorar su eficiencia y competitividad en el mercado.

En América Latina y el Caribe, las pymes constituyen un pilar fundamental del tejido socioeconómico. Ellas no solo representan aproximadamente el 90% del total de empresas en la región, sino que también emplean a más de la mitad de la fuerza laboral. A pesar de su relevancia numérica, estas empresas enfrentan desafíos significativos que limitan su capacidad de crecimiento, generación de empleo de calidad y aporte al Producto Interno Bruto (PIB) regional, donde su contribución actual se sitúa en torno al 25% (Díaz-Granados, 2023).

A nivel mundial, las PYMES constituyen el motor trascendental de crecimiento económico, innovación y empleo. Según datos de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), las PYMES constituyen alrededor del 99% de todas las empresas en sus países miembros y generan entre el 50% y el 60% del valor agregado total. Además, son responsables de una significativa proporción del empleo, proporcionando entre el 60% y el 70% de los empleos en el sector privado en los países de la OCDE.

A pesar de su importancia, las PYMES enfrentan desafíos en términos de acceso a financiamiento, tecnología y mercados. Estas limitaciones pueden afectar su capacidad para crecer y competir a nivel global. Las PYMES son fundamentales para la innovación, sin embargo, su capacidad para innovar puede verse limitada por recursos financieros escasos y/o restringidos, acceso limitado a nuevas tecnologías y conocimientos especializados. A pesar de esto, las PYMES a menudo son más ágiles y adaptativas, lo que les permite responder rápidamente a los cambios del mercado y las nuevas oportunidades.

1.11.3. Ciberresiliencia

Definición: Ciberresiliencia es la habilidad de una organización para prever, resistir, recuperarse y adaptarse con el propósito de fortalecer sus capacidades para proteger su información frente a amenazas cibernéticas (Instituto Nacional de Ciberseguridad, 2023).

Estado actual: Hoy tenemos una creciente brecha en ciberseguridad entre las organizaciones ciberresilientes y las que enfrentan grandes retos por serlo. Existe un desequilibrio marcado por la disparidad en la adopción de tecnologías, facilidad de acceso a bienes, servicios, herramientas, habilidades, experiencias y hasta regulaciones que influyen en la construcción de un ciberespacio más seguro (Bueermann & Rohrs, 2024).

El último informe del Foro Económico Mundial sobre Ciberseguridad Global destaca varios hitos y recalco uno clave: en 2022 la economía de ciberseguridad creció dos veces más rápido que la economía mundial, y en 2023, cuatro veces. La celeridad del sector de la ciberseguridad hace que las PYMES con tasas discretas de crecimiento queden cada vez más rezagadas dando origen al fenómeno “línea de pobreza de ciberseguridad”.

1.11.4. Ecosistema global

La desigualdad en ciberseguridad afecta directamente a la capacidad de ciberresiliencia de las PYMES; es importante tomar en cuenta que sus consecuencias afectan a todo el ecosistema ya que las grandes organizaciones interactúan constantemente con las PYMES. Para las organizaciones ciberresilientes el hecho que otras no lo sean debería ser alarmante pues también forman parte del ecosistema: el 98% de las organizaciones tiene relación con al menos un tercero que ha experimentado una vulneración de datos en los últimos dos años (Bueermann & Rohrs, 2024).

El número más bajo de organizaciones ciberresilientes se encuentra en América Latina y África, y al mismo tiempo el índice más alto de organizaciones insuficientemente ciberresilientes; paralelamente las soluciones de seguridad se están volviendo demasiado sofisticadas, hasta el punto de que muchas PYMES tienen serias dificultades tanto para costearlas como para operarlas (Bueermann & Rohrs, 2024).

1.11.5. Inteligencia Artificial (IA)

El Foro Económico Mundial señala que la IA generativa aumentará el PIB global en 7% en los próximos 10 años. La aplicación de la IA en la ciberseguridad ha revolucionado la manera de proteger los activos digitales de las organizaciones. Una de las innovaciones más destacadas es el uso de IA para la detección y respuesta automática a amenazas, aprenden y evolucionan continuamente, permitiendo identificar patrones complejos de ataques que serían indetectables para los sistemas tradicionales. Además, la IA puede detectar y neutralizar proactivamente amenazas, mejorando la eficiencia y reduciendo la carga de trabajo de los equipos de ciberseguridad.

Sin embargo, la IA también es usada por los cibercriminales, FraudGPT o WormGPT, phishing, vishing, smishing y la desinformación (deep fakes) generada y difundida en grandes volúmenes dificulta su detección y control (Bueermann & Rohrs, 2024). El informe de Seguridad Global 2024 también advierte que en los últimos 5 años se ha duplicado el número de familias de malware y variantes que se han infiltrado en al menos 10% de las organizaciones globales. El mismo informe revela una encuesta realizada a 120 líderes de la reunión anual sobre ciberseguridad en el Foro Económico Mundial, en que el 13% afirma que los empleados fueron el motivo de un incidente en los últimos 12 meses.

1.11.6. Impacto de las incidencias cibernéticas

Los impactos económicos de las incidencias cibernéticas pueden ser devastadores, especialmente para las PYMES. Estos pueden ser pérdidas directas por interrupciones del negocio, servicios, o la cadena de suministros, pérdida de productividad, potencial pérdida de datos críticos o de propiedad intelectual, costos de recuperación, sanciones legales y daños a la reputación.

En Ecuador el 26 de Mayo de 2021 se publicó en el Registro Oficial Quinto Suplemento N° 459 la Ley Orgánica de Protección de Datos Personales, y sus medidas correctivas y sancionatorias entraron en vigencia el pasado 26 de Mayo de 2023. Complementariamente el 13 de Noviembre de 2023 se publicó en el Registro Oficial el Reglamento de la Ley Orgánica de Protección de Datos Personales, por lo que es importante para las organizaciones cumplir con las obligaciones de dicha Ley para evitar incurrir en alguna de las sanciones legales previstas.

1.11.7. Retos para las PYMES

Las PYMES enfrentan grandes retos para alcanzar la ciberresiliencia mínima viable (operación crítica), las que están en este grupo se han reducido en un 30%; deben lidiar con los recursos limitados para la seguridad cibernética, falta de personal especializado y vulnerabilidades propias por su tamaño y nivel de operaciones. El 31% de los líderes de PYMES indican que les faltan personas y habilidades críticas, comparado con el 11% de los líderes de organizaciones grandes (Bueermann & Rohrs, 2024).

La oferta tecnológica que continuamente se une a los ecosistemas digitales aumenta la demanda de personal calificado, cada año aumentan las organizaciones que carecen del número idóneo de personas con habilidades requeridas para cumplir con la ciberresiliencia. En la reunión de 2022 el 6% de los líderes manifestaron que les faltaban personas para responder a un ataque cibernético, en 2023 la cifra se duplicó, 12%. Este año, es el 20% (Bueermann & Rohrs, 2024).

El informe también indica que el 91% de las organizaciones están dispuestas a pagar por capacitación y certificación en ciberseguridad para sus empleados, y el 29% de los líderes afirmaron que su organización sufrió un impacto material en los últimos 12 meses. Para los líderes de la región de Norteamérica y Europa, la principal preocupación es la interrupción operativa, para los de América Latina, África y Asia, lo son las pérdidas financieras directas por un ataque de ransomware y para los del Medio Oriente, el daño a la marca y la reputación.

1.12 Diseño marco metodológico

Esta investigación analizará la desigualdad en ciberseguridad entre grandes organizaciones y PYMES, y su impacto en la ciberresiliencia de estas últimas. La revisión de literatura se presenta como una herramienta oportuna e importante para comprender la magnitud y evolución de dicha brecha.

Metodología:

1. Definición del Alcance y Objetivos:

El estudio busca identificar, analizar y sintetizar datos relevantes sobre la desigualdad en ciberseguridad en las organizaciones y su incidencia en la capacidad de ciberresiliencia de las PYMES.

2. Búsqueda y Selección de Fuentes:

Se realizará una búsqueda exhaustiva de datos secundarios en bases de datos científicas, organismos públicos y privados, y proveedores de seguridad mundialmente reconocidos. Se priorizarán publicaciones, artículos y documentos de investigación de los últimos 3 años, asegurando actualidad y relevancia.

Criterios de Inclusión:

- Relevancia para la ciberseguridad en PYMES.
- Datos empíricos sobre la brecha de ciberseguridad y su impacto.
- Palabras clave: Cybersecurity, resilience, SME.
- Publicación en los últimos 5 años.
- Análisis de tendencias, desafíos y soluciones en ciberseguridad, especialmente en PYMES.

Criterios de Exclusión:

- Temas no relacionados con la desigualdad en ciberseguridad en las organizaciones.
- Enfoque meramente teórico sin base empírica.
- Ausencia de análisis sobre la ciberresiliencia.
- Análisis sobre un sector muy específico.

(Ver Anexo A)

3. Extracción y Análisis de Datos:

Se aplicarán técnicas cualitativas y cuantitativas para analizar los datos.

4. Evaluación de la Calidad de los Estudios:

Se evaluará la calidad de los estudios en base a su relevancia, metodología y solidez de sus conclusiones, asegurando la validez y confiabilidad de los datos.

(Ver Anexo B)

Herramientas de Análisis:

Se utilizarán herramientas estadísticas y de análisis de datos para procesar y analizar los datos. Se aplicarán técnicas de análisis cuantitativo y cualitativo para las respuestas de la encuesta.

Validación de Datos:

Se buscará corroborar la información a través de múltiples fuentes para asegurar la validez y confiabilidad de los resultados.

5. Síntesis de la Información:

Se sintetizarán los resultados para presentar una visión clara de la situación actual de la ciberseguridad en las PYMES, identificando patrones y tendencias clave. Se integrarán los hallazgos de las fuentes secundarias y del estudio empírico para ofrecer una visión holística. Se analizarán los resultados en el contexto de las tendencias globales y locales, destacando las particularidades del contexto ecuatoriano.

Se presentarán los hallazgos de manera clara y concisa, examinando su relación con los objetivos de la investigación. Se valorarán las implicaciones prácticas de los resultados tanto a nivel global como local, relacionando las particularidades del contexto global con el local, y se formularán recomendaciones para políticas, estrategias y prácticas que puedan ayudar a reducir la brecha y mejorar la ciberresiliencia de las PYMES.

1.13 Procedimientos éticos

No aplica.

Capítulo II. Diagnóstico Situacional

2.1. Introducción

Este diagnóstico situacional examina el contexto actual de la ciberseguridad en las PYMES, identifica amenazas y vulnerabilidades, el impacto de la desigualdad digital en la ciberresiliencia; es crucial comprender cómo la desigualdad digital afecta la capacidad de las PYMES para resistir y recuperarse de los ciberataques que pueden tener consecuencias devastadoras que ponen en riesgo su operatividad y supervivencia.

2.2. Metodología del diagnóstico

Para llevar a cabo este diagnóstico, se ha empleado una metodología que incluye el análisis de documentos científicos recientes y relevantes, encuestas a organizaciones grandes y PYMES, entrevistas con expertos en ciberseguridad, tanto en países desarrollados como en vías de desarrollo. También se ha incorporado informes sobre ciberseguridad que incluyen estudios de amenazas internas, globales, tendencias en ataques y vulnerabilidades. Esta aproximación mixta permite obtener una visión comprensiva y detallada de la situación actual y de las necesidades específicas de las PYMES en términos de ciberseguridad y ciberresiliencia.

2.3. Análisis Situacional

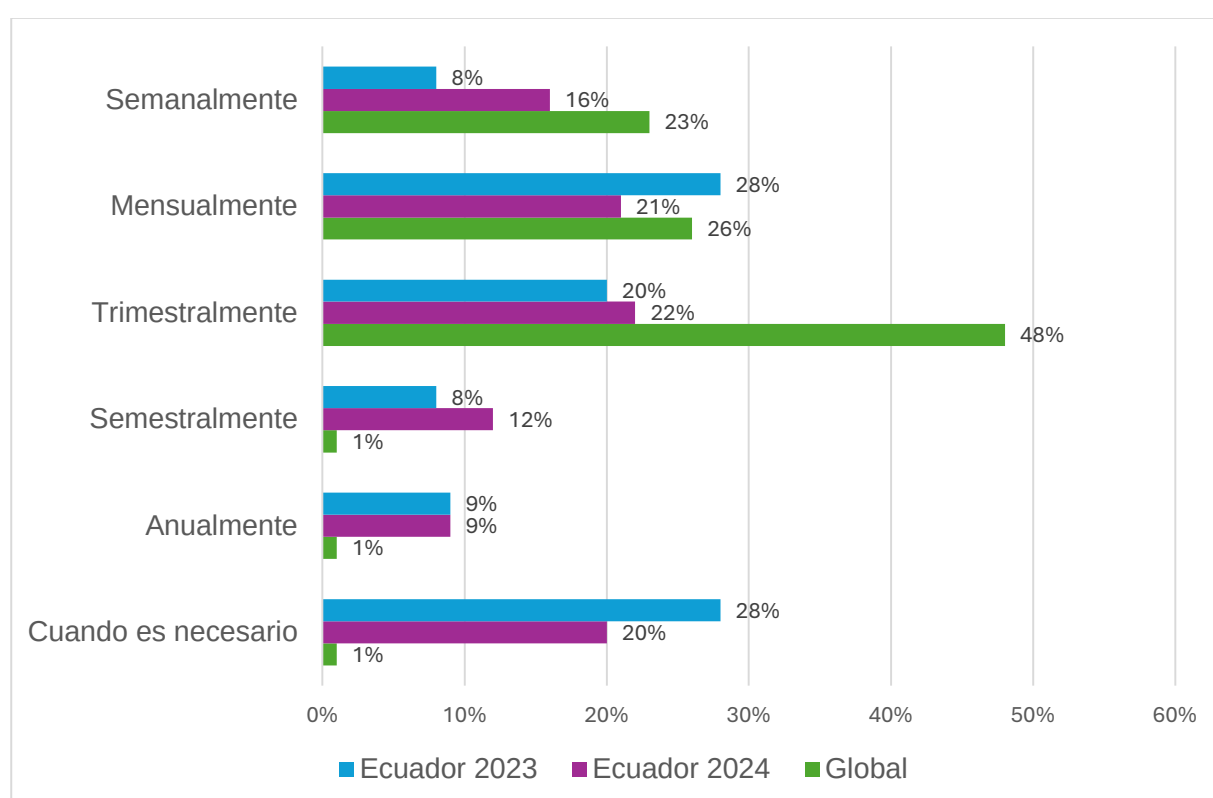
2.3.1. Contexto actual de la ciberseguridad en las PYMES

Las pequeñas y medianas empresas (PYMES) se enfrentan a un panorama de ciberamenazas en constante evolución, con un aumento en la frecuencia y sofisticación de

ataques como el ransomware y el phishing. En Ecuador, la situación no es diferente; los informes de 2023 y 2024 señalan que el ransomware y el phishing son las principales preocupaciones para las PYMES locales. Si bien la gestión de riesgos de ciberseguridad en las juntas directivas ha aumentado ligeramente para este 2024, aún queda mucho por hacer para alcanzar los niveles de empresas internacionales más maduras (IT Ahora & Deloitte, 2024).

Figura 1

Frecuencia de revisión de temas de ciberseguridad con la Junta Directiva



Nota: La figura muestra con qué frecuencia la junta directiva en su organización aborda temas relacionadas con la ciberseguridad. Fuente: IT Ahora & Deloitte (2024).

Las PYMES enfrentan un aumento en la frecuencia y sofisticación de los ciberataques. Según el reporte de Google Cloud (2024), las tácticas, técnicas y procedimientos (TTPs) de los

atacantes han evolucionado, haciendo uso de tecnologías avanzadas como la inteligencia artificial generativa para personalizar y escalar campañas de phishing. Esta situación complica la defensa, especialmente para empresas con recursos limitados. A pesar de los esfuerzos para mejorar la conciencia y las prácticas de ciberseguridad, muchas PYMES aún carecen de procesos y herramientas adecuadas para protegerse eficazmente (Erdogan et al., 2023).

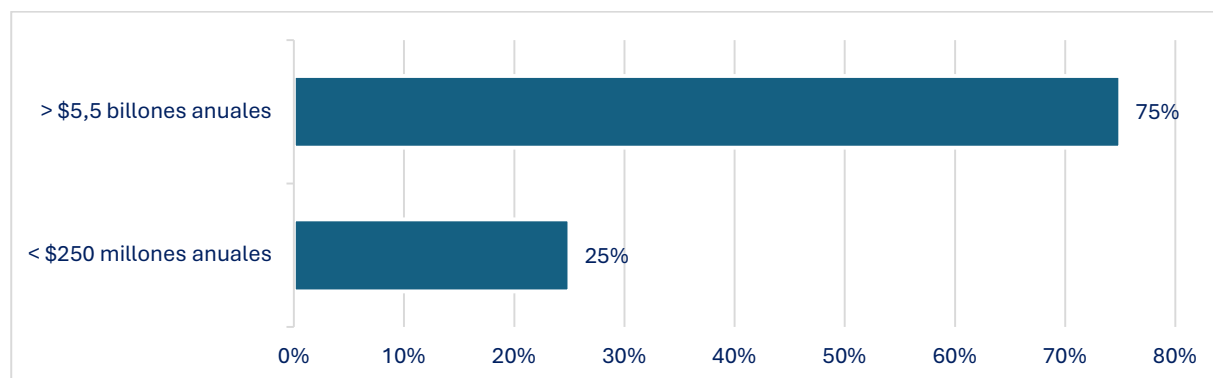
2.3.2. Brecha digital

La brecha digital en el ámbito de la ciberseguridad se ha convertido en un factor crítico para las pequeñas y medianas empresas (PYMES). Esta disparidad en el acceso y uso de tecnologías avanzadas, así como en la capacitación del personal, las expone a un mayor riesgo de ciberataques. Mientras que las grandes empresas cuentan con recursos para invertir en soluciones de seguridad robustas, muchas PYMES carecen de infraestructura adecuada y personal capacitado, lo que las convierte en objetivos vulnerables.

Esta desigualdad no solo afecta la capacidad de las PYMES para protegerse, sino también su competitividad en un entorno cada vez más digitalizado. La falta de acceso a tecnologías avanzadas y la falta de conciencia sobre los riesgos cibernéticos las dejan en desventaja frente a las grandes empresas. Esta situación es especialmente preocupante en regiones como América Latina y el Medio Oriente, donde las PYMES enfrentan desafíos adicionales debido a la falta de infraestructura tecnológica adecuada (Espinoza-Zelaya & Moon, 2023).

Figura 2

Organizaciones que tienen seguro cibernético por ingresos



Nota: La figura muestra la disparidad en la adopción de seguros cibernéticos según los ingresos de las organizaciones, destacando la brecha de ciberseguridad entre organizaciones con diferentes niveles de ingresos (Bueermann & Rohrs, 2024).

En Ecuador, esta brecha se evidencia en la falta de infraestructura adecuada y la dependencia de tecnologías obsoletas en las PYMES, la diferencia de madurez cibernética, una menor frecuencia en la actualización de sus planes de ciberseguridad y en la capacitación de su personal, lo que aumenta su vulnerabilidad frente a las amenazas cibernéticas. Esta situación se ve agravada por la falta de inversión en ciberseguridad, que se convierte en una barrera para reducir la brecha y proteger los activos de las empresas adecuada y personal capacitado, lo que las convierte en objetivos vulnerables (IT Ahora & Deloitte, 2024).

Es fundamental abordar esta brecha digital para garantizar la seguridad y la sostenibilidad de las PYMES. Se requiere un enfoque integral que incluya la inversión en infraestructura tecnológica, la capacitación del personal y la concienciación sobre los riesgos cibernéticos. Solo así las PYMES podrán proteger sus activos y competir en igualdad de condiciones en el entorno digital (European Union Agency for Cybersecurity, 2021).

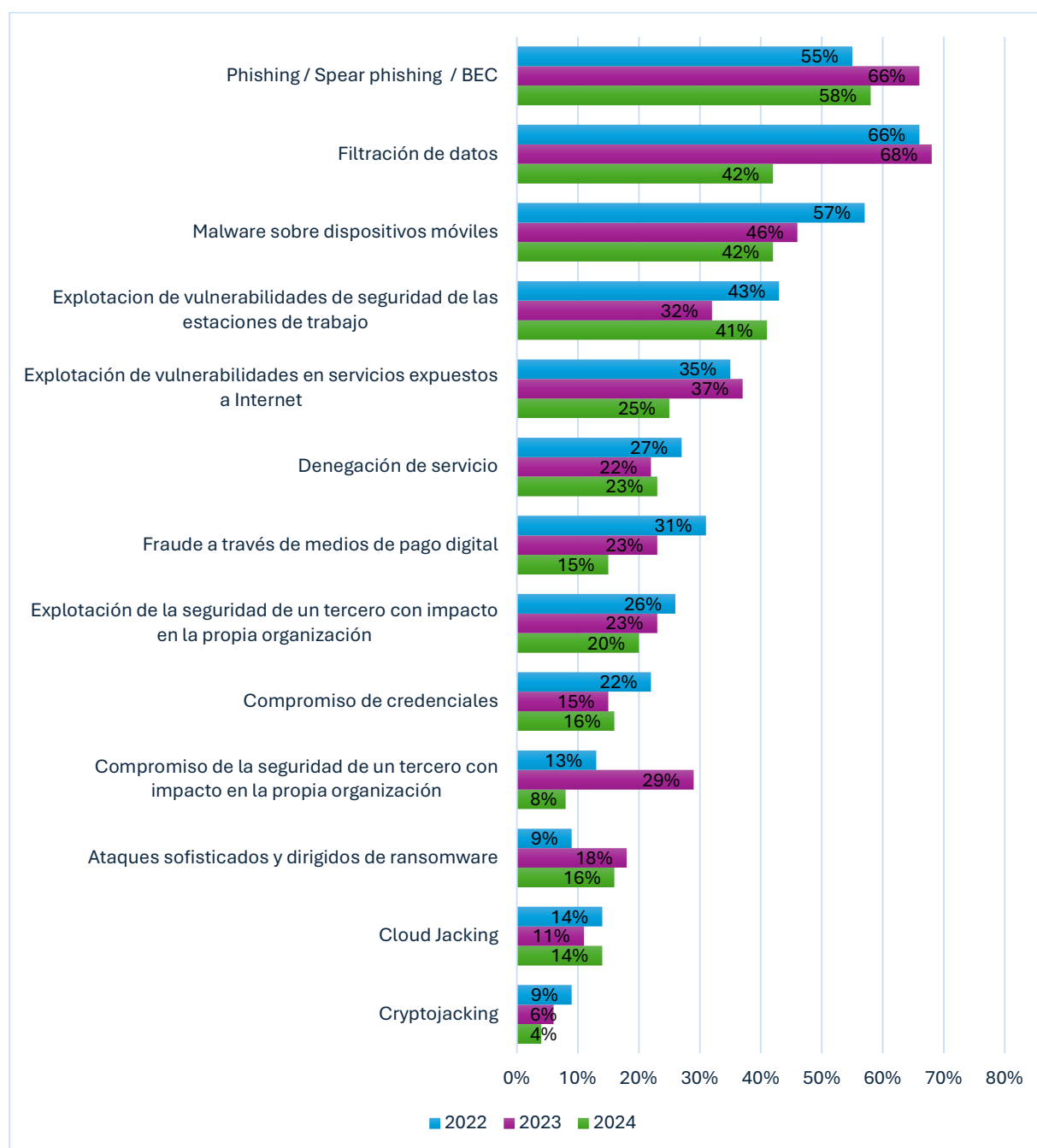
2.3.3. Identificación de amenazas y vulnerabilidades

La identificación de amenazas y vulnerabilidades es esencial para la seguridad de la información en cualquier organización. Estos dos conceptos, aunque relacionados, tienen diferencias clave: las vulnerabilidades son defectos o debilidades en un activo, mientras que las amenazas pueden explotar esas vulnerabilidades para comprometer diferentes aspectos de dicho activo.

Las pequeñas y medianas empresas (PYMES) se enfrentan a una amplia gama de amenazas cibernéticas, siendo las más comunes el phishing, el ransomware y las filtraciones de datos (IT Ahora & Deloitte, 2024). Estas amenazas afectan tanto a nivel nacional como internacional, aunque se observan prácticas más avanzadas de mitigación en los países desarrollados (Bueermann & Rohrs, 2024).

Figura 3

Amenazas que causan preocupación



Nota: La figura muestra al Phishing /Spear Phishing/BEC como la amenaza más importante para el sector privado de Ecuador. Fuente: IT Ahora & Deloitte (2024).

En Ecuador, el phishing, el spear phishing y el Business Email Compromise (BEC) son las amenazas más comunes, afectando a un 58% de las organizaciones. El phishing disminuyó

ligeramente entre 2023 y 2024, pero los ataques de ransomware y filtración de datos se mantienen persistentes. Además, la explotación de vulnerabilidades en estaciones de trabajo remotas ha aumentado considerablemente (IT Ahora y Deloitte, 2024).

Según Insider Threat Report (2023) los ataques internos también representan una amenaza significativa, con un 74% de las organizaciones sintiéndose vulnerables. Adicionalmente, las vulnerabilidades de día cero y los dispositivos de borde son objetivos atractivos para los atacantes.

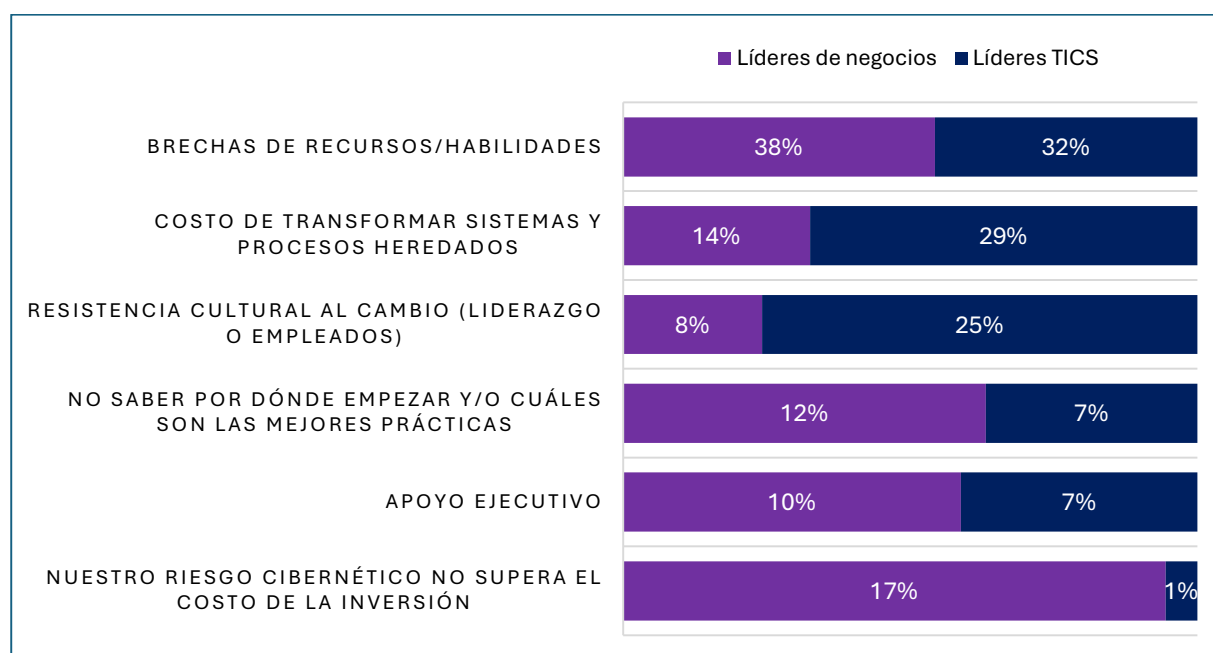
La falta de políticas de seguridad adecuadas, baja inversión en ciberseguridad y ausencia de capacitación del personal incrementan la vulnerabilidad de las PYMES. Depender de proveedores externos sin un control estricto de las vulnerabilidades agravan estos riesgos. La identificación y mitigación de amenazas suele ser reactiva y no sistemática. Es fundamental que se realicen evaluaciones periódicas de riesgos y se implementen medidas preventivas para mitigar los impactos de los ciberataques (Cisco Public, 2016).

2.3.4. Nivel de ciberresiliencia

La ciberresiliencia en las pequeñas y medianas empresas (PYMES) tanto en Ecuador como a nivel global, presenta un panorama complejo y desafiante. A pesar de los avances tecnológicos, muchas PYMES aún no han adoptado soluciones de ciberseguridad de manera efectiva debido a la falta de recursos y personal especializado, lo que limita su capacidad de respuesta y recuperación ante incidentes (Google LLC, 2023).

Figura 4

¿Cuáles son las principales barreras para la ciberresiliencia?



Nota: La figura identifica las principales barreras para la ciberresiliencia según líderes de seguridad y líderes empresariales. (Bueermann & Rohrs, 2024).

Según el Informe Estado actual de la Ciberseguridad Ecuador (2024), aunque se observa una mejora en la ciberresiliencia, persisten brechas significativas en comparación con los estándares internacionales. La falta de atención constante a la ciberseguridad reduce la capacidad de respuesta y recuperación ante incidentes. En Ecuador, solo el 47% de las PYMES realizaron capacitaciones anuales de conciencia cibernética en 2024, una disminución respecto al 66% en 2023. Además, la implementación de planes de respuesta a incidentes y ciberseguridad también ha disminuido, evidenciando la necesidad de mejorar la preparación y respuesta ante ciberamenazas.

Para las PYMES, esto implica desarrollar estrategias de gestión de riesgos, implementar medidas de protección y establecer planes de continuidad del negocio. Aunque

algunas PYMES han comenzado a implementar medidas básicas, como el uso de antivirus y copias de seguridad, estas acciones son insuficientes frente a ataques más sofisticados.

Figura 5

Capacidades de vigilancia de ciberseguridad



Nota: La figura muestra con que capacidades de vigilancia de ciberseguridad cuentan las organizaciones en Ecuador. Fuente: IT Ahora & Deloitte (2024).

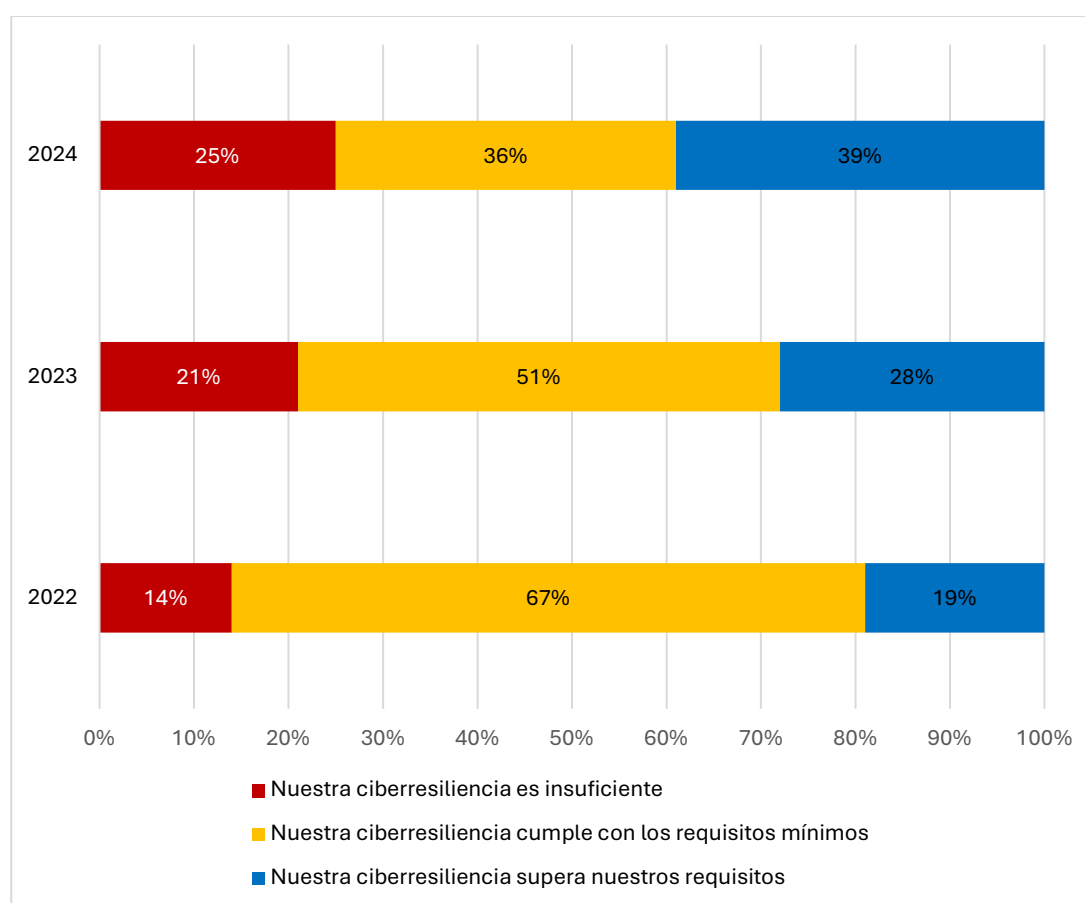
Es fundamental que las PYMES comprendan la importancia de la ciberresiliencia y desarrollen estrategias integrales que abarquen la gestión de riesgos, la implementación de medidas de protección y la planificación de la continuidad del negocio. Solo así podrán minimizar el impacto de los ciberataques y garantizar la continuidad de sus operaciones (Carias et al., 2020).

2.3.5. Impacto de la desigualdad digital en la ciberresiliencia

En Ecuador, la situación es particularmente preocupante, muchas PYMES carecen de personal especializado y presupuesto adecuado para ciberseguridad, lo que las convierte en blancos atractivos para los ciberatacantes; esta necesidad de formación y retención de personal capacitado aumenta el riesgo de ataques exitosos. Esta realidad contrasta con la mayor resiliencia exhibida por empresas grandes y tecnológicamente avanzadas, capaces de invertir en protección y adaptarse rápidamente a las amenazas.

Figura 6

¿Cuál es el estado de la ciberresiliencia de su organización este año?

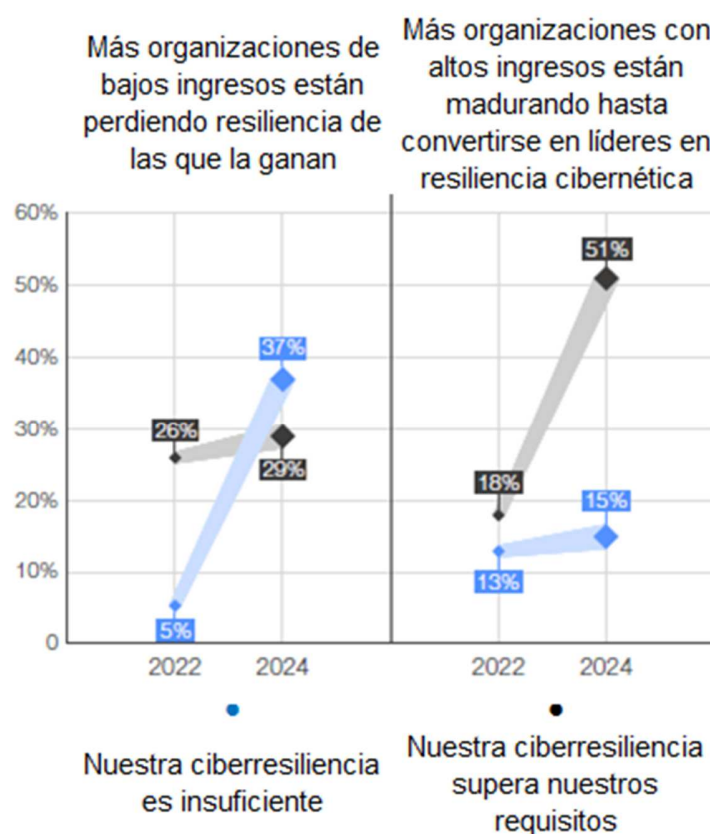


Nota: La figura muestra como crecen año a año las organizaciones con una ciberresiliencia insuficiente. (Bueermann & Rohrs, 2024).

Es esencial mejorar la ciberresiliencia de las PYMES reduciendo la brecha digital, esto implica proporcionar apoyo técnico y financiero a estas empresas para fortalecer su infraestructura de ciberseguridad, así como facilitar el acceso a recursos y programas de concienciación. Sólo a través de estas iniciativas se podrá garantizar un entorno digital más seguro y equitativo para todas las empresas, independientemente de su tamaño o recursos.

Figura 7

Evolución de la ciberresiliencia en las organizaciones según su nivel de ingresos



Nota: La figura muestra como las organizaciones de bajos ingresos crecen a grandes pasos hacia una ciberresiliencia insuficiente, mientras las de altos ingresos cada vez son mas resilientes. (Bueermann & Rohrs, 2024).

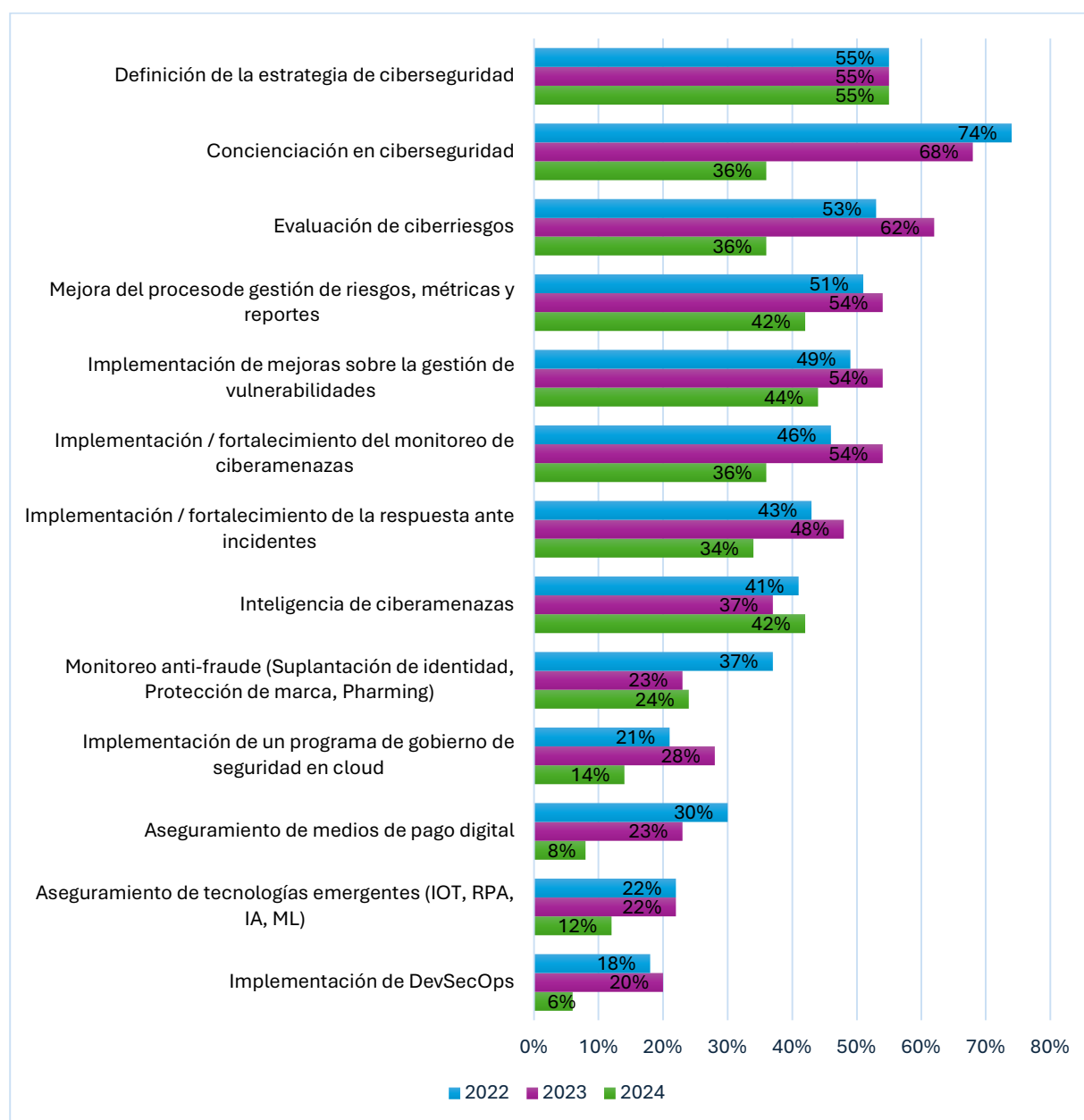
2.4. Análisis comparativo

2.4.1. Comparación entre PYMES y grandes empresas

La ciberseguridad es un desafío creciente para todas las organizaciones, la brecha entre las pequeñas y medianas empresas (PYMES) y las grandes empresas es notable. Esta diferencia significativa en la inversión les permite implementar tecnologías avanzadas, como inteligencia artificial y automatización, contratar personal especializado y realizar auditorías regulares, mejorando su capacidad de detección y respuesta ante incidentes (Symantec Broadcom, 2023).

Figura 8

Iniciativas de ciberseguridad para 2024



Nota: La figura muestra que la estrategia de ciberseguridad es la iniciativa más común y persistente en el sector privado de Ecuador. Fuente: IT Ahora & Deloitte (2024).

En Ecuador, esta disparidad es evidente, con muchas PYMES reportando dificultades para alinear su inversión en ciberseguridad con sus necesidades operativas. Las grandes empresas suelen tener departamentos dedicados a la ciberseguridad y una mayor frecuencia

de revisión de estos temas en sus juntas directivas, mientras que una proporción significativa de PYMES no tiene un presupuesto aprobado para ciberseguridad (IT Ahora & Deloitte, 2024).

2.4.2. Comparación con estándares

Las Pequeñas y Medianas Empresas (PYMES) ecuatorianas enfrentan desafíos significativos en la adopción de estándares internacionales de ciberseguridad, como ISO/IEC 27001 y NIST Cybersecurity Framework. A diferencia de las grandes empresas, que cuentan con recursos y conocimientos para implementar y mantener estrategias robustas, las PYMES a menudo carecen de los medios necesarios. Esta disparidad se refleja en la brecha existente entre las prácticas locales y los niveles de madurez observados en economías más avanzadas (IT Ahora & Deloitte, 2024).

La comparación con estándares internacionales revela que las PYMES ecuatorianas están por debajo de la media global en la implementación de prácticas clave, como los programas de gobierno de seguridad en la nube. Además, la adopción de certificaciones como ISO 27001 es menos común debido a los costos y la complejidad asociados (Carías Juan Francisco et al., 2021). Esta falta de cumplimiento se traduce en deficiencias en la implementación de políticas de seguridad, gestión de riesgos y controles de seguridad, aumentando la vulnerabilidad de las PYMES frente a ciberamenazas (Instituto Nacional de Ciberseguridad, 2020).

A diferencia de las grandes empresas y entidades gubernamentales, que priorizan la inversión en seguridad, las PYMES a menudo carecen de los medios para implementar las mejores prácticas recomendadas por marcos como NIST Cybersecurity Framework. Para abordar esta problemática, se han desarrollado programas de certificación ligeros, que buscan

adaptar los estándares a las capacidades y necesidades específicas de las PYMES (Ponsard et al., 2020).

Capítulo III. Propuesta

3.1. Introducción

La desigualdad digital y la ciberresiliencia son problemas críticos para las PYMES en Ecuador donde la digitalización está en crecimiento, pero enfrenta desafíos únicos debido a limitaciones de recursos y conocimientos técnicos. Las PYMES constituyen una parte importante de la economía ecuatoriana, pero la falta de ciberresiliencia las hace especialmente vulnerables a los ciberataques, que pueden tener impactos devastadores en su operación y supervivencia. Esta propuesta tiene como objetivo presentar estrategias específicas para reducir la brecha digital y fortalecer la ciberresiliencia de dichas PYMES, asegurando su sostenibilidad y crecimiento en un entorno digital cada vez más amenazante.

El entorno digital en Ecuador está marcado por una creciente adopción de tecnologías, pero también por una falta de infraestructura y capacitación adecuada en ciberseguridad. Según el informe "Estado actual de la ciberseguridad en Ecuador 2024", muchas PYMES no cuentan con políticas de seguridad robustas ni con personal capacitado para manejar incidentes cibernéticos. Esta propuesta busca abordar estas deficiencias mediante la implementación de programas de capacitación, acceso a tecnologías asequibles y la adopción de marcos de ciberseguridad reconocidos.

La ciberresiliencia no solo implica la protección contra ataques, sino también la capacidad de las PYMES para recuperarse y adaptarse después de un incidente cibernético. En un entorno donde las amenazas son constantes y evolucionan rápidamente, es crucial que las PYMES en Ecuador desarrollen una estrategia integral que abarque desde la prevención hasta la respuesta y recuperación.

3.2. Fundamentos

Las PYMES en Ecuador son especialmente vulnerables a los ciberataques debido a su falta de madurez y resiliencia en ciberseguridad. El informe State of Cybersecurity de CompTIA (2023) revela que más del 60% de los ataques cibernéticos se dirigen a PYMES, con un impacto significativo en su operación y supervivencia. Esta alta incidencia de ataques se debe en parte a la percepción errónea de que las PYMES son objetivos menos atractivos para los atacantes. Sin embargo, la realidad es que su tamaño y la falta de recursos dedicados a la ciberseguridad las convierten en blancos fáciles.

Un estudio de Ambreena et al. (2024) destaca que las PYMES tienden a subestimar el riesgo cibernético, lo que aumenta su vulnerabilidad. Además, muchas PYMES carecen de un enfoque estructurado para la gestión de riesgos cibernéticos, lo que dificulta su capacidad para identificar y mitigar amenazas de manera efectiva.

El fortalecimiento de la ciberresiliencia de las PYMES requiere un enfoque integral que incluya la evaluación de riesgos, la implementación de marcos de ciberseguridad y el desarrollo de planes de respuesta y recuperación. Adoptar marcos reconocidos, como el NIST Cybersecurity Framework, puede ayudar a estructurar y guiar las prácticas de seguridad cibernética de las PYMES, asegurando que estén preparadas para enfrentar y recuperarse de incidentes cibernéticos.

3.3. Descripción detallada de la propuesta

3.3.1. Estrategias para reducir la brecha digital

Para reducir la brecha digital, se propone implementar programas de formación y capacitación en ciberseguridad dirigidos específicamente a PYMES en Ecuador. Estos programas deben incluir:

1. Capacitación en habilidades digitales básicas y avanzadas: Asegurar que los empleados de PYMES posean competencias digitales fundamentales y avanzadas para manejar herramientas y plataformas tecnológicas de manera segura. Esto no solo mejora la productividad, sino que también reduce el riesgo de errores humanos que puedan comprometer la seguridad de la información.
2. Concienciación sobre ciberseguridad: Implementar campañas de concienciación sobre las amenazas cibernéticas y las mejores prácticas de seguridad. Esto puede incluir talleres, seminarios web y materiales educativos accesibles para todos los niveles de la organización. La concienciación continua ayuda a crear una cultura de seguridad dentro de la empresa.
3. Acceso a recursos tecnológicos: Facilitar el acceso a tecnologías y herramientas de ciberseguridad, como software antivirus, firewalls y sistemas de detección de intrusiones, mediante subvenciones o programas de apoyo financiero. Esto es especialmente importante para PYMES con presupuestos limitados, permitiéndoles implementar soluciones de seguridad efectivas sin incurrir en altos costos.

3.3.2. Fortalecimiento de la ciberresiliencia

El fortalecimiento de la ciberresiliencia de las PYMES requiere un enfoque integral que incluya:

1. Evaluación de riesgos cibernéticos: Realizar evaluaciones periódicas de riesgos para identificar vulnerabilidades y amenazas específicas a las que se enfrenta la organización. Estas evaluaciones deben ser realizadas por expertos en ciberseguridad para asegurar una identificación precisa y exhaustiva de los riesgos.
2. Implementación de un marco de ciberseguridad: Adoptar marcos reconocidos, como el NIST Cybersecurity Framework, para estructurar y guiar las prácticas de seguridad cibernética. Este marco ayuda a las PYMES a identificar, proteger, detectar, responder y recuperarse de incidentes cibernéticos. La implementación de un marco estructurado proporciona una guía clara y comprobada para gestionar la ciberseguridad.
3. Desarrollo de planes de respuesta y recuperación: Establecer y probar planes de respuesta a incidentes y recuperación ante desastres para asegurar que las PYMES puedan mantener la continuidad del negocio durante y después de un ataque cibernético. Estos planes deben incluir procedimientos claros para la identificación, contención y mitigación de incidentes cibernéticos, así como estrategias para la recuperación rápida de las operaciones.

3.3.3. Adaptación a las necesidades de las PYMES

Las estrategias de ciberseguridad deben adaptarse a las necesidades y capacidades específicas de las PYMES en Ecuador. Esto incluye:

1. Soluciones personalizadas y escalables: Ofrecer soluciones de ciberseguridad que sean asequibles y escalables, permitiendo a las PYMES adoptar medidas de seguridad progresivamente a medida que crecen sus recursos y necesidades. Las soluciones

deben ser flexibles para ajustarse a los cambios en el tamaño y la complejidad de la empresa.

2. Asesoramiento y apoyo continuo: Proveer asesoramiento y soporte técnico continuo a través de redes de expertos en ciberseguridad y programas de mentoría para ayudar a las PYMES a implementar y mantener sus medidas de seguridad. Este apoyo continuo es crucial para asegurar que las PYMES puedan adaptarse rápidamente a nuevas amenazas y tecnologías.
3. Implementación gradual: Adoptar un enfoque de implementación gradual que permita a las PYMES desarrollar y fortalecer su ciberseguridad sin sobrecargar sus recursos. Esto puede incluir la priorización de medidas críticas a corto plazo, seguidas de mejoras adicionales a medida que se disponga de más recursos.

3.4. Evaluación de la propuesta

La evaluación de la propuesta debe basarse en indicadores clave de rendimiento (KPI) que midan la eficacia de las estrategias implementadas. Estos indicadores pueden incluir:

1. Reducción en el número de incidentes cibernéticos: Monitorizar la cantidad de incidentes cibernéticos reportados antes y después de la implementación de las estrategias propuestas. Un descenso en el número de incidentes indicará la efectividad de las medidas implementadas.
2. Aumento en el nivel de concientización y capacitación: Evaluar el incremento en la participación de empleados en programas de capacitación y su nivel de comprensión de las mejores prácticas de ciberseguridad. Esto se puede medir mediante encuestas y pruebas de conocimiento antes y después de las sesiones de capacitación.

3. Mejora en la resiliencia operativa: Medir la capacidad de las PYMES para continuar sus operaciones durante y después de un incidente cibernético, evaluando la eficacia de sus planes de respuesta y recuperación. Indicadores como el tiempo de recuperación y la capacidad para mantener operaciones críticas durante un incidente son métricas clave.

La evaluación debe ser continua y adaptativa, permitiendo ajustes en las estrategias según sea necesario para abordar nuevas amenazas y cambios en el entorno empresarial. Además, la retroalimentación de los empleados y las auditorías regulares pueden proporcionar información valiosa para mejorar continuamente las medidas de ciberseguridad.

3.5. Plan de implementación

El plan de implementación debe seguir un enfoque escalonado para garantizar una adopción efectiva de las medidas propuestas:

Fase	Actividad	Duración
Fase 1: Diagnóstico inicial	Realizar una evaluación inicial de ciberseguridad para identificar puntos críticos y establecer una línea base. Esto incluye la identificación de vulnerabilidades en la infraestructura de TI, la evaluación de las prácticas de seguridad actuales y la recopilación de información sobre los activos más críticos de la empresa. Utilizando herramientas de análisis y entrevistas con el personal clave, se debe crear un informe detallado	1 mes

	de la situación actual y las áreas de mejora necesarias.	
Fase 2: Desarrollo de políticas	Crear políticas de ciberseguridad que normen la ejecución de las fases siguientes. Estas políticas deben incluir la definición de roles y responsabilidades, procedimientos para la gestión de incidentes, protocolos para la capacitación continua, normas para la implementación y uso de tecnologías de ciberseguridad, y directrices para la evaluación y monitoreo constante de riesgos. Se deben basar en marcos reconocidos y adaptarse a las necesidades específicas de las PYMES ecuatorianas, garantizando así una estructura clara y coherente para todas las actividades de seguridad.	1 mes
Fase 3: Capacitación y concienciación	Implementar programas de capacitación y concienciación para todos los empleados y directivos, centrándose en las mejores prácticas de ciberseguridad. Estos programas deben incluir talleres, seminarios web y materiales educativos accesibles para todos los niveles de la organización. La capacitación debe cubrir aspectos como la identificación de correos electrónicos de phishing, la gestión segura de contraseñas y la protección de datos personales. Es crucial fomentar una cultura de	2 meses

	ciberseguridad donde cada empleado entienda su papel en la protección de la organización.	
Fase 4: Implementación de tecnologías	Desplegar las tecnologías de ciberseguridad necesarias, como firewalls, sistemas de detección de intrusiones y soluciones antivirus. Esta fase debe incluir la instalación y configuración de herramientas de seguridad, así como la integración de estas tecnologías en la infraestructura existente. Es importante seleccionar soluciones que sean escalables y adecuadas para el tamaño y las necesidades específicas de la PYME, asegurando que se maximice el retorno de la inversión.	3 meses
Fase 5: Desarrollo de planes de respuesta y recuperación	Establecer y probar planes de respuesta a incidentes y recuperación ante desastres. Estos planes deben delinear los pasos a seguir en caso de un incidente cibernético, incluyendo la identificación y contención del ataque, la mitigación de daños y la recuperación de las operaciones. Se deben realizar simulacros regulares para asegurar que todos los empleados conozcan sus roles y responsabilidades durante un incidente y que los planes sean efectivos y actualizados.	2 meses
Fase 6: Monitoreo y evaluación continua	Realizar evaluaciones periódicas para medir la eficacia de las medidas implementadas y hacer ajustes según sea necesario. Este monitoreo debe	Continuo

incluir auditorías de seguridad, revisiones de políticas y procedimientos, y la implementación de mejoras continuas basadas en nuevas amenazas y vulnerabilidades identificadas. Además, se deben establecer métricas y KPIs para evaluar el desempeño de las iniciativas de ciberseguridad y asegurar que la organización se mantenga protegida de manera proactiva.

La implementación de estas fases no solo reducirá la brecha digital y fortalecerá la ciberresiliencia de las PYMES en Ecuador, sino que también contribuirá a su competitividad y sostenibilidad en el entorno digital global.

3.6. Métodos de seguimiento y evaluación

Para asegurar la eficacia continua de la propuesta, se deben implementar métodos de seguimiento y evaluación específicos que complementen las actividades de monitoreo continuo:

1. Auditorías de ciberseguridad: Realizar auditorías regulares llevadas a cabo por terceros independientes para proporcionar una evaluación imparcial de la infraestructura de seguridad de la organización. Estas auditorías deben enfocarse en identificar nuevas vulnerabilidades y asegurar que las políticas y procedimientos de ciberseguridad se estén siguiendo adecuadamente.
2. Revisiones de desempeño trimestrales: Evaluar trimestralmente el desempeño de las estrategias de ciberseguridad mediante revisiones de los indicadores clave de

rendimiento (KPI). Estas revisiones deben analizar datos recopilados durante las auditorías y el monitoreo continuo, permitiendo ajustes y mejoras en las políticas y prácticas implementadas.

3. Retroalimentación estructurada: Fomentar la retroalimentación continua de los empleados y partes interesadas a través de encuestas, entrevistas y reuniones regulares. La retroalimentación debe ser recopilada de manera sistemática y utilizada para identificar áreas de mejora y ajustar las estrategias de ciberseguridad según sea necesario.
4. Benchmarking: Comparar regularmente las prácticas de ciberseguridad de la organización con las mejores prácticas del sector y con organizaciones similares en términos de tamaño y complejidad. El benchmarking permite identificar brechas y oportunidades para mejorar la postura de ciberseguridad de la PYME.
5. Actualización de políticas y tecnologías: Revisar y actualizar periódicamente las políticas de ciberseguridad y las tecnologías implementadas para asegurar que se mantengan efectivas frente a nuevas amenazas y vulnerabilidades. Esta actividad debe incluir la evaluación de nuevas herramientas y soluciones tecnológicas que puedan mejorar la protección y la resiliencia de la organización.
6. Informes de progreso: Generar informes de progreso detallados que resuman las actividades de seguimiento y evaluación, los hallazgos de las auditorías y revisiones, y las acciones correctivas implementadas. Estos informes deben ser presentados a la alta dirección y otras partes interesadas para asegurar la transparencia y el compromiso continuo con la ciberseguridad.

Implementando estos métodos de seguimiento y evaluación, las PYMES en Ecuador pueden asegurar que sus estrategias de ciberseguridad sean efectivas y adaptativas,

proporcionando una defensa robusta contra las amenazas cibernéticas y apoyando su crecimiento y sostenibilidad en el entorno digital.

Capítulo IV. Conclusiones y recomendaciones

4.1. Conclusiones

1. Vulnerabilidad de las PYMES ecuatorianas: nuestras PYMES son altamente vulnerables a ciberataques debido a la desigualdad digital, la falta de recursos, la inversión insuficiente en ciberseguridad y la carencia de personal especializado.
2. Principales amenazas: el phishing y el ransomware son las principales amenazas que enfrentan las PYMES, tanto en Ecuador como globalmente, lo que resalta la necesidad de concientización y capacitación en ciberseguridad.
3. Brecha digital y falta de recursos: la brecha digital limita el acceso de las PYMES a tecnologías avanzadas y recursos de ciberseguridad, lo que agrava su vulnerabilidad. La falta de inversión en ciberseguridad impide la implementación de medidas de protección adecuadas.
4. Concienciación y capacitación insuficientes: La falta de concienciación y capacitación en ciberseguridad entre empleados y directivos de las PYMES aumenta el riesgo de ataques exitosos. Esta falta de conocimiento puede llevar a una percepción errónea de la seguridad real de la empresa, subestimando los riesgos existentes.
5. Ausencia de planes de respuesta y estrategias: la mayoría de las PYMES carecen de planes de respuesta a incidentes y estrategias claras para enfrentar las ciberamenazas, lo que dificulta su recuperación en caso de ataques.
6. Impacto económico de los ciberataques: los ciberataques tienen un impacto económico significativo en las PYMES, afectando su estabilidad operativa, su reputación y su capacidad para recuperarse.
7. Limitada colaboración intersectorial: la colaboración entre diferentes sectores en Ecuador para abordar la ciberseguridad es limitada, lo que impide una respuesta más

coordinada y efectiva. A nivel global existen iniciativas de este tipo, sobre todo en países desarrollados.

8. Aumento de amenazas internas: el incremento de ataques internos en las PYMES resalta la importancia de fortalecer las políticas de seguridad interna y la capacitación del personal.
9. Importancia de la ciberresiliencia: es crucial para que las PYMES puedan recuperarse rápidamente de incidentes cibernéticos y garantizar la continuidad de sus operaciones.
10. Necesidad de políticas y estándares: la implementación de políticas de seguridad sólidas y la adopción de estándares internacionales de ciberseguridad son fundamentales para proteger a las PYMES.
11. Colaboración y apoyo externo: la colaboración con proveedores de servicios de ciberseguridad y la adopción de tecnologías avanzadas, como la inteligencia artificial, pueden mejorar la ciberresiliencia de las PYMES.
12. Monitoreo y evaluación continuos: el monitoreo constante de los sistemas y la evaluación periódica de las estrategias de ciberseguridad son esenciales para adaptarse a las nuevas amenazas y garantizar la eficacia de las medidas de protección.

4.2. Recomendaciones

1. Capacitación y concienciación, aumentar la inversión en programas de capacitación y educación en ciberseguridad para el personal de las PYMES ecuatorianas, mejorando su capacidad para identificar y responder a amenazas.
2. Acceso a financiamiento y subsidios, facilitando la adquisición de tecnologías avanzadas de ciberseguridad.
3. Políticas y procedimientos: desarrollar e implementar políticas y procedimientos robustos de ciberseguridad adaptados específicamente a las PYMES ecuatorianas.

4. Revisión en juntas directivas: establecer una mayor frecuencia en la revisión de temas de ciberseguridad en las juntas directivas de las PYMES ecuatorianas.
5. Estrategias claras: crear estrategias de ciberseguridad alineadas con los objetivos empresariales de las PYMES ecuatorianas para mejorar su resiliencia.
6. Monitoreo continuo: establecer sistemas de monitoreo continuo para evaluar la efectividad de las medidas de ciberseguridad adoptadas en Ecuador.
7. Plataformas colaborativas: crear plataformas colaborativas donde las PYMES ecuatorianas puedan compartir conocimientos y recursos de ciberseguridad.
8. Auditorías regulares: llevar a cabo auditorías regulares para asegurar el cumplimiento de las políticas de ciberseguridad y mejorar las prácticas existentes en Ecuador.
9. Evaluación y ajuste anual: implementar un proceso de revisión anual para evaluar el progreso de las estrategias de ciberseguridad y hacer ajustes según los resultados.
10. Asesoramiento personalizado y accesible para ayudar a las PYMES ecuatorianas a implementar medidas de seguridad adecuadas sin incurrir en altos costos.

Figura 2

Evaluación de calidad de los estudios en base a su relevancia, metodología y solidez de sus conclusiones, se agrega número de vistas y citas en otros trabajos de investigación.

Cod.	Uso	Rvw	Citas	Referencia	Tipo	Nombre	Año	Autor
1	5	5758	11 OK	Total	Journal Article	A Shared Cyber Threat Intelligence Solution for SMEs	2021	Van Haastrecht, Max
2	5	1136	8 OK	Total	Conference Proceedings	An Analysis of Cybersecurity Awareness Efforts for Swiss SMEs	2023	Byrce, C
3	4	2581	7 OK	Total	Disertación	Cyber Resilience Operationalization Framework CR-OF for SMEs	2021	Carras, Juan Francisco, Hernandez, Joseune, Arrabalaga, Slic
4	5	1512	0 OK	Total	Conference Proceedings	Cybersecurity Awareness and Capacities of SMEs	2023	Erdogan, Geney, Helvostud Begnild, Bolestis Costas, Iye
5	5	173	3 OK	Total	Conference Proceedings	Cybersecurity in SMEs in the Baltic Sea Region	2022	Falch, Møllen, Oleksen Hemming, Skouby Knud Erik, Taddayor
6	4	31	2 OK	Total	Journal Article	Cybersecurity Readiness A Model for SMEs based on the Socio-Technical Perspective	2022	Perezto Hual, Zaghoul Fatema, Ravarini Aurelio
7	5	1485	1 OK	Total	Journal Article	Digital Transformation and Cybersecurity Challenges for Businesses Resilience Issues and Recommendations	2023	Fernandez de Arroyabe Juan Carlos, Arroyabe Maria, Fern
8	4	14325	14 OK	Total	Journal Article	Effective Cybersecurity risk management practices for small and medium-sized enterprises A comprehensive review	2023	Saeed Saql, Altamimi Salim, Alkayal North, Alshehri Eht
9	5	87	0 OK	Total	Journal Article	Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response	2024	Amrbeen Lubna, Jain Manjula, Yadav Rakesh Kumar, Looel
10	5	3142	8 OK	SOC	Journal Article	Exploring Cybersecurity Ecosystem in the Middle East Towards an SME Recommender System	2023	Illa Lucian, Lucian Ogrutan, Bilan Titus
11	4	4957	5 OK	Total	Journal Article	From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium	2021	Naveed Ahmed Nadir, Naveeth Krishnadas
12	4	463	10 OK	Total	Conference Proceedings	Improving Cybersecurity Awareness Among SMEs in the Manufacturing Industry	2020	Ponsard Christophe, Massonet Philippe, Grandclaudon Jer
13	4	327	2 OK	Total	Journal Article	Redefining the Approach to Cybersecurity	2022	Johnanson Kevin, Paulsson Tim, Beegstom Erik, Selgerott
14	5	1139	8 OK	Total	Journal Article	Organizational Cybersecurity Readiness in the ICT sector a quant-qualitative assessment	2024	Neri Martina, Niccolini Federico, Martino Luigi
15	4	807	2 OK	Total	Book Section	Redefining the Approach to Cybersecurity	2020	Corradini Isabella
16	5	88	9 OK	Total	Journal Article	Rispe for SMEs A Systematic Review of Socio-Technical Cybersecurity Metrics	2021	van Haastrecht Max, Vigot Oskar Bilge, Brinkhuis Mathieu
17	5	4311	12 OK	Total	Journal Article	Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs) A Meta-Analysis Approach	2023	Al-Osairi Khalifa, Fetais Noora
18	5	6789	5 OK	Total	Journal Article	Survey and Lessons Learned on Raising SME Awareness about Cybersecurity	2019	Ponsard Christophe, Grandclaudon Jeremy, Bul Sebastian
19	5	185	12 OK	Belgica	Conference Proceedings	Systematic Approach to Cyber Resilience Operationalization in SMEs	2020	Carras Juan Francisco, Borges Marcos, Labaka Lere, Arrat
20	5	4737	28 OK	Marco para PYMES	Journal Article	Raising Cybersecurity Awareness in Small and Medium-sized Businesses in Norway	2022	Siggeund Martine
21	4	430	4 OK	Parcial, Noruega	Teis	Cheramenazas contra entornos empresariales	2020	
22	4			Total	Guia	Global Cybersecurity Outlook 2024	2024	Bueemann Gretchen, Rohrs Michael
23	5			Total	Informe	Decálogo Ciberseguridad Empreas	2017	
24	5			Total	Informe	Cybersecurity guide for SMEs	2021	
25	4			OK	Working Paper	State of Vulnerability Management Report	2023	Sysence
26	4			OK	Informe	Ransomware Report	2023	Bullwall
27	4			OK	Informe	Insider Threat Report	2023	Gurcul
28	5			OK	Informe	SME cybersecurity awareness program 2	2021	
29	4	246	5 OK	Programas a bajo costo Working Paper	Informe	Cybersecurity for SMEs Challenges and Recommendations	2021	
30	4			OK	Informe	Cost of a Data Breach Report 2023	2023	
31	5			OK	Informe	Cyber Resilienc: Safeguarding the Digital Organization	2016	Huica Angel, Manley Brittany, Rogers Lamy
32	4			OK	Working Paper	Building a Cybersecurity Awareness Program	2020	
33	5			OK	Informe	Metodología de evaluación de indicadores para Mejora de la ciberresiliencia (IMC)	2023	Gupta Mananik, Akiri Charanumar, Aryal Kishiz, Parker El
34	5			OK	Informe	AI Automation and Cybersecurity	2023	
35	4	136 OK		Uso de IA en ciberseguridad Informe	Informe	Google cloud cybersecurity forecast 2024	2024	
36	4			OK	Informe	Red Report 2023 10 tecnicas mas usadas por cibercriminales	2024	Cherles Carmakal, Sandra Ioyce, Sunil Pott, Phil Verables
37	4			OK	Informe	Symantec, Ransomware, Threat Landscape 2024	2023	
38	4			OK	Informe	Estado actual de la ciberseguridad Ecuador 2024	2024	
39	4			OK	Informe			
40	4			OK	Informe			
41	5	N/A		estadísticas utiles	Informe			

Bibliografía

- Ambreen, L., Jain, M., Yadav, R. K., & Loonkar, S. (2024). Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, 6, 2023ss080. <https://doi.org/10.31893/multirev.2023ss080>
- Bueermann, G., & Rohrs, M. (2024). *Global Security Outlook 2024*.
- Candau, J. (2021). Ciberseguridad Evolución y tendencias. *Boletín IEEE*, 23, 460-494.
- Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*, 8, 174200-174221. <https://doi.org/10.1109/ACCESS.2020.3026063>
- Carías Juan Francisco, Hernantes Josune, & Arrizabalaga Saioa. (2021). *Cyber Resilience Operationalization Framework CR OF for SMEs*. 1-220.
- Cisco Public. (2016). *Cyber Resilience: Safeguarding the Digital Organization*.
- Comisión Europea. (2016). *Guía del usuario sobre la definición del concepto de pyme*.
- Computing Technology Industry Association. (2023). *State of Cybersecurity 2024*.
- Díaz-Granados, S. (2023, noviembre 29). *La vía verde y digital de las pymes latinoamericanas*. CAF Banco de Desarrollo de América Latina y el Caribe.
- Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. (2023). Cybersecurity Awareness and Capacities of SMEs. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, 296-304. <https://doi.org/10.5220/0011609600003405>
- Espinoza-Zelaya, C., & Moon, Y. B. (2023). Framework for enhancing the operational resilience of cyber-manufacturing systems against cyber-attacks. *Manufacturing Letters*, 35, 843-850. <https://doi.org/10.1016/j.mfglet.2023.07.004>
- European Union Agency for Cybersecurity. (2021). *Cybersecurity for SMES Challenges and Recommendations*.
- Google LLC. (2023). *Google Cloud Cybersecurity Forecast 2024*.
- Gurukul. (2023). *Insider Threat Report*.
- Instituto Nacional de Ciberseguridad. (2017). *Decálogo ciberseguridad empresas*.
- Instituto Nacional de Ciberseguridad. (2020). *Ciberamenazas contra entornos empresariales*.
- Instituto Nacional de Ciberseguridad. (2023). *Metodología de evaluación de Indicadores para Mejora de la Ciberresiliencia (IMC)*.
- IT Ahora & Deloitte. (2024). *Estado actual de la ciberseguridad Ecuador 2024*.
- Ponsard, C., Massonet, P., Grandclaoudon, J., & Point, N. (2020). From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. *2020 IEEE European*

Symposium on Security and Privacy Workshops (EuroS&PW), 75-78.
<https://doi.org/10.1109/EuroSPW51379.2020.00019>

Real Academia Española. (2024, enero 12). *Diccionario de la Lengua Española*.

Servicio Ecuatoriano de Normalización. (2024, enero 13). *Mipymes y Organizaciones de Economía Popular y Solidaria son una pieza clave para la economía del país*. Mipymes.

Symantec Broadcom. (2023). *AI Automation and Cybersecurity*.