LA IMPORTANCIA DE LA CIBERRESILENCIA EN LAS EMPRESAS PYMES EN COLOMBIA

Oscar Julian Morera León[1], Andrés Camilo Ochoa Bermúdez[2], John Fredy Farfán Mancera[3], Héctor Manuel Herrera[4]

[1]Fundación Universitaria Los Libertadores – Estudiante Especialización
[2]Fundación Universitaria Los Libertadores – Estudiante Especialización
[3]Fundación Universitaria Los Libertadores – Estudiante Especialización
[4]Fundación Universitaria Los Libertadores – Director Proyecto de Aplicación

RESUMEN

Este artículo se plantea la importancia de la ciberresiliencia en las pequeñas y medianas empresas (PYMES) de Colombia, analizando en profundidad la situación actual de estas empresas en cuanto a la concientización y la implementación de medidas de seguridad. La ciberresiliencia se refiere a la capacidad de una organización para prepararse, responder y recuperarse de los ciberataques, y es esencial para garantizar la continuidad operativa y la protección de la información crítica.

En este estudio, se pretende identificar el grado de madurez en el que se encuentran las PYMES para afrontar y superar un ciberataque, evaluando su capacidad de respuesta y recuperación ante incidentes de seguridad.

Para profundizar en la importancia de la ciberresiliencia, este artículo se centrará en el despliegue de una encuesta dirigida a PYMES de diferentes sectores de mercado. Las preguntas de la encuesta estarán orientadas en los controles de las normas ISO 27001 y 27005, dos estándares internacionales fundamentales para la gestión de la seguridad de la información y la gestión de riesgos, respectivamente. La norma ISO 27001 establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), mientras que la ISO 27005 proporciona directrices para la gestión de riesgos asociados a la seguridad de la información.

Al finalizar, se consolidarán los resultados obtenidos para obtener un mayor entendimiento del enfoque del problema y, con ello, proporcionar un listado de recomendaciones y buenas prácticas que estas empresas deberían integrar en sus negocios. Estas recomendaciones incluirán estrategias para mejorar la concientización sobre la ciberseguridad, medidas para fortalecer las políticas de seguridad y sugerencias para optimizar la asignación de recursos a la gestión de riesgos. Asimismo, se propondrán acciones específicas para mejorar la capacidad de respuesta y recuperación ante ciberataques, garantizando así una mayor ciberresiliencia en las PYMES colombianas.

Palabras clave: amenazas, seguridad digital, activos, negocio, estrategia, continuidad.

ABSTRACT

This article considers the importance of cyber resilience in small and medium-sized businesses (SMEs) in Colombia, analyzing in depth the current situation of these companies in terms of awareness and implementation of security measures. Cyber resilience refers to an organization's ability to prepare, respond and recover from cyber attacks, and is essential to ensure operational continuity and the protection of critical information.

In this study, the aim is to identify the degree of maturity in which SMEs are to face and overcome a cyber attack, evaluating their capacity to respond and recover from security incidents. To delve deeper into the importance of cyber resilience, this article will focus on the deployment of a survey aimed at SMEs from different market sectors. The survey questions will be oriented towards the controls of the ISO 27001 and 27005 standards, two fundamental international standards for information security management and risk management, respectively. ISO 27001 establishes the requirements for an information security management system (ISMS), while ISO 27005 provides guidelines for managing risks associated with information security.

At the end, the results obtained will be consolidated to obtain a greater understanding of the approach to the problem and, with this, provide a list of recommendations and good practices that these companies should integrate into their businesses. These recommendations will include strategies to improve cybersecurity awareness, measures to strengthen security policies, and suggestions to optimize resource allocation to risk management. Likewise, specific actions will be proposed to improve the response and recovery capacity against cyber attacks, thus guaranteeing greater cyber resilience in Colombian SMEs.

Keywords: threats, digital security, assets, business, strategy, continuity.

1. INTRODUCCIÓN

El avance de la tecnología ha traído consigo numerosos beneficios, pero también ha aumentado la exposición de los sistemas de información a los ataques cibernéticos. Para protegerse contra estas amenazas, las organizaciones deben implementar medidas de seguridad sólidas, mantenerse al día con las mejores prácticas de ciberseguridad y estar preparadas para responder de manera efectiva en caso de un incidente de seguridad.

A medida que la tecnología avanza, los sistemas de información se vuelven más expuestos a ataques cibernéticos debido a varios factores:

- Interconexión creciente: Con la expansión de Internet y la adopción de tecnologías como la nube y el Internet de las cosas (IoT), los sistemas están más interconectados que nunca. Cada dispositivo conectado representa un punto potencial de vulnerabilidad que los ciberdelincuentes pueden explotar.
- Complejidad de los sistemas: Los sistemas de información modernos son cada vez más complejos, con múltiples capas de software, hardware y protocolos de comunicación. Esta complejidad aumenta la superficie de ataque y hace que sea más difícil proteger todos los puntos de acceso.
- Dependencia de datos y tecnología: En la era digital, las organizaciones dependen en gran medida de los datos y la tecnología para operar. Esto significa que los ciberataques pueden tener consecuencias graves, desde la interrupción de operaciones comerciales hasta la pérdida de datos confidenciales o la manipulación de información crítica.
- Avances en herramientas de hacking: Los ciberdelincuentes tienen acceso a herramientas cada vez más sofisticadas y automatizadas que les

permiten llevar a cabo ataques de manera más eficiente y efectiva. Esto incluye ransomware, malware avanzado, técnicas de ingeniería social y exploits de vulnerabilidades.

- Escasez de habilidades en ciberseguridad: Aunque la demanda de expertos en ciberseguridad está en aumento, aún existe una escasez de talento en este campo. Esto significa que muchas organizaciones no cuentan con los recursos necesarios para proteger adecuadamente sus sistemas de información contra ataques cibernéticos.

Las empresas tipo PYMES deben priorizar la madurez en ciberresiliencia, ya que esta les permite elaborar planes de acción eficaces para mitigar riesgos, recuperarse rápidamente de ataques y asegurar la continuidad del negocio al minimizar su impacto. La confianza del cliente resulta vital en este contexto, pues los ciberataques pueden comprometer datos confidenciales y dañar la reputación empresarial. Por ende, la ciberresiliencia refleja un compromiso serio con la seguridad de los datos, lo que contribuye a proteger la confianza del cliente. Además, el cumplimiento normativo se vuelve esencial para evitar multas y sanciones, y la ciberresiliencia ayuda a las PYMES a cumplir con regulaciones sobre protección de datos y ciberseguridad, reduciendo así riesgos legales y financieros.

En un mercado competitivo, una sólida ciberresiliencia se convierte en un factor diferenciador para las empresas. Los clientes valoran la seguridad de los datos y prefieren trabajar con empresas comprometidas con la ciberseguridad, lo que puede influir en sus decisiones de colaboración.

1.1 **JUSTIFICACIÓN.**

Colombia, al igual que muchas otras naciones, enfrenta una creciente amenaza de ciberataques debido al aumento de la digitalización de los negocios y la información. Las PYMES, en particular, pueden ser más vulnerables debido a recursos limitados y una menor conciencia sobre ciberseguridad. Por lo tanto, comprender los riesgos específicos que enfrentan estas empresas en el contexto colombiano es esencial para desarrollar estrategias efectivas de ciberresiliencia.

En segundo lugar, las PYMES representan una parte significativa de la economía colombiana y desempeñan un papel vital en la generación de empleo y el crecimiento económico. Proteger estas empresas de los ciberataques es crucial para salvaguardar la estabilidad y el desarrollo económico del país. La interrupción de las operaciones comerciales debido a un ciberataque puede tener repercusiones devastadoras, especialmente para las PYMES que pueden carecer de los recursos para recuperarse rápidamente.

Además, la confianza del cliente es un activo invaluable para cualquier empresa, y las PYMES no son una excepción. Los consumidores colombianos esperan que sus datos personales estén seguros y protegidos cuando interactúan con empresas en línea. Por lo tanto, la incapacidad de las PYMES para garantizar la seguridad de los datos puede erosionar la confianza del cliente y dañar la reputación de la empresa.

Investigar el análisis de por qué las empresas tipo PYMES en Colombia deben ser ciberresilientes es esencial para comprender los riesgos específicos que enfrentan estas empresas. Esta investigación proporcionaría una base sólida para desarrollar estrategias efectivas de ciberseguridad que fortalezcan la resiliencia de las PYMES colombianas frente a las crecientes amenazas cibernéticas.

1.2 **PREGUNTA PROBLEMA.**

¿Qué tan importante es que las empresas PYMES Colombia sean ciberresilientes para la continuidad de sus negocios?

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL.

Analizar el impacto que genera la ciberresilencia en la continuidad del negocio en

las empresas PYMES en Colombia.

1.3.2 OBJETIVOS ESPECIFICOS.

Evaluar el nivel de conciencia sobre ciberseguridad de las empresas PYMES de Colombia.

Identificar las principales amenazas cibernéticas que enfrentan las empresas PYMES en Colombia.

Proponer estrategias y buenas prácticas para fortalecer la ciberresiliencia en las empresas PYMES en Colombia, mediante normativas encaminadas hacia la seguridad de seguridad (ISO27001) y gestión de riesgos de seguridad de la información (ISO 27005).

1.4 ALCANCE.

El presente artículo se enfocará en el análisis de la ciberresiliencia en las empresas de Colombia de tipo PYMES, teniendo en cuenta aspectos como la concientización sobre la ciberseguridad, el valor de la información, la recuperación de desastres y la continuidad del negocio. Con lo anterior, se estipularán recomendaciones basadas en las normas ISO 27001 y 27002, que apalanque la seguridad digital, para que las empresas tengan como referente, puedan aplicar a sus negocios.

2. REFERENTES TEÓRICOS.

Para el Resilience Institute, la capacidad resiliente de las organizaciones parte de las personas y crea un paralelo en diferentes niveles de evolución, estableciendo un punto de inflexión entre el deber ser (positivo) y lo no aceptable (negativo), en la medida que se cumple con los 60 factores de resiliencia que están organizados en 11 categorías. La meta es evolucionar y sostener dicha evolución en la medida que se reconoce las debilidades y riesgos y se trabaja para resolverlos.

La División CERT se encuentra dentro de la SEI, un centro de investigación y desarrollo financiado por el gobierno federal en la Universidad Carnegie Mellon, ubicada en la ciudad de Pittsburgh (Pensilvania); la cual es una de las universidades más destacada en investigación superior de los Estados Unidos en el área de ciencias de la computación y robótica.

La División de CERT está catalogado como un bien de los Estados Unidos en el campo de la ciberseguridad y se reconoce como una organización de confianza, una autoridad dedicada a mejorar la seguridad y la resiliencia de los sistemas y redes informáticas. La División CERT regularmente se asocia con el gobierno, la industria, la aplicación de la ley, y la academia de los Estados Unidos para desarrollar métodos y tecnologías avanzadas con el fin de contrarrestar a gran escala, las amenazas informáticas más sofisticadas.

Robo de información sensible de Estados:

Impacto: En medio de una tensión entre la transparencia y la protección de la información clave para la defensa del Estado, los adversarios distraen la atención de los Gobiernos con eventos de gran magnitud para poder, mediante el reconocimiento de los puntos débiles de sus infraestructuras, materializar fugas de información durante estas distracciones, que permitan crear ventajas estratégicas en el contexto regional y global (Daswani, 2021). Evidencia: Se ha hallado robo de información de servidores públicos, fuga de información de miembros de las fuerzas militares (FF. MM.) y revelación de información de inteligencia.

Los atacantes en Colombia han centrado la atención en bases de datos de los miembros de las FF. MM., particularmente de inteligencia, que han generado tensiones internas por la sensibilidad de la información filtrada y la posibilidad de poner en riesgo la integridad física de los integrantes de las FF. MM. (Noticias Caracol, 2021). Teniendo en cuenta que la lista de vulnerabilidades está relacionada con el software que posee la organización y su versión, en esta investigación

se seleccionaron los paquetes de Softwares comerciales comúnmente usados en las pymes en Colombia. La estrategia propuesta para la especificación y construcción de una herramienta para la búsqueda de vulnerabilidades cibernéticas en pymes considera un proceso sistémico y sistemático cuya definición y declaración inicial corresponde con el planteamiento de un proyecto de investigación. (García-González y Sánchez-Sánchez, 2020).

A nivel territorial cada país cuenta con políticas enfocadas para la protección de la información, para la república de Colombia se cuenta con el Consejo Nacional de Política Económica y Social -CONPES 3995 del año 2020, de la política nacional de confianza y seguridad digital en el que se busca fortalecer la capacidad en materia de la seguridad digital de los ciudadanos en el sector privado o público y aumentar la confianza en el manejo de la información digital del país, es por ello que las empresas que no cumplan con estándares en materia de ciberseguridad pueden llegar a incurrir en sanciones que pueden llegar a causar el fracaso de una empresa (Conpes 3995, 2020).

También es importante capacitar constantemente a los miembros del equipo para mantener los conocimientos actualizados, tener diferentes métodos de autenticación para lograr que los datos estén más blindados y usar la nube para tener resguardo de los datos de la empresa. (Tania valentina pulido pulido - Bogotá D.C 2 de diciembre de 2022)

Algunas de las razones por las cuales las empresas no tienen la certificación de la NTC/ISO27001:2013 es el costo y que requiere un seguimiento constante, pero si nos ponemos a analizar, cuesta más solucionar un ataque que puede acabar con la empresa, que evitarlos haciendo uso de la normativa en ciberseguridad. (Conpes 3995, 2020)

Opinan que los esfuerzos de las empresas en tecnología y desarrollo pueden llegar a ser en vano si sus empleados no siguen los procesos definidos para la ciberseguridad, con temas como autenticación segura, claves dinámicas y completa confidencialidad. (González, A. 2020).

Para muchas empresas colombianas, el planear o asignar un presupuesto destinado a ciberseguridad y estar abiertas a confrontar estos retos digitales solo se evidencia en un 34.5%, debido a que sus políticas en ataques de ciberseguridad, herramientas tecnológicas avanzadas y planes de contingencia a futuro no están implementadas como requisito de funcionamiento dentro de las organizaciones. (Universidad EAN. 28 de noviembre de 2022. Estrategias de ciberseguridad en organizaciones en Colombia)

Así mismo, solo el 36.2% de las organizaciones encuestadas tiene un oficial o profesional encargado de la seguridad informativa, lo que hace concluir que la ciberseguridad está muy relacionada con el grado de implementación tecnológica en la empresa junto con la cantidad de dispositivos tecnológicos y su estructura organizacional destinada a su funcionamiento. (Universidad EAN - Estrategias de ciberseguridad en organizaciones en Colombia - Bogotá, D.C., 28 de noviembre de 2022)

Por consiguiente, el asignar o incrementar el presupuesto de ciberseguridad anualmente, refuerza las estrategias en riesgos informáticos en caso de enfrentar nuevos retos y desafíos cuando en las empresas se tiene cambios sustanciales en su organización. (Universidad EAN - Estrategias de ciberseguridad en organizaciones en Colombia - Bogotá, D.C., 28 de noviembre de 2022)

El objetivo de la ciberseguridad es contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para lograr sus objetivos. Para ello se busca reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo

razonable y a un coste aceptable. (Yamith Andrés Fernando Niño Wilches – 2015)

La gestión del riesgo hace parte de las buenas prácticas gerenciales. Esta es un proceso lógico y sistemático que permite “establecer el contexto, identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar las pérdidas y maximizar las oportunidades (Australia, 1999). Robert Kaplan, en su obra “Enteprise Risk Management”, enfatiza la importancia de que los gerentes conozcan y dimensionen los riesgos a los que está expuesta su compañía. (Dumitrescu, A. et Al., 2015)

Los resultados de la investigación de la encuesta arrojaron que, para el 100% de las pequeñas y medianas empresas consultadas, la ciberseguridad es importante como concepto; pero más del 65 % no tiene políticas para orientar buenas prácticas en el uso de activos de información, no tienen identificados los activos asociados a procesos críticos, no desarrollan una metodología de análisis de riesgo enfocado a TI que les permita gestionarlos de la manera adecuada; no asignan presupuesto y tampoco tienen personal con funciones de ciberseguridad. (Yamith Andrés Fernando Niño Wilches – 2015)

La implementación de estos elementos permitirá a las pequeñas y medianas empresas la gestión de los riesgos de las tecnologías de la información, asegurar los activos asociados a los procesos críticos, crear una cultura en torno a la ciberseguridad e incrementar la posibilidad de alcanzar las metas organizacionales. (Yamith Andrés Fernando Niño Wilches – 2015)

Los elementos identificados que componen el concepto de ciberseguridad son: políticas en materia de ciberseguridad, análisis y gestión del riesgo de tecnologías de la Información, cultura organizacional, Estructura organizacional, Herramientas tecnológicas y Planes de contingencia, cada uno de estos se debe implementar en menor o mayor medida de acuerdo al grado de exposición riesgo y al nivel de dependencia tecnológica que tenga la organización. (Yamith Andrés Fernando Niño Wilches – 2015)

La ciberseguridad es un factor clave para la competitividad y el desarrollo de las PYMES en Colombia, ya que les permite proteger su información, su reputación, su continuidad y su innovación. La información es el activo más valioso de las pymes, y su pérdida o compromiso puede tener consecuencias graves para su negocio. También es un requisito legal y normativo para las PYMES, ya que deben cumplir con las disposiciones vigentes en materia de protección de datos personales, ciberseguridad y demás aspectos relacionados con la gestión de la información. El incumplimiento de estas disposiciones puede acarrear sanciones legales y reputacionales para las pymes. La seguridad de los datos desafío constante para las PYMES, ya que se enfrentan a amenazas cada vez más sofisticadas y variadas, que pueden provenir de actores maliciosos internos o externos, o de errores humanos o técnicos. Las PYMES deben estar preparadas para prevenir, detectar y responder a estos incidentes, y recuperarse de ellos. (Carlos Alberto Peña Montenegro – 2023)

Las PYME son muy importantes para la economía y el desarrollo del país, ya que representan el 90% de las empresas colombianas y generan el 65% del empleo formal. Según Confecámaras, en 2020 había cerca de 1.7 millones de PYME registradas en el país, de los cuales el 96% eran microempresas, el 3.4% pequeñas y el 0,6% medianas empresas. La mayoría de las PYMES se concentran en los sectores de comercio, servicios y manufactura. (Carlos Alberto Peña Montenegro – 2023).

La norma ISO/IEC 27001 ayuda a las pymes a estructurar la capacitación en seguridad cibernética de acuerdo con las mejores prácticas internacionales, así como a definir responsabilidades en caso de incumplimiento (BSI, 2022)

La ciberseguridad no ha sido una alta

prioridad para la mayoría de las pymes (Benz & Chatterjee, 2020), aun cuando la mayoría de ellas parecen tener un nivel de conciencia sobre la importancia de la ciberseguridad. Al observar las estadísticas de ataques, continúa habiendo fallas. Una primera explicación es que las medidas de seguridad se perciben como demasiado complejas, lentas y que requieren un alto nivel de conocimientos técnicos sobre los sistemas de informática. Otra razón es la dificultad para pasar de la concientización inicial a la emergencia de una cultura de ciberseguridad interna, debido a la falta de recursos, tales como dinero, tiempo y experiencia (Ponsard et al., 2019)

Las tecnologías de información proporcionan accesibilidad masiva a varios servicios esenciales, como las redes en línea y, lo que es más importante, permite compartir datos e información entre los empleados de la organización. A pesar de los beneficios que las tecnologías ofrecen a las PYMES, estas también tienen puntos débiles, pues pueden ser explotadas por cibercriminales que busquen dañar a las organizaciones para cumplir con sus objetivos (Alahmari & Duncan, 2020). Según Saleem, Adebisi, Ande, & Hammoudeh (2017) en la actualidad, las empresas pequeñas y medianas sufren constantes ataques digitales en todo el mundo. Esto se debe a múltiples factores, entre los cuales destacan:

- Debido al tamaño de estas empresas, no se cuenta con el presupuesto suficiente para implementar los controles necesarios para protegerse ante ciberataques.

- Las empresas pequeñas subestiman el impacto de las ciber amenazas.

- No existen suficientes profesionales con experiencia en seguridad de información o ciberseguridad para suplir la creciente demanda.

- Los altos costos de las auditorías de seguridad y las campañas de entrenamiento para los usuarios no permiten que las PYMES identifiquen sus deficiencias y desplieguen. defensas digitales efectivas. (Villayzan Chancafe & Gutierrez Perona, 2020).

Las pequeñas empresas a menudo tienen menos recursos y carecen de experiencia en seguridad, lo que las hace más vulnerables a los ataques de phishing selectivo, y los ciberdelincuentes se están aprovechando. (Hageman, 2022)

Es fundamental considerar que las amenazas cibernéticas afectan tanto a las grandes como a las pequeñas empresas. Un informe de la firma de seguridad informática Hiscox reveló que, en 2020, el 28% de las pequeñas empresas sufrieron al menos un ciberataque, y el costo promedio de recuperación fue de más de $200,000 dólares. (Hiscox, 2021)

El ritmo acelerado en el crecimiento de los ciberataques ha llevado a la ciberseguridad a evolucionar en la gestión de las ciberamenazas, lo cual genera que las organizaciones adopten el concepto de ciberesiliencia, el cual se basa en la capacidad organizacional para anticipar, detectar, soportar, recuperarse y evolucionar después de los incidentes cibernéticos de manera estratégica. (Boot et al., 2021).

La acelerada evolución de la convergencia tecnológica, el aumento de la densidad digital y la asimetría de la información en una sociedad cada vez más digital y tecnológicamente modificada, establece un escenario de análisis más elaborado y complejo, que exige de parte de los analistas de negocio, de seguridad de la información y de ciberseguridad, una vista mucho más holística y el entendimiento de relaciones emergentes antes ignoradas por los saberes disciplinares y segmentados. (Jeimy J. Cano M.1, Alvaro Rocha)

La historia reciente ha dejado claro que la inevitabilidad es una constante: actualmente ninguna nación ni organización está exenta de sufrir un ciberataque. Lamentablemente, aún con numerosos esfuerzos preventivos que se vierten en regulaciones, estrategias y mejores prácticas para fortalecer la ciberseguridad, siempre existe la posibilidad de ser atacado con

éxito. (Mandiant, 2021).

En el mundo del ciberespacio, lo anterior lleva a observar que la cyberresiliencia no es en principio para evitar ciberataques; en caso de que ocurran, será para determinar el grado en que afectarán a las organizaciones y deberán adaptarse ante las nuevas condiciones. Es de gran importancia que muchos estudios de ciberresiliencia parecen tener un enfoque preventivo y de reacción inmediata; no obstante, existen otros documentos en los que se resalta la resiliencia como la capacidad para evolucionar, adaptarse y alcanzar un nuevo equilibrio. En el primero podría ser una resiliencia total [no pasó nada]; en el segundo, hubo un evento y se derivan secuelas, pero se debe seguir adelante. Para el autor de este artículo, esa última es la noción que se debe tener de ciber-resiliencia. (Arturo García Hernández)

Un modelo de madurez es un conjunto de características, atributos, indicadores o patrones que representan la capacidad y la progresión en una disciplina en particular. El contenido del modelo típicamente ejemplifica las mejores prácticas y puede incorporar normas u otros códigos de práctica de la disciplina. Los modelos de madurez en ciberseguridad consideran la seguridad cibernética a través de diferentes áreas/dimensiones, entendiendo que cada dimensión no es necesariamente independiente de las otras. (Rea-Guaman, A. M., Sánchez-García, I. D., San Feliu, T., & Calvo-Manzano, J. A.)

En la actualidad los sistemas de información, la internet y la computación en la nube son el soporte para el almacenamiento, gestión y aplicación de información personal y organizacional, convirtiéndose en el blanco para quienes la quieren robar, manipular o dañar, o desean afectar a sus propietarios. Esto se presenta porque las personas y las organizaciones soportan su rutina en esta información, de manera que cualquier manipulación o fallo termina afectándolos notoriamente, a nivel individual y colectivo. Osorio, A. (2017).

3. METODOLOGÍA.

Figura 1. Metodología propia (PHVA e iso27001 & 27005).

Nuestra metodología se basa en el modelo PHVA (Planear, Hacer, Verificar y Actuar), integrándolo con las normas ISO/IEC 27001 y 27005. En la fase de Planear, utilizamos la norma ISO 27005 para identificar y evaluar los riesgos y amenazas que enfrentan las empresas. Durante la etapa de Hacer, llevamos a cabo encuestas para analizar el estado de la ciberseguridad en las PYMES, siguiendo las directrices de la norma 27001.

En la fase de Verificar, evaluamos los resultados y el impacto que la implementación de controles y buenas prácticas de ciberseguridad tendría en estas empresas, con el objetivo de mitigar los riesgos identificados. Por último, en la fase de Actuar, nos centramos en concienciar a las PYMES sobre la importancia de adoptar estas buenas prácticas de ciberseguridad, proporcionando recomendaciones específicas para hacer frente a posibles ataques cibernéticos y garantizar la continuidad de sus negocios.

4. RESULTADOS

Para evaluar y analizar la conciencia sobre ciberseguridad en las PYMES, se distribuyó una encuesta (forms.office.com/r/LtwcstFbs3) a una lista de correos electrónicos de empresas PYMES de diversos sectores económicos (Ranking 1000

pymes). La encuesta incluye preguntas específicas sobre los controles básicos que las empresas deberían implementar para garantizar la continuidad de sus negocios y fortalecer su ciberseguridad frente a los ataques cibernéticos a los que se exponen.

Al finalizar el ejercicio, consolidamos 32 respuestas, lo que nos proporciona una visión general del estado de la ciberseguridad en estas empresas. Con esta información, podremos realizar un análisis detallado al respecto.

La encuesta consta de 11 preguntas y lleva como título: ¿Qué tan ciberresiliente es su empresa?:

Figura 2. *Encabezado del formulario lanzado a las pymes.*

Se obtuvieron respuesta de diferentes sectores económicos, entre los que más resaltan son los siguientes:

Figura 3. *Diferentes sectores económicos que participaron en la encuesta.*

Las preguntas del formulario y sus respuestas correspondientes fueron las siguientes:

1. *¿En su empresa hay un responsable sobre la seguridad de la información y la ciberseguridad?*

Gráfica 1 Consolidado respuestas pregunta 1.

Encontramos que el 63% de las empresas encuestadas no cuentan con un responsable dedicado a la seguridad de la información y ciberseguridad. En comparación con un 37% que si cuentan con él.

El análisis de las respuestas sugiere que hay una necesidad significativa de mejorar la postura de seguridad de la información en las empresas. Las organizaciones deben considerar seriamente la designación de un responsable para esta área crítica para proteger sus activos y garantizar la continuidad del negocio.

2. *¿La empresa tiene políticas y procedimientos de seguridad de la información formalmente documentados?*

Gráfica 2 Consolidado respuestas pregunta 2.

La distribución de respuestas muestra una tendencia preocupante en cuanto a la documentación y actualización de las políticas de seguridad de la información:

Completamente documentados y actualizados regularmente (1 empresa): Representa el 3.1% del total.

Documentados, pero no actualizados regularmente (19 empresas): Representa el 59.4% del total.

No completamente documentados (11 empresas): Representa el 34.4% del total.

No tenemos políticas y procedimientos formales (1 empresa): Representa el 3.1% del total.

El análisis de las respuestas revela una preocupación significativa sobre la gestión de las políticas y procedimientos de seguridad de la información en las empresas. Aunque muchas empresas tienen políticas documentadas, la falta de actualización regular es un problema común. Las empresas deben priorizar la revisión y actualización regular de sus políticas de seguridad para mantenerse protegidas contra las amenazas emergentes y cumplir con las regulaciones.

3. *¿La empresa proporciona capacitación regular en ciberseguridad a todos los empleados?*

Gráfica 3 Consolidado respuestas pregunta 3.

La distribución de las respuestas muestra variaciones significativas en la frecuencia y alcance de la capacitación en ciberseguridad en las empresas:

Capacitación anual para todos los empleados (1 empresa): Representa el 3.1% del total.

Capacitación menos frecuente (5 empresas): Representa el 15.6% del total.

Capacitación sólo para ciertos empleados (15 empresas): Representa el 46.9% del total.

Sin capacitación en ciberseguridad (11 empresas): Representa el 34.4% del total.

El análisis de las respuestas muestra que la mayoría de las empresas no están proporcionando capacitación adecuada y regular en ciberseguridad a todos sus empleados. Esto representa un riesgo significativo para la seguridad de la información y la resiliencia de las empresas ante ataques cibernéticos. Es esencial que las organizaciones inviertan en programas de capacitación integrales y regulares para todos los empleados para fortalecer su postura de seguridad y reducir la probabilidad de incidentes de seguridad.

4. *¿La empresa realiza evaluaciones regulares de riesgos de seguridad de la información?*

Gráfica 4 Consolidado respuestas pregunta 4.

La distribución de las respuestas muestra que la mayoría de las empresas no realizan evaluaciones de riesgos de seguridad de manera sistemática:

Evaluaciones sistemáticas y documentadas (2 empresas): Representa el 6.3% del total.

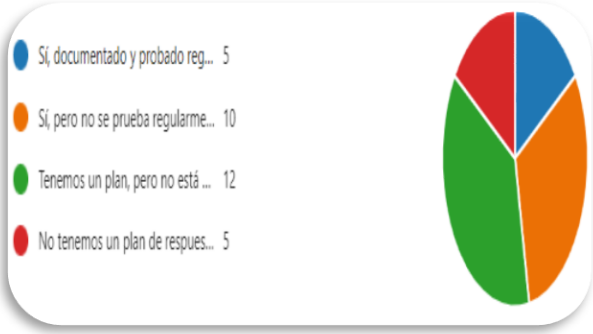
Evaluaciones no siempre sistemáticas (13 empresas): Representa el 40.6% del total.

Evaluaciones ocasionales sin proceso definido (16 empresas): Representa el 50% del total.

Sin evaluaciones de riesgos (1 empresa): Representa el 3.1% del total.

El análisis de las respuestas revela que la mayoría de las empresas no realizan evaluaciones de riesgos de seguridad de manera sistemática y documentada. Esto representa una debilidad significativa en la gestión de la seguridad de la información. Es crucial que las organizaciones adopten un enfoque estructurado y regular para la evaluación de riesgos, documentando los procesos y asegurando que se tomen medidas proactivas para mitigar los riesgos identificados. Esto no solo mejorará la postura de seguridad de la empresa, sino que también garantizará el cumplimiento normativo y la preparación ante posibles incidentes de seguridad.

5. *¿La empresa cuenta con un plan de respuesta a incidentes de seguridad?*



Gráfica 5 Consolidado respuestas pregunta 5.

La distribución de respuestas muestra que muchas empresas tienen planes de respuesta a incidentes, pero con diversas limitaciones en su implementación y prueba:

Documentado y probado regularmente (5 empresas): Representa el 15.6% del total.

Documentado, pero no probado regularmente (10 empresas): Representa el 31.3% del total.

No documentado (12 empresas): Representa el 37.5% del total.

Sin plan de respuesta a incidentes (5 empresas): Representa el 15.6% del total.

El análisis de las respuestas indica que, aunque muchas empresas tienen algún tipo de plan de respuesta a incidentes de seguridad, hay una falta generalizada de pruebas regulares y documentación adecuada. Esto puede comprometer la efectividad de la respuesta a incidentes y aumentar el riesgo y el impacto de los incidentes de seguridad. Es crucial que las organizaciones desarrollen, documenten y prueben regularmente sus planes de respuesta a incidentes para asegurar una respuesta eficaz y minimizar el impacto de los incidentes de seguridad.

6. *¿La empresa tiene implementado medios de seguridad en los equipos como firewall, AD, DLP y endpoints?*

Gráfica 6 Consolidado respuestas pregunta 6.

La distribución de respuestas muestra un rango en la implementación de medios de seguridad en los equipos:

Todos los medios implementados (1 empresa): Representa el 3.1% del total.

Al menos 2 medios implementados (19 empresas): Representa el 59.4% del total.

Un medio implementado (12 empresas): Representa el 37.5% del total.

Ningún medio implementado (0 empresas): Representa el 0% del total.

El análisis de las respuestas muestra que, aunque la mayoría de las empresas tienen implementados algunos medios de seguridad, muy pocas tienen una cobertura completa con firewall, antivirus, AD, y DLP. Esto deja a muchas empresas con áreas potenciales de vulnerabilidad. Es crucial que las empresas trabajen para implementar una combinación completa de medios de seguridad para asegurar una defensa robusta y minimizar el riesgo de brechas y otros incidentes de seguridad.

7. *¿La empresa utiliza autenticación multifactor (MFA) para el acceso a sistemas críticos?*

Gráfica 7 Consolidado respuestas pregunta 7.

La distribución de respuestas muestra la implementación variable de la autenticación multifactor en las empresas:

Para todos los sistemas críticos (2 empresas): Representa el 6.3% del total.

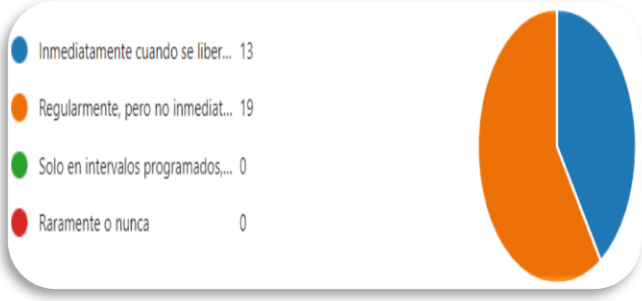
Para algunos sistemas críticos (9 empresas): Representa el 28.1% del total.

Considerando implementarlo (15 empresas): Representa el 46.9% del total.

No utilizan autenticación multifactor (6 empresas): Representa el 18.8% del total.

El análisis de las respuestas indica que, aunque hay una tendencia positiva hacia la consideración e implementación de MFA, la mayoría de las empresas aún no han adoptado completamente esta medida de seguridad esencial. Solo una pequeña fracción de las empresas ha implementado MFA para todos sus sistemas críticos, lo cual es crucial para proteger contra accesos no autorizados y mejorar la postura de seguridad general. Es vital que más empresas adopten MFA de manera completa y regular para fortalecer sus defensas contra amenazas cibernéticas.

8. *¿Con qué frecuencia se aplican parches y actualizaciones de seguridad en los sistemas de la empresa?*



Gráfica 8 Consolidado respuestas pregunta 8.

La distribución de respuestas muestra que las empresas son diligentes en la aplicación de parches y actualizaciones de seguridad:

Inmediatamente cuando se liberan (13 empresas): Representa el 40.6% del total.

Regularmente, pero no inmediatamente (19 empresas): Representa el 59.4% del total.

Solo en intervalos programados, sin urgencia (0 empresas): Representa el 0% del total.

Raramente o nunca (0 empresas): Representa el 0% del total.

El análisis de las respuestas muestra que la mayoría de las empresas son diligentes en la aplicación de parches y actualizaciones de seguridad, con una porción significativa que los aplica inmediatamente cuando se liberan. Esta práctica es crucial para mantener la seguridad y la integridad de los sistemas empresariales. Las empresas que aplican actualizaciones regularmente, aunque no de manera inmediata, deberían considerar acelerar el proceso para reducir aún más el riesgo de exposición a vulnerabilidades recién descubiertas. En general, es positivo ver que ninguna empresa reporta una falta de atención a la aplicación de parches y actualizaciones de seguridad.

9. *¿La empresa maneja respaldos de información o backUps de la información crítica?*

Gráfica 9 Consolidado respuestas pregunta 9.

La distribución de respuestas muestra una variedad en la frecuencia y ubicación del almacenamiento de respaldos:

Respaldos diarios y almacenamiento en múltiples ubicaciones (2 empresas): Representa el 6.3% del total.

Respaldos semanales y almacenamiento en múltiples ubicaciones (4 empresas): Representa el 12.5% del total.

Respaldos mensuales y almacenamiento en una ubicación (23 empresas): Representa el 71.9% del total.

No realizan respaldos (3 empresas): Representa el 9.4% del total.

El análisis de las respuestas revela que, aunque la mayoría de las empresas realizan algún tipo de respaldo de información, la frecuencia y la seguridad de estos varían considerablemente. Solo una pequeña fracción de las empresas practica las mejores medidas de realizar respaldos diarios y almacenarlos en múltiples ubicaciones. La mayoría realiza respaldos mensuales y los almacena en una sola ubicación, lo que puede no ser suficiente para proteger adecuadamente los datos críticos. Es crucial que las empresas adopten prácticas más robustas y frecuentes de respaldo y almacenamiento de datos para asegurar la protección y la recuperación eficiente en caso de pérdida de datos.

10. *¿La empresa tiene un Plan de Recuperación ante Desastres?*

Gráfica 10 Consolidado respuestas pregunta 10.

La distribución de respuestas muestra una variabilidad en la existencia y prueba de los planes de recuperación ante desastres:

Documentado y probado regularmente (3 empresas): Representa el 9.4% del total.

Documentado, pero no probado regularmente (5 empresas): Representa el 15.6% del total.

No documentado (19 empresas): Representa el 59.4% del total.

Sin plan (5 empresas): Representa el 15.6% del total.

El análisis de las respuestas revela que una pequeña fracción de las empresas tiene un plan de recuperación ante desastres documentado y probado regularmente. La mayoría de las empresas tienen un plan no documentado o no probado regularmente, lo cual puede comprometer la eficacia del plan en una situación real de desastre. Además, un número significativo de empresas no tiene ningún plan de recuperación, lo que las deja muy vulnerables. Es esencial que las empresas adopten prácticas robustas para desarrollar, documentar, probar y actualizar regularmente sus planes de recuperación ante desastres para asegurar la continuidad del negocio y minimizar el impacto de posibles desastres.

11. *¿La empresa realiza simulacros y pruebas de seguridad (como simulacros de phishing)?*

Gráfica 11 Consolidado respuestas pregunta 11.

Las respuestas revelan la frecuencia y la consistencia en la realización de simulacros y pruebas de seguridad:

Al menos una vez al año (2 empresas): Representa el 5.9% del total.

Sí, pero no regularmente (3 empresas): Representa el 8.8% del total.

Ocasionalmente, sin un cronograma definido (10 empresas): Representa el 29.4% del total.

No realizamos simulacros ni pruebas de seguridad (17 empresas): Representa el 50% del total.

El análisis muestra que la mayoría de las empresas no realizan simulacros o pruebas de seguridad de manera regular o consistente. Solo una pequeña fracción de las empresas realiza simulacros al menos una vez al año, lo cual es una práctica recomendada para mantener la preparación y la conciencia de seguridad. La falta de simulacros y pruebas de seguridad puede dejar a las empresas mal preparadas para responder a amenazas reales y aumentar su vulnerabilidad a los ataques cibernéticos. Es esencial que las empresas reconozcan la importancia de los simulacros y pruebas de seguridad y los incorporen regularmente en sus prácticas de seguridad.

De acuerdo con la información obtenida mediante el análisis de la encuesta presentada en esta investigación se ha revelado que las pequeñas y medianas empresas (PYMES) en Colombia enfrentan significativos desafíos en términos de ciberresiliencia. Estos desafíos se deben principalmente a dos factores críticos: el desconocimiento del tema y la falta de inversión en los recursos necesarios.

Uno de los obstáculos que enfrentan las PYMES colombianas en su camino hacia una mayor ciberresiliencia es la falta de conocimiento adecuado sobre el tema. Muchas empresas no comprenden completamente los riesgos asociados a las amenazas cibernéticas ni las mejores prácticas para mitigarlos. Esta carencia de conocimiento abarca desde la identificación de posibles vulnerabilidades hasta la implementación de medidas de respuesta ante incidentes cibernéticos.

Otro factor determinante es la falta de inversión en ciberseguridad y ciberresiliencia. Las PYMES suelen tener recursos limitados y, en muchos casos, priorizan otras áreas de negocio antes que la seguridad informática. Esta insuficiente inversión se refleja en la ausencia de infraestructura tecnológica adecuada, la falta de personal especializado y la escasez de programas de capacitación en ciberseguridad.

La combinación de estos factores deja a las PYMES vulnerables a diversos tipos de ciberataques, desde el phishing, diferentes tipos de malware hasta los ataques de ransomware. La falta de preparación y de recursos adecuados puede llevar a consecuencias severas, incluyendo la pérdida de datos sensibles, interrupciones en las operaciones comerciales y daños reputacionales significativos.

Con esta información, se analiza cuáles son las principales amenazas que se pueden presentar y los departamentos con mayor presencia de estos.

Es crucial para este estudio identificar los diversos tipos de ataques cibernéticos a los que están expuestas las empresas pymes. Esta comprensión nos proporciona una visión más clara de las amenazas cibernéticas que estas empresas pueden enfrentar. Por lo tanto, resulta fundamental analizar los posibles ataques cibernéticos que podrían afectar su seguridad y operaciones.

Para obtener un contexto general y de macroentorno, comenzamos identificando a nivel nacional las denuncias relacionadas con delitos informáticos y analizando su comportamiento para obtener un enfoque claro. Para este propósito, utilizamos datos históricos de denuncias, mapeamos las ciberamenazas correspondientes a cada una de ellas y las representamos visualmente a través de una herramienta de Business Intelligence (BI):

BI Figura 4. panorama de ciberataques reportados en Colombia (fuente datos.gov.co).

Gracias a esta herramienta, se puede observar el ranking de las ciberamenazas y los departamentos que más registra denuncias en el país y como ha sido la tendencia a lo largo de los años.

El top5 de las ciberamenazas en este análisis son las siguientes:

Phishing: Es un intento de engañar a las personas para que revelen información personal, como contraseñas o datos financieros, a través de correos electrónicos, mensajes de texto u otros medios electrónicos.

Ransomware: Es un tipo de software malicioso que bloquea el acceso a los archivos o sistemas de una computadora y exige un rescate para desbloquearlos.

Spyware: Es un software malicioso diseñado para recopilar información sobre las actividades de un usuario en línea sin su conocimiento, como historial de navegación, contraseñas o detalles de tarjetas de crédito.

Ingeniería Social: Es una técnica que utiliza la manipulación psicológica para engañar a las personas y obtener información confidencial o acceso no autorizado a sistemas informáticos.

Malware: Es un término general que abarca todo tipo de software malicioso diseñado para dañar o infiltrarse en un sistema informático sin el consentimiento del usuario

Estas amenazas no solo impactan a las empresas grandes y multinacionales, sino también a las PYMES. Una vez se manifiestan, pueden materializarse y poner en peligro la continuidad de los negocios de estas empresas. Esto puede traducirse en la interrupción de operaciones, daños a equipos y sistemas críticos, así como pérdidas económicas significativas.

4.1 PROPUESTA

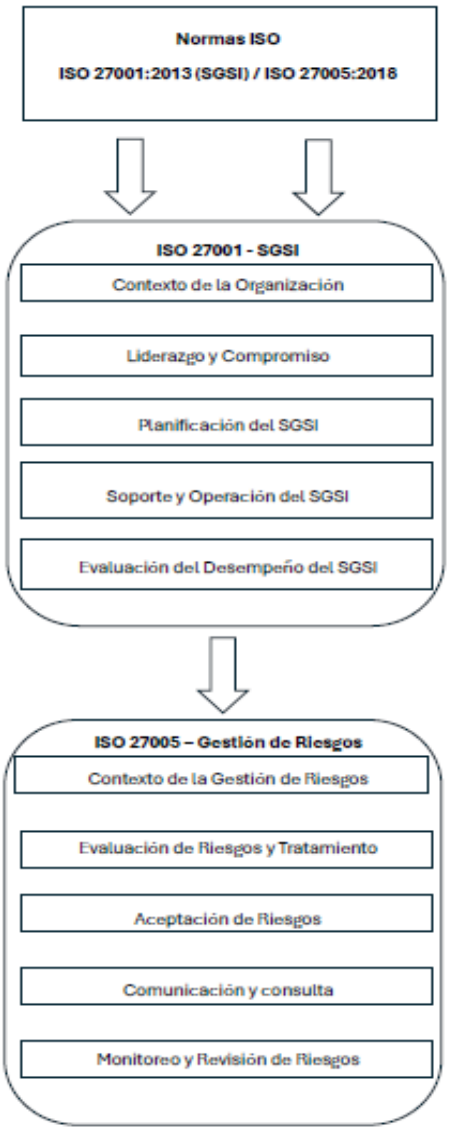


Figura 5. Metodología para Aplicar en la empresa (Imagen propia)

La ciberseguridad se ha convertido en un aspecto crítico para el funcionamiento seguro y exitoso de las empresas. Con el aumento constante de las amenazas cibernéticas, desde ataques de phishing hasta malware avanzado, es imperativo que las organizaciones implementen medidas sólidas de protección para salvaguardar sus activos digitales, la información confidencial y la confianza de sus clientes.

Esta propuesta tendrá un impacto positivo al mejorar la capacidad de respuesta y recuperación de la empresa frente a incidentes cibernéticos. Asegurará que la empresa pueda recuperarse rápidamente de cualquier incidente, minimizando así el tiempo de inactividad y los costos asociados con la interrupción de las operaciones comerciales.

Planteamos estas recomendaciones para fomentar la importancia de las buenas prácticas en ciberseguridad.

Crear Conciencia: Educar a todos los empleados sobre las amenazas cibernéticas y las mejores prácticas de seguridad para fomentar una cultura de seguridad en toda la organización.

Proteger la Infraestructura Tecnológica: Implementar medidas de seguridad robustas para proteger los sistemas, redes y dispositivos contra intrusiones y ataques maliciosos.

Gestionar el Riesgo: Identificar, evaluar y gestionar proactivamente los riesgos de seguridad cibernética para minimizar el impacto potencial de las amenazas.

Cumplir con los Requisitos Regulatorios: Garantizar el cumplimiento de las normativas y regulaciones de seguridad cibernética pertinentes para su industria y ubicación geográfica.

Componentes Clave de un Programa Integral de Seguridad Cibernética:

Capacitación en Concientización de Seguridad: Desarrollo de programas de formación en seguridad cibernética para todos los empleados, incluyendo sesiones de sensibilización, simulacros de phishing y cursos de seguridad en línea.

Implementación de Soluciones de Seguridad Tecnológica: Despliegue de firewalls avanzados, sistemas de detección de intrusiones, software antivirus actualizado y otras herramientas de seguridad para proteger los activos digitales de la empresa.

Auditorías de Seguridad Regulares: Realización de auditorías periódicas de seguridad cibernética para evaluar la eficacia de los controles de seguridad existentes, identificar

posibles vulnerabilidades y tomar medidas correctivas.

Desarrollo de Políticas y Procedimientos de Seguridad: Elaboración y aplicación de políticas y procedimientos claros en materia de seguridad cibernética, incluyendo políticas de contraseñas, acceso a datos y gestión de incidentes.

Gestión de Incidentes y Respuesta ante Emergencias: Establecimiento de un plan de respuesta a incidentes para abordar de manera eficiente y efectiva las brechas de seguridad y las amenazas cibernéticas en caso de que ocurran.

Beneficios de la Implementación de un Programa Integral de Seguridad Cibernética:

Mejora de la protección de los activos digitales y la información confidencial.

Reducción del riesgo de interrupciones operativas y pérdidas financieras debido a incidentes de seguridad cibernética.

Cumplimiento de los requisitos regulatorios y fortalecimiento de la reputación de la empresa.

Fomento de la confianza del cliente y la lealtad al demostrar un compromiso con la seguridad de los datos.

Elaboramos el siguiente esquema de ciberseguridad, donde se presenta un paso a paso a seguir con el fin de prevenir posibles vulnerabilidades y proteger los activos digitales de la empresa ante amenazas cibernéticas

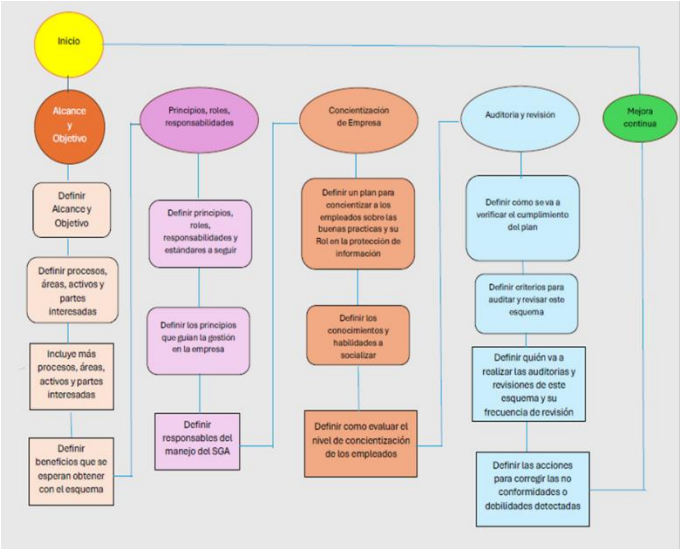


Figura 6. Esquema de ciberseguridad para PYMES en Colombia (Imagen propia) .

5. CONCLUSIONES.

Ciberresiliencia se refiere a la capacidad de una organización para prepararse, responder y recuperarse de los ciberataques y otros eventos disruptivos relacionados con la ciberseguridad. La implementación de ISO 27001 e ISO 27005 contribuye significativamente a la continuidad del negocio de las PYMES de las siguientes maneras:

Preparación: Establece políticas, procedimientos y controles que preparan a la PYME para enfrentar amenazas de seguridad de la información.

Respuesta: Define procesos claros para responder a incidentes de seguridad, minimizando el impacto en la operación de la empresa.

Recuperación: Facilita la rápida recuperación de incidentes al tener medidas de contingencia y recuperación bien definidas.

Las normas ISO 27001 y 27005 proporcionan a las PYMES un marco integral para gestionar la seguridad de la información y los riesgos asociados, lo que es esencial para mantener la ciberresiliencia en un entorno de

amenazas en constante evolución. Implementarlas no solo mejora la seguridad de la información, sino que también fortalece la capacidad de la empresa para resistir y recuperarse de incidentes cibernéticos.

Las PYMES son una parte esencial de la economía colombiana y, al ser blanco de ataques cibernéticos por su percepción como más vulnerables, la falta de preparación puede tener consecuencias devastadoras. El desconocimiento del tema y la insuficiente inversión en recursos de ciberseguridad exponen a estas empresas a riesgos significativos que pueden comprometer su continuidad operativa y reputación.

Para abordar estos desafíos, es crucial que las PYMES colombianas tomen conciencia de la importancia de la ciberresiliencia y adopten medidas proactivas. Invertir en tecnología adecuada, capacitar a su personal y desarrollar planes de respuesta a incidentes son pasos esenciales para mejorar su capacidad de recuperación ante ciberataques. La implementación de estas estrategias no solo protege a las empresas de posibles pérdidas y daños, sino que también fortalece su posición competitiva en un mercado cada vez más digitalizado.

REFERENCIAS

Mosquera Bernal, A., Fontecha Bernal, C. C., Romero Gómez, J. R., Santos Sanabria, I. A., & Pita Moreno, Z. C. (2023). *Estrategias de ciberseguridad en organizaciones en Colombia* (Bachelor's thesis, Especialización en Gerencia de Proyectos-Virtual). https://repository.universidadean.edu.co/handle/10882/12467

The Resilience Institute. (2021). Resilience Spiral. Recuperado de: https://resiliencei.com/resources/resilience-spiral/

Software Engineering Institute – CERT RMM. (s.f.). Recuperado de: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9479

Software Engineering Institute – CERT RMM, v1.1. (s.f.). Recuperado de: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9849

Noticias Caracol. (2021, 11 de julio). La historia secreta del hackeo más grave contra las fuerzas Militares de Colombia. Recuperado de: https://bit.ly/3wwpN9U

García-González, J. R., & Sánchez-Sánchez, P. A. (2020). Diseño teórico de la investigación: instrucciones metodológicas para el desarrollo de propuestas y proyectos de investigación científica. Información Tecnológica, 31(6), 159-170. https://dx.doi.org/10.4067/S0718-07642020000600159

CONPES Política Social la distribución territorial y sectorial. (2020, July 1). Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

González, A. (2020, December 30). Seguridad lógica en informática. ¿En qué consiste? Ayuda Ley Protección Datos. Recuperado de: https://ayudaleyprotecciondatos.es/2020/12/30/seguridad-logica

Pulido Pulido, T. V. La ciberseguridad es clave en el éxito empresarial. https://repository.unimilitar.edu.co/handle/10654/44244

Niño Wilches, Y. A. Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo Pymes. https://repository.unimilitar.edu.co/handle/10654/73255

Peña Montenegro, C. A. (2023). Esquema de ciberseguridad y recomendaciones para el manejo de información de PYMES en Colombia. https://fundacionlibertadores-my.sharepoint.com/personal/hmherrerah_libertadores_edu_co/_layouts/15/onedrive.aspx?FolderCTID=0x012000CE02B54500E8014C8FEF417B484DF747&id=%2Fpersonal%2Fhmherrerah%5Flibertadores%5Fedu%5Fco%2FDocuments%2FProyecto%20de%20aplicaci%C3%B3n%202024%2D1%2F3%2E%20Morera%5FOchoa%5FFarfan%2FArticulos%2F4%2EEsquema%20de%20ciberseguridad%20y%20recomendaciones%20para%20el%20manejo%20de%20informaci%C3%B3n%20de%20PYMES%20en%20Colombia%2E%2Epdf&parent=%2Fpersonal%2Fhmherrerah%5Flibertadores%5Fedu%5Fco%2FDocuments%2FProyecto%20de%20aplicaci%C3%B3n%202024%2D1%2F3%2E%20Morera%5FOchoa%5FFarfan%2FArticulos

BSI. (2022). Cybersecurity confidence for the SME. BSI Blog. Recuperado de: https://www.bsigroup.com/enGB/blog/Small-Business-Blog/cybersecurity-confidence-forthe-sme/

Ortega, O. B., & Segura, J. R. (2022). Protocolo básico de ciberseguridad para pymes. Interfases, (016), 168-186. https://revistas.ulima.edu.pe/index.php/Interfases/article/view/6021

Villayzan Chancafe, R. A., & Gutiérrez Perona, J. D. (2022). Modelo de identificación de ciberamenazas para PYMES de servicios tecnológicos usando herramientas de Data Analytics. Recuperado de: https://repositorioacademico.upc.edu.pe/handle/10757/653631

Diaz Jimenez, C. D., Ariza Rodriguez, E., & Ruiz Moncada, M. Y. (2023). *La Ciberseguridad en las Pymes* (Bachelor's thesis, Universidad EAN). https://repository.universidadean.edu.co/handle/10882/12818

Boot, A., Hoffmann, P., Laeven, L., & Ratnovski, L. (2021). Fintech: what's ol d, what's new? Journal of Financial Stability, 53. https://doi.org/10.1016/j.jfs.2020.100836

Cano, J. J., & Rocha, A. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital/Cybersecurity and cyberdefense. Challenges and perspectives in a digital world. RISTI (Revista Iberica de Sistemas e Tecnologias de Informacao), (32), vii-vii. https://go.gale.com/ps/i.do?id=GALE%7CA596318112&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=16469895&p=AONE&sw=w&userGroupName=anon%7Ebc1f7bca&aty=open-web-entry

Mandiant. (2021). M-Trends. Recuperado de: https://www.mandiant.com/resources/m-trends-202

Rea-Guaman, A. M., & Sánchez-García, I. D. (s.f.). Universidad Politécnica de Madrid ETS Ingenieros Informáticos.

Lalinde, A. O., López, G. L., Henao, L. M. A., & Méndez, T. A. (2017). Ciberseguridad y ciberdefensa: Pilares fundamentales de la seguridad y defensa nacional. *Revista de las Fuerzas Armadas*, (241), 6-14. https://esdegrevistas.edu.co/index.php/refa/article/view/823

Ranking 1000 pymes – especiales Dinero, Semana.com. https://especiales.dinero.com/ranking-1000-pymes-ganadoras/index.html