UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Propuesta metodológica para mitigar los riesgos sobre ciberataques a Pymes, usando la Metodología NIST

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Berru Escajadillo, Sergio Andre (orcid.org/0000-0002-6425-3344)

Yarleque Golles, Luis Fernando (orcid.org/0000-0001-9865-099X)

ASESORES:

Dr. Tavara Ramos, Anthony Paul (orcid.org/0000-0002-4159-930X)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Apoyo a la reducción de brechas y carencias en la educación en todos sus niveles

PIURA - PERÚ

2023

DEDICATORIA

Este proyecto universitario está destinado a nuestro creador Dios, quien es nuestra principal inspiración en la búsqueda de uno de nuestros mayores anhelos.

Queremos expresar nuestro más profundo agradecimiento a nuestros padres, cuyo amor, dedicación y sacrificio a lo largo de todos estos años nos han permitido llegar hasta este punto y convertirnos en las personas que somos hoy en día.

AGRADECIMIENTO

Le damos gracias a Dios, que sin su protección no somos nada, A nuestros padres por sus consejos y enseñanzas.

A nuestros docentes de la universidad que nos apoyaron y brindaron sus conocimientos para la elaboración de la presente investigación.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

RESUMEN

En los últimos años, se ha observado un crecimiento significativo de las pequeñas y medianas empresas (PYMES) en Perú. Sin embargo, a pesar de su tamaño reducido, estas empresas no están exentas de sufrir ataques cibernéticos, que representan la principal amenaza para las empresas, independientemente de su tamaño. Los ciberataques se han convertido en la modalidad más común utilizada para el robo de información, lo que puede generar consecuencias negativas tanto en el ámbito económico como en el de la seguridad de las PYMES.

Por esta razón, se ha desarrollado un proyecto enfocado específicamente en las PYMES, con el objetivo de proponer una metodología basada en los estándares del Instituto Nacional de Estándares y Tecnología (NIST) para mitigar los riesgos cibernéticos. En este proyecto, se llevó a cabo un análisis cuantitativo que consideró como variables de estudio los "ciberataques" y la "metodología NIST". Para recopilar los datos necesarios, se realizó una encuesta que se diseñó teniendo en cuenta los indicadores de investigación pertinentes. La información recopilada fue analizada utilizando técnicas estadísticas como la prueba de Shapiro-Wilk, lo que permitió destacar los indicadores y objetivos específicos relevantes.

Los resultados obtenidos resaltan la dependencia de la aplicación de la metodología en varios factores que influyen en las PYMES. A través de la metodología basada en NIST, se identificaron diferentes resultados relacionados con la vulnerabilidad de las PYMES, el conocimiento sobre ciberataques, la implementación de controles y los tipos de ciberataques enfrentados. Estos resultados proporcionan información valiosa para la aplicación de la metodología propuesta y para evaluar su efectividad.

Palabras clave: Cibercrimen, Seguridad de los datos, Protección de datos.

ABSTRACT

In recent years, small and medium-sized enterprises (SMEs) have been growing in Peru, reflecting the entrepreneurial spirit of its citizens. However, being small in size does not exempt these businesses from falling victim to cyberattacks. Cyberattacks pose a significant threat to companies of all sizes and have become the most commonly employed method for information theft and malicious activities. This not only results in information loss but also has detrimental financial implications for SMEs.

Therefore, this project focuses on SMEs and proposes a methodological approach based on the National Institute of Standards and Technology (NIST) framework to mitigate cyber risks. The analysis was conducted using a quantitative approach, with "Cyberattacks" and "NIST Methodology" as the variables of study. Data collection was performed through a survey, incorporating research indicators. The collected data was statistically analyzed using the Shapiro-Wilk test to highlight relevant information related to the indicators and specific objectives.

The findings underscore the importance of various factors influencing the application of the NIST-based methodology for SMEs. By applying this methodology, different outcomes were identified, such as vulnerable SMEs, knowledge of cyberattacks, implemented controls, and various types of cyberattacks. This information is crucial for the effective implementation and validation of the proposed methodology.

Keywords: Cybercrime, data security, Data Protection.

I. INTRODUCCIÓN

Es ampliamente reconocido que las pequeñas y medianas empresas (PYMES), se enfrentan diariamente a muchos de los mismos problemas de ciberseguridad que las grandes empresas, pero no tienen los recursos usuales para abordar los riesgos de forma efectiva (Horn, 2017). Estas empresas acostumbran ser proveedores, contratistas y socios de empresas mayores y permanecen conectadas digitalmente. Por consiguiente, los ciber atacantes las usan como puertas de entrada para hackear los sistemas de las organizaciones mayores (Better Business Bureau, 2017).

Un enorme número de las pymes no tienen el conocimiento del enorme problema que tienen y por el cual luchan día tras día tomando en cuenta de esta forma a la estabilidad informática como algo no primordial, por lo que no contratan al personal adecuado, ni invierten en el recurso financiero para reducir peligros de ataques cibernéticos, la cual corre el riesgo de que esa información robada pueda ser destruida o vendida a la competencia.

La amenaza que más perjudica a la estabilidad de la información de una pyme es su carencia de conocimiento, la confiabilidad hacia ella, la totalidad y los recursos de información que disponen son inadecuados. Por lo que deja a las pymes con muchos problemas, como es el retraso del progreso operacional diario, el cual tiene como resultado una pérdida de ingresos monetarios y retrasos de tiempo que no son esperados en producción.

En el presente, existen múltiples elementos que amenazan la estabilidad de las PYMES al comprometer su información. Con frecuencia, los recursos destinados a salvaguardar y resguardar los datos en las redes externas de internet resultan insuficientes para detectar y gestionar de manera adecuada las debilidades existentes en la seguridad interna de la red.

Los atacantes han estado evolucionando rápidamente en sus métodos, a diferencia de la metodología de defensa que se ha quedado rezagada en su desarrollo. Esto se destaca en el Estudio de Referencia de las Capacidades de Seguridad de Cisco 2018. (CISCO, 2018) determina el valor de considerar la exploración y explotación de las vulnerabilidades y debilidades en las IoT(Internet Of The Things), el cual

permite obtener el ingreso a los sistemas de control, y pocas empresas y/o compañías ven esto como una amenaza.

Una pequeña y mediana empresa conocidas como PYMES, tienen una debilidad creciente de ciberataques, tomando en cuenta lo difícil que es proteger sus sistemas, datos sensibles y confidenciales es mucho mayor a comparación de las empresas grandes por la carencia de recursos, todas las empresas tienen importancia, no solo las grandes empresas o corporaciones, es hora de comenzar a tomar conciencia de eso y aplicar la ciberseguridad entre socios, clientes y proveedores.

Esta información contiene distintos capítulos, entre ellos está el primero que es el marco teórico, en el que se encontrara un conjunto de antecedentes y conceptos por autores. En segundo, la metodología aplicada, que contiene las variables, materiales y métodos que fueron utilizados para la elaboración de esta investigación. En tercero tenemos los aspectos administrativos, que se ha usado para desarrollar la tesis.

Para mitigar estos riesgos de ciberataques, no necesariamente se tiene que implementar una solución que se tenga que invertir grandes cantidades de dinero, unas de las opciones factibles es aplicar controles de seguridad basados en técnicas o metodologías, también como planes de seguridad informática, esto se puede aplicar mediante responsabilidades y pasos que pueden seguir los miembros que conforman la pyme, con el fin de resguardar los datos. Es por esto que esta investigación resulta fundamental para que las pymes conozcan el valor de proteger su información, usando la metodología Nist.

Ante la situación mencionada, se detectó el problema y se planteó la siguiente pregunta de investigación ¿De qué manera los riesgos de ciberataques a pymes se mitigan usando una metodología basada en Nist?

Se estableció como objetivo general del presente proyecto de investigación: Aplicar una propuesta para mitigar los riesgos que generan los ciberataques en las pymes. Como objetivos específicos se determinaron: Identificar los distintos tipos de ciberataques a las pymes, Clasificar los distintos ataques con mayor impacto a pymes y Mitigar riesgos asociados a los ciberataques.

El proyecto de investigación presenta la siguiente hipótesis: Los riesgos de ciberataques a PYMES son mitigados usando la metodología basada en NIST.

II. MARCO TEÓRICO

La presente investigación tiene como fin definir características relevantes del tema a investigar. Se llevó a cabo una investigación minuciosa que incluyó el análisis de una amplia variedad de antecedentes publicados a nivel internacional, nacional y local. La revisión de artículos permitió la identificación de enfoques previos y diferentes perspectivas en torno al tema, lo que, a su vez, posibilitó la generación de nuevas ideas. Este análisis de los artículos nos proporcionó una base sólida para abordar el problema y desarrollar soluciones efectivas.

Ciberataques a pymes, Según Michael Benz y Dave Chatterjee en su artículo ¿Riesgo calculado? Una herramienta de evaluación de la ciberseguridad para las PYMES (2020). Las pequeñas y medianas empresas (PYMES) han experimentado una demora en la adopción de tecnología y medidas adecuadas de seguridad para gestionar eficazmente los riesgos a los que se enfrentan. Es crucial que no subestimen la importancia de estar preparados en temas de ciberseguridad, ya que esto puede determinar su capacidad para sobrevivir y mantenerse a flote en el entorno digital actual. En consecuencia, las PYMES no pueden darse el lujo de ignorar este problema y deben tomar medidas proactivas para proteger sus sistemas y activos digitales.

Según Shekhar Pawar DBA Dr. Hemant Palivela en su artículo, LCCI: Un esquema básico de medidas de seguridad cibernética para las pequeñas y medianas empresas (PYMEs) (2022) se ha desarrollado con el objetivo de reducir el peligro de ser víctimas de ataques informáticos, es crucial que se implementen recomendaciones de ciberseguridad específicas y escalonadas. Es importante que estas recomendaciones sean adecuadas para las necesidades y capacidades de cada empresa, ya que esto puede mejorar significativamente su capacidad para detectar, prevenir y responder a posibles amenazas. En consecuencia, es fundamental que las PYMEs adopten un enfoque proactivo hacia la ciberseguridad y estén al tanto de las recomendaciones y mejores prácticas disponibles para garantizar la protección de sus activos digitales.

Según Villayzan Chancafe y Renzo Adrian en su tesis titulada Modelo de identificación de ciberamenazas para PYMES de servicios tecnológicos, el propósito de este proyecto consiste en mejorar la capacidad de detección de amenazas cibernéticas en empresas de menor tamaño que operan en el sector de servicios tecnológicos. En los entornos de estas organizaciones, existen amenazas que pueden pasar desapercibidas para las alternativas de seguridad convencionales, como los softwares de protección contra virus. El objetivo principal de este proyecto consiste en desarrollar un modelo de análisis de registros de actividad (logs) que sea capaz de identificar estas amenazas cibernéticas. Para lograrlo, se emplearán herramientas de análisis de datos (Data Analytics) especialmente diseñadas para satisfacer las exigencias específicas de las PYMES del ámbito de los servicios tecnológicos. De acuerdo con una investigación llevada a cabo por el Instituto Ponemon en 2018, se reveló que el 82% de las empresas encuestadas informaron que las soluciones antivirus no fueron efectivas en la detección de exploits maliciosos.

Mejorando la gestión de tecnología de la información mediante un modelo de ciberseguridad en un Instituto Superior Tecnológico público, Lima - 2021" Manrique, Victor (2022). El objetivo fundamental de esta investigación fue presentar un enfoque innovador de ciberseguridad que contribuya significativamente a la mejora de la administración de tecnología de la información en un instituto superior tecnológico de naturaleza pública. Con este fin, se realizó un estudio aplicado basado en un enfoque de investigación-acción. Como resultado de la investigación, se recomienda realizar evaluaciones periódicas de riesgos para identificar las vulnerabilidades de los activos en la red y así mitigar las amenazas. Asimismo, se sugiere llevar a cabo capacitaciones en ciberseguridad con el objetivo de reducir las brechas en los ataques de ingeniería social, dado que los usuarios desempeñan un papel crucial en la protección de la información. Según (Grinblatt, 2002), Se basa en evaluar y gestionar, gracias a instrumentos financieros, seguro y mecanismos el nivel de exposición de la compañía a diversas fuentes de peligro.

Alguna de las condiciones de peligro que tienen la posibilidad de exponer dentro del ámbito de trabajo tienen la posibilidad de o no estar atribuidas a: prácticas incompletas de la dirección, carencia de sistemas de competidores externos.

Mientras tanto que uno de los componentes internos dentro del plan podría ser: Planeación excesivamente optimista, diseño no adecuado, elaboración de una interfaz no adecuada, diseño bastante complicado. Por consiguiente, es necesario de un grupo de ocupaciones estratégicas, de ocupaciones de prevenir y de recuperar en caso de una emergencia y que algún peligro aparezca en un rato definido. Es por esto que para consumar los metas planteados dentro del plan se necesita disponer de la ayuda tanto económico, técnico como humano en la compañía, para así maximizar las maneras de triunfo y reducir todos los componentes que logren incidir de forma negativas en las metas de los proyectos apalancados por las organizaciones creadoras de fábricas. (McConnell, 2002).

Ciberataques, según (Nahun Frett, 2015), Son sucesos en los que se realizan agravios, perjuicios o males en oposición a los individuos o conjuntos de ellas, entidades o instituciones y que en la mayoría de los casos son ejecutados mediante pcs y por medio de la Internet. No precisamente tienen la posibilidad de ser realizados plenamente por dichos medios, sino además desde los mismos. Puede dirigirse tanto a los grupos y sistemas de computación que operan en la red a nivel global, como a la información almacenada en bases de datos. Al ser dirigidos a los conjuntos y sistemas, tienen la posibilidad de averiguar la abolición del servicio que éstos prestan, de una forma temporal o persistente. Los ataques que se ejecutan contra los datos, por su lado, tienen la posibilidad de ir a partir del hurto de los mismos con fines militares o comerciales.

Algunos tipos de ciberataques son: Los virus informáticos: son programas maliciosos diseñados con el propósito de infectar otros archivos dentro del sistema, causando alteraciones en la información o daños en el sistema informático afectado. Estos virus introducen secuencias de código malicioso que se dirigen específicamente a los archivos ejecutables del sistema objetivo. (Norton LifeLock, 2021), El correo no deseado: también conocido como SPAM, se refiere al envío masivo de mensajes no solicitados, los cuales provienen de remitentes desconocidos y suelen contener publicidad con la intención de perjudicar al receptor. A este tipo de acción se le denomina spamming. (Francisco J. Urueña Centeno, 2015), Spoofing: Se trata de un método en el que el atacante oculta su identidad durante un ataque, con el objetivo de obtener acceso a recursos en otro

sistema que ha depositado cierta confianza en la dirección IP del host suplantado. Este tipo de ataque sigue representando una amenaza potencialmente peligrosa para organizaciones de cualquier índole. (Cisco, 2021), Keyloggers: Los keyloggers son ataques maliciosos utilizados para registrar y grabar las pulsaciones de teclas con el propósito de almacenarlas en un archivo y enviarlas a través de Internet. Su objetivo es obtener información privada y confidencial de las víctimas. (Francisco J. Urueña Centeno, 2015), Utilización de troyanos para el robo de información: Los troyanos informáticos son ataques que se distinguen por engañar a los usuarios al hacerse pasar por programas comunes de uso diario, como correos electrónicos, imágenes o fotos. Su objetivo es robar información personal y valiosa. Algunos ejemplos de estos troyanos son Back Orifice 2000, SubSeven, Cybersensor, entre otros. (Francisco J. Urueña Centeno, 2015), Rootkits: Los rootkits son un conjunto de herramientas utilizadas en ataques cibernéticos que logran ocultar un acceso no autorizado a un sistema informático. Su propósito es ocultar archivos y procesos que permiten al atacante mantener el control del sistema. Estos ataques están diseñados para pasar desapercibidos, lo que los hace difíciles de detectar. (Francisco J. Urueña Centeno, 2015).

Metodología Nist, Según Fernando Rocha Moreira, Demétrio Antonio Da Silva Filho, Georges Daniel Amvame Nze, Rafael Timóteo De Sousa Júnior y Rafael Rabelo Nunes en su artículo, Evaluación del desempeño de los controles de seguridad cibernética del marco del NIST a través de una metodología constructivista de criterios múltiples 2021, El Marco de mejora de la seguridad cibernética de la infraestructura crítica desarrollado por la metodologia NIST tiene como objetivo asistir a los operadores de infraestructuras críticas en la identificación y desarrollo de directrices para la gestión del riesgo de seguridad cibernética. Este marco se compone de un conjunto de supuestos, actividades, resultados y referencias informativas sobre ciberseguridad presentadas en diversos escenarios de infraestructuras críticas. La implementación de este marco puede ayudar a mejorar significativamente la capacidad de las organizaciones para proteger sus activos críticos y reducir la exposición a posibles amenazas cibernéticas. En consecuencia, es fundamental que los operadores de infraestructuras críticas estén

al tanto del marco y lo implementen de manera efectiva para mejorar su postura de seguridad cibernética.

La metodología NIST, Se fundamenta en 3 pasos: evaluación del peligro, estudio y evaluación de solución; la metodología podría ser aplicable a la evaluación de sistemas (Arias & LLanos, 2012).

Recomienda un grupo de sugerencias y ocupaciones para una idónea administración de peligros como parte de la administración de la estabilidad de la información; no obstante, esto no es idóneo, puesto que resulta indispensable contar con el respaldo y colaboración de todos los miembros de la organización. y así las metas y alcance de la administración de peligros terminen exitosamente (Avalos Serrano, 2007).

Es fundamental que las organizaciones tengan en cuenta esta metodología para proteger su información, debido a que actualmente es la que más trascendencia tiene, inclusive tenemos la posibilidad de nombrar que la organización no solo debería proteger su capital, sino también la información como un bien de la compañía por esa razón debería ser completa la información, disponible para los individuos correctos y lo más relevante confidencial. (Roxana & Yesenia, 2013).

La metodología que se presenta consta de nueve pasos para la exploración de peligros, según lo descrito por Arias y Llanos en 2012. El primer paso es la caracterización del sistema, que establece el alcance del ejercicio de evaluación del peligro y proporciona información sustancial para conceptualizar el peligro. El segundo paso es la identificación de amenazas, donde se identifican las amenazas con mayor impacto que podrían explotar las vulnerabilidades del sistema y se clasifican en tres categorías: humana, natural y ambiental. El tercer paso es la identificación de vulnerabilidades, mientras que el cuarto es el estudio de los controles existentes. En el quinto paso, se toma la decisión de probabilidades, y en el sexto, se realiza un estudio de efecto. El séptimo paso es la decisión del peligro, seguido de sugerencias de control en el octavo paso. El último paso es documentar los resultados de todo el proceso de evaluación del peligro.

Esta metodología tiene la ventaja de permitir la determinación del grado de amenaza con mayor impacto y sus peligros asociados con un sistema de tecnología de información y comunicación (TIC). Además, el proceso de evaluación del peligro ayuda a resolver los distintos componentes de vulnerabilidad y mejora la estabilidad de los sistemas. Sin embargo, una posible desventaja es que, al ser una metodología robusta, puede resultar restrictiva en su aplicación en organizaciones con altas restricciones de personal, tal como señalaron Arias y Llanos en 2012.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1 Tipo de investigación

El proyecto de investigación en consideración se encuentra dentro de la categoría de investigación aplicada, dado que su propósito radica en la generación de conocimiento mediante la implementación directa de soluciones a los desafíos que la sociedad enfrenta en la actualidad.

La investigación aplicada se caracteriza por utilizar métodos específicos, como la investigación básica, para abordar problemas prácticos y lograr avances tecnológicos en diversos campos, como la ingeniería, la biotecnología, las ciencias sociales y la salud mental. (García 2018)

3.1.2 Diseño de investigación.

El enfoque utilizado para obtener la información necesaria para el análisis se clasifica como no experimental, ya que implica realizar estudios sin la manipulación intencional de variables. En este caso, se observan los eventos o sucesos en la realidad para su posterior estudio y análisis.

3.2. Variables y operacionalización

Variable 1: Ciberataques a pymes.

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición
Ciberataques a pymes	La acción consiste en	La información			Ordinal

	fomentar la implementación de regulaciones relacionadas con la protección de infraestructuras críticas, así como promover el desarrollo de habilidades básicas para garantizar la seguridad de los servicios esenciales. (Presidencia del gobierno de España, 2013)	se recopila utilizando distintas técnicas e instrumentos de recolección de datos, como encuestas y análisis de antecedentes sobre la frecuencia de ataques cibernéticos en años anteriores.	Nivel de Ciberseguridad	Nivel de afectación	
				Vulnerabilidades detectadas	
				Vulnerabilidades tratadas	
				Conocimiento	

Variable 2: Metodología NIST.

Variable	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición

Metodología Nist	Es fundamental que las organizaciones tengan en cuenta esta metodología para proteger su información, debido a que actualmente es la que más trascendencia tiene, inclusive tenemos la posibilidad de nombrar que la organización no solo debería proteger su capital, sino también la información como un bien de la compañía por esa razón debería ser completa la información, disponible para los individuos correctos y lo más relevante confidencial.	Este marco de ciberseguridad consta de 5 funciones: 1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar	Rendimiento	Controles aplicados	Razón /continua

	(Roxana & Yesenia, 2013).				

3.3. Población, muestra y muestreo

3.1.1 Población

Según Villasís (2016), La población de estudio se refiere a un conjunto particular de casos que está claramente delimitado, accesible y se utiliza como base para la selección de nuestra muestra. Esta población satisface una serie de criterios previamente establecidos y no se limita exclusivamente a seres humanos, sino que puede abarcar también animales, familias, objetos y otros ejemplos afines.

Para esta investigación, se tomó una población de 5 pymes de la ciudad de Piura, con 8 integrantes por cada PYME seleccionada, lo que resulta en un total de 40 encuestados. Estos integrantes fueron seleccionados de diferentes áreas dentro de las PYMES, como gerentes, empleados de TI, personal de recursos humanos, etc. Se incluyen PYMES que han sido víctimas de vulnerabilidades y ataques cibernéticos, que carecen de conocimiento de ciberseguridad o de áreas de TI.

Tabla 1. Detalles de la Población de las Pymes en Piura

POBLACIÓN	CANTIDAD
PYMES	5
TOTAL	5

Acotación: Elaborado por autor

3.1.2 Muestra

Según Hernández (2018), Una muestra es una parte o subconjunto de la población o universo que es objeto de interés en nuestra investigación. En esta muestra, se recolectan los datos relevantes, y es crucial que la muestra sea representativa de toda la población. En el contexto de este proyecto de investigación, la muestra consiste en una única PYME que fue seleccionada a través de una encuesta como aquella con el mayor riesgo y vulnerabilidades. Se ha tenido en cuenta un margen de error aceptable del 5% y un nivel de confianza del 95%.

Tabla 2. Detalle de la muestra poblacional

POBLACIÓN	CANTIDAD
PYME VULNERABLE	1
TOTAL	1

Acotación: Elaborado por autor con instrumento aplicado.

3.1.3 Muestreo

Se aplicó el muestreo teórico por lo que es un tipo seleccionado de manera intencional y no aleatorio, conforme menciona Yin, R. K. (2018). Que este tipo corresponde que la muestra poblacional en el que los involucrados han sido seleccionados de manera específica que son relevantes para la investigación, por lo que en este caso se han buscado PYMES, que han sido vulnerables ante ciberataques, y que se puede aplicar una metodología basada en NIST para mitigar estos riesgos, Las PYMES han sido seleccionadas de manera intencional, por lo que se busca examinar el efecto de la metodología en la mitigación de riesgos.

3.4. Técnicas e instrumentos de recolección de datos

Los instrumentos de recopilación de información utilizados en el estudio nos posibilitaron identificar la naturaleza y las características del problema, así como establecer los objetivos de la investigación.

Se utilizó la técnica de la encuesta, en la cual se puede recoger información a través de un cuestionario, permitiendo la recolección de información en relación de las variables en estudio. (Cubas, 2022)

Se empleó el cuestionario como instrumento para la recolección de datos, en función que se trata de un conjunto de preguntas que ofrecen alternativas de respuestas y permiten obtener información sobre las variables de estudio y así recopilar datos necesarios para el cumplimiento de la investigación.

En el presente estudio, se empleó un cuestionario validado mediante el juicio de expertos (consultar Anexo 3). Este cuestionario se utilizó para recopilar datos sobre las vulnerabilidades y el control de seguridad en las PYMES. El cuestionario empleó una escala de respuesta similar a la escala de Likert, que proporcionó diversas opciones de respuesta en relación con la afirmación evaluada. A continuación, se muestra la Tabla 1, que representa el instrumento utilizado para recopilar los datos mediante esta técnica.

Tabla 3. Tabla Muestreo

Variable de estudio	**Técnica**	**Ítems**	**Instrumento**
PYMES VULNERALES	Encuesta	5	Cuestionario

3.5. Procedimientos

En un primer momento, se definió la estrategia de recopilación de datos para obtener información detallada sobre los diversos tipos de ataques sufridos por las pequeñas y medianas empresas (PYMES) en los últimos

años. Se utilizó una combinación de antecedentes y encuestas para recabar los datos necesarios relacionados con cada variable de estudio, con ayuda de la encuesta pudimos determinar que PYME es vulnerable ante ciberataques, con la cual cumple esos requisitos para aplicar la propuesta.

Tabla 4. Pyme y método elegido.

PYME ELEGIDA	METODO
Think Solutions	Metodología NIST

Tras la selección de la pequeña y mediana empresa (pyme), se decidió llevar a cabo una simulación exhaustiva de un ataque cibernético.

Enviar ciberataque a víctima

Una vez se ha creado el código malicioso, es necesario enviarlo a la víctima u organización con el propósito de ejecutar una acción perjudicial, como el robo de credenciales o el ransomware, entre otros. En este caso, se optó por emplear la técnica conocida como "Phishing de correo electrónico", tal como se describe en un artículo sobre seguridad de Microsoft. De acuerdo con Microsoft, este tipo de ataque phishing utiliza estrategias como enlaces engañosos para atraer a los destinatarios de correos electrónicos y convencerlos de que compartan su información personal. Los atacantes suelen suplantar la identidad de reconocidos proveedores de servicios, como Microsoft o Google, e incluso pueden hacerse pasar por un compañero de trabajo. Cabe mencionar que estas pruebas se llevaron a cabo en un entorno simulado y controlado con fines educativos.

Abrir phishing email

Cuando la persona receptora del correo electrónico lo abre, no recibe ninguna advertencia y continúa con sus acciones sin realizar una verificación minuciosa. Como resultado, la persona hace clic en el enlace que le han enviado.

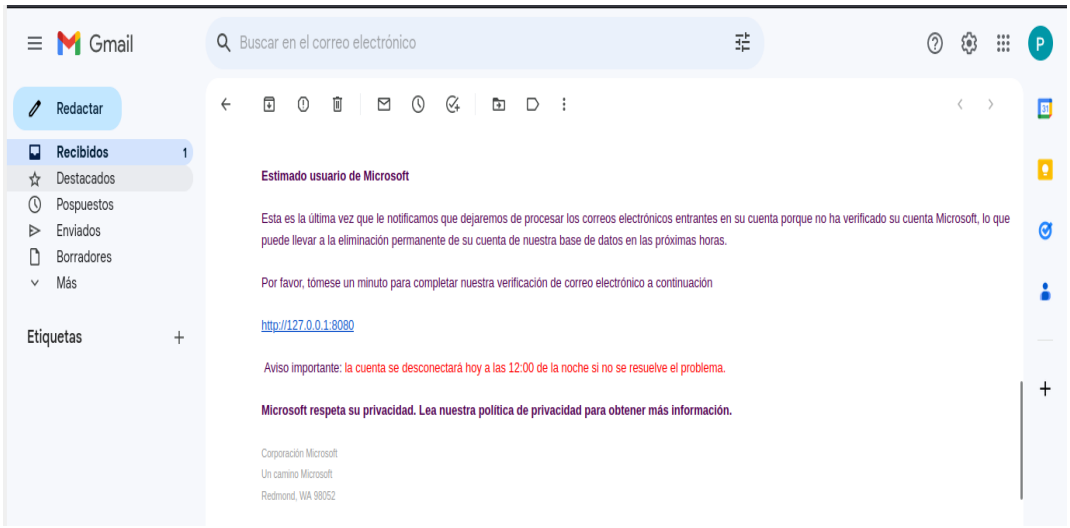

Ilustración 1. Correo electrónico recibido por el usuario

Abrir enlace y rellenar datos

Después de que el usuario accede al enlace, es redirigido a una réplica de la página de inicio de sesión de Microsoft, diseñada para obtener sus credenciales. Una vez que el usuario ingresa sus datos, se muestra un mensaje indicando que la contraseña es incorrecta y luego se le redirige a la página oficial de Microsoft. Durante este intervalo, el atacante ya ha obtenido las credenciales del usuario.

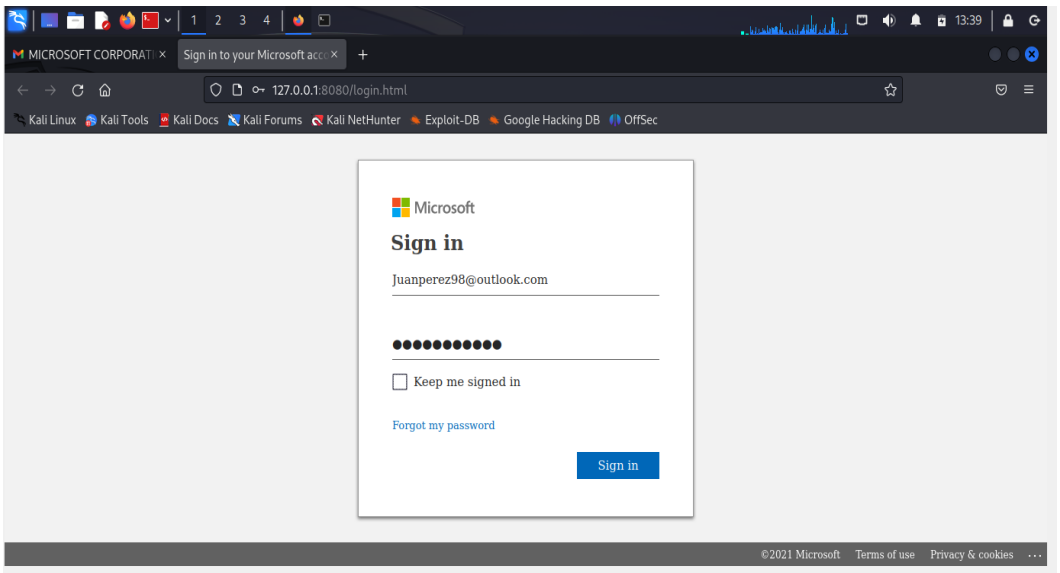

Ilustración 2. Método usado para obligar al usuario que ingrese sus datos

Por último, una vez que el usuario haya ingresado sus datos, se recopilará toda la información de sus credenciales con el propósito de llevar a cabo manipulaciones malintencionadas (como obtener acceso a su correo, contraseña, dirección IP, entre otros).

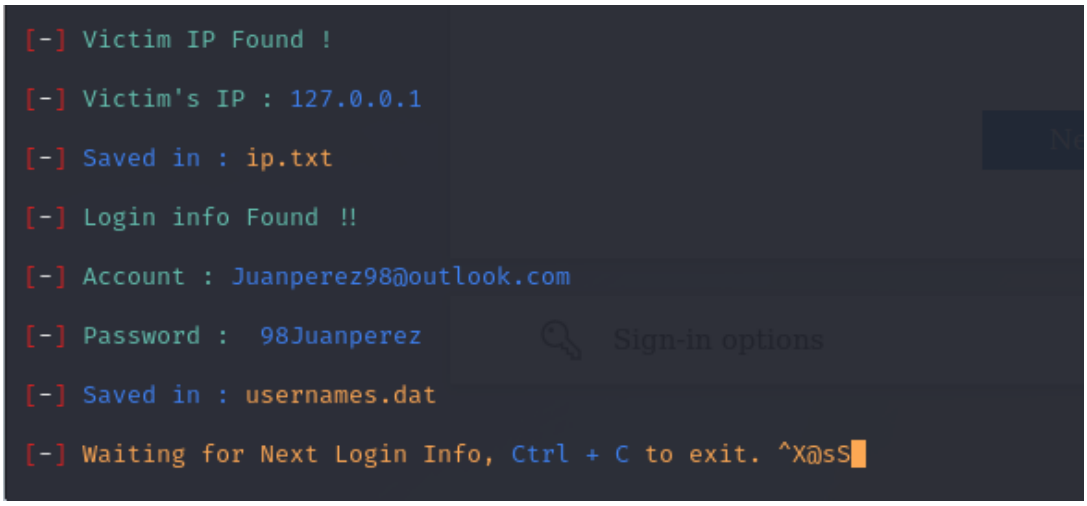

Ilustración 3. Visor de información

A continuación, se realizó la selección de la metodología, la cual se basó en el enfoque de investigación aplicada y en el diseño de investigación no experimental. Esta elección se hizo con el propósito de obtener información relevante que permitiera comprender el potencial impacto de la investigación en cuestión.

Posteriormente, se optó por implementar la Metodología NIST con el fin de mitigar los riesgos identificados. Esta metodología proporcionó una propuesta de pasos concretos para que las PYMES pudieran reducir los riesgos asociados con los ciberataques.

Metodología NIST

El marco de trabajo propuesto, se ha basado en una propuesta metodológica para mitigar los riesgos sobre ciberataques a PYMES. A continuación, se presenta una síntesis donde mostrara los esquemas de fases o etapas.

El marco de trabajo NIST consta de cuatro etapas. La primera etapa es la identificación, la segunda etapa es la protección, la tercera etapa es la detección y la cuarta y última etapa es la respuesta y recuperación.

IDENTIFICAR:

Para esta primera etapa, es fundamental que las pequeñas y medianas empresas consideren la importancia de que el responsable de ciberseguridad conozca a fondo su organización, su actividad empresarial, sus metas y su estrategia.

a. Evaluación integral de la empresa

Una vez que se haya comprendido lo mencionado previamente, resulta necesario llevar a cabo un examen PEST (Político, Económico, Social y Tecnológico), el cual es una herramienta empleada para evaluar el contexto externo de una empresa o industria. Dicho análisis posibilita identificar las condiciones ambientales que requieren la implementación de la administración de ciberseguridad en la organización. La elección de esta técnica se fundamenta en su capacidad para brindar una perspectiva global del entorno y los factores fundamentales que influyen en la ciberseguridad.

Tabla 5. Analisis PEST

POLITICO	ECONOMICO
Políticas gubernamentales en el sector tecnológico, Políticas de apoyo a la innovación y Estabilidad política.	Tendencias económicas, Presupuesto de los consumidores y Acceso a financiamiento.
SOCIAL	TECNOLOGICO
Tendencias de consumo, Cambios demográficos y Conciencia ambiental	Avances tecnológicos, Infraestructura tecnológica y Ciberseguridad

Fuente: Elaboración propia

Análisis Político:

Se refiere a la evaluación de los factores políticos que pueden influir en el entorno externo de la organización. Se centra en examinar las políticas gubernamentales, regulaciones y eventos políticos que pueden tener un impacto en el negocio.

Implica considerar las leyes y regulaciones relacionadas con la industria en la que opera la organización, como las normativas de protección de datos, ciberseguridad, propiedad intelectual o comercio electrónico. Además, incluye la evaluación de las políticas gubernamentales que afectan directamente al sector tecnológico, como la promoción de la innovación, el apoyo a los startups o la inversión en infraestructura tecnológica.

Análisis Económico:

Se refiere a la evaluación de los factores económicos que pueden impactar en el entorno externo de la organización. Se centra en examinar las condiciones económicas generales y su influencia en el negocio.

Implica tener en consideración diversos aspectos, como el crecimiento económico, las tasas de interés, la inflación, el desempleo y la disponibilidad de crédito. Estos factores pueden tener un efecto significativo en la demanda de productos y servicios de tecnología, así como en la capacidad de las Pymes para acceder a financiamiento y llevar a cabo operaciones comerciales.

Análisis Social:

Se refiere a la evaluación de los factores sociales que pueden impactar en el entorno externo de la organización.

Implica considerar diversos aspectos, como las tendencias de consumo, los cambios demográficos y las preferencias sociales. Se busca comprender cómo las características de la sociedad pueden influir en la demanda de productos y servicios de tecnología, así como en las expectativas y preferencias de los consumidores.

Análisis tecnológico:

Se refiere a la evaluación de los factores tecnológicos que pueden impactar en el entorno externo de la organización. Se centra en examinar las innovaciones tecnológicas y los cambios en la infraestructura tecnológica que pueden influir en el negocio.

Implica considerar diversos aspectos, como los avances tecnológicos, las tendencias de la industria y la disponibilidad de infraestructura tecnológica. Se busca comprender cómo las nuevas tecnologías pueden influir en el mercado y en la forma en que se desarrollan, producen y comercializan los productos y servicios de tecnología.

b. Identificación Partes interesadas

Existen diversas partes interesadas involucradas. Los clientes, quienes son fundamentales para el éxito y desarrollo de la empresa, ya que son aquellos que adquieren sus productos o servicios. Los empleados, por su parte, desempeñan un rol crucial en el funcionamiento interno de la organización, aportando su trabajo y conocimientos para alcanzar los objetivos establecidos. Asimismo, los proveedores de tecnología también forman parte de las partes interesadas, ya que suministran los recursos tecnológicos necesarios para la operación eficiente de la empresa. Los socios comerciales, por otro lado, representan colaboradores estratégicos que contribuyen a la expansión y crecimiento del negocio mediante alianzas y acuerdos comerciales. Además, no podemos dejar de mencionar a los competidores, quienes desempeñan un papel relevante en el mercado al ofrecer productos o servicios similares, generando una competencia que impulsa a la empresa a mejorar y diferenciarse. Por último, los usuarios finales, es decir, aquellos que utilizan los productos o servicios ofrecidos por la empresa, también son partes interesadas importantes, ya que su satisfacción y fidelidad son clave para el éxito a largo plazo.

Debe tenerse en cuenta los siguientes puntos:

Identificar requerimientos:

Identificar los requisitos y las expectativas de todas las partes interesadas implica reconocer las necesidades y deseos que pueden ser expresados de manera directa o indirecta. Por ejemplo, establecer un límite máximo de inversión para la ciberseguridad.

Validar los requerimientos:

Evaluar las necesidades de seguridad implica analizar si las medidas existentes satisfacen las preocupaciones, intereses y situaciones reales de la organización.

Realizar una evaluación y revisión de los procedimientos actuales para comprobar si las expectativas y enfoques de trabajo están correctos o no.

Identificar roles

Establecer las expectativas, nivel de participación y apoyo esperados de cada parte interesada.

Elaborar un programa de actividades para los grupos fundamentado en un horario colaborativo que facilite el progreso en la ejecución de una estrategia metodológica, sin interferir con las labores individuales de cada equipo.

Este análisis nos permitió contar con los primeros resultados:

Determinar las particularidades de los factores internos y externos que impactan en la administración de riesgos, lo cual abarca la misión y visión de la entidad, los actores y/o partes interesadas clave involucrados, así como la estructura organizativa interna.

c. Identificar procesos clave

Es importante que el que lidere esta propuesta sea el gerente

Es esencial que la organización tenga un pleno entendimiento de la diversidad de productos y servicios que ofrece, ya que esto puede exponerla a distintos tipos de riesgos operativos, tecnológicos, crediticios y legales, dependiendo de su modelo de negocio. Además, es crucial que

el líder del proyecto posea un profundo conocimiento de los procesos operativos que respaldan el negocio, ya que la ejecución de dichos procesos puede exponer a la organización a riesgos de ciberseguridad. En consecuencia, el responsable de esta labor debe examinar y comprender la naturaleza de dichos procedimientos, además de detectar los riesgos directos e indirectos a los que la organización se expone durante la ejecución de sus actividades.

Con toda la información brindada, es de vital importancia que realicen una buena identificación de sus activos de información, de manera de que los responsables deben priorizar: Identificar de forma precisa los propietarios de los activos, identificar de manera precisa los sitios en los que se lleva a cabo el procesamiento, almacenamiento y transporte de los recursos a través de los sistemas de información, y establecer el nivel de importancia que la empresa otorga a los recursos evaluados, ya sea en valores absolutos o comparativos.

d. Infraestructura

Como NIST nos indica, la infraestructura debe estar bien identificada, documentada, valorada.

Tabla 6. Infraestructura

CATEGORIA	CONCEPTO	DESCRIPCIÓN
HW	Componentes físicos y tangibles de los equipos de TI	Laptops, computadoras, impresoras, etc.
SW	Programas, aplicaciones y sistemas informáticos intangibles	Sistema operativo, Programas de ofimática, etc.
LUGAR	En donde se realizan las operaciones	Oficinas

RED	Equipos de telecomunicaciones	Cables de red, interruptores.

Fuente: Elaboración propia

Objetivos

Debemos analizar los siguientes factores para determinar los objetivos.

Revisión de eventos de riesgo pasados dentro de la organización y análisis de su tendencia a lo largo del tiempo, Estudio de los aumentos en costos y pérdidas derivados de eventos anteriores, Evaluación del desempeño de proyectos previos de seguridad de la información, teniendo en cuenta tanto los logros como los fracasos, Consideración de los resultados de auditorías internas y externas que hayan identificado vulnerabilidades en la seguridad y Evaluación de la cultura y nivel de conciencia de la organización en relación con la ciberseguridad y la protección de la información.

Además del análisis previo, es importante plantear tres preguntas fundamentales al equipo encargado de implementar esta propuesta. Estas tienen como objetivo identificar el valor que esta propuesta aportará a la organización ¿El enfoque en la ciberseguridad puede ayudar a mitigar o prevenir vulnerabilidades? ¿La adopción de medidas de seguridad cibernética puede mejorar la efectividad en la administración de la seguridad de la información? ¿La implementación de esta iniciativa puede generar beneficios competitivos para la empresa?.

Después de analizar los factores y plantear las tres preguntas mencionadas, es importante comenzar a formular los objetivos. Estos objetivos deben abarcar diferentes aspectos necesarios para la exitosa implementación de la propuesta en la organización. A continuación, se presentan algunos ejemplos de objetivos que pueden servir como orientación:

Establecer el grado de riesgo intrínseco de la organización.

Crear métricas de seguridad cibernética: Medir los costos asociados a incidentes de seguridad cibernética, Evaluar el tiempo de inactividad

causado por incidentes de ciberseguridad y Supervisar la obsolescencia tecnológica, como bases de datos y sistemas operativos que se encuentren sin soporte.

Implementar procedimientos y controles operativos que respalden las directrices de trabajo establecidas.

Llevar a cabo un programa integral de capacitación y fomento de una cultura de ciberseguridad en la organización.

Establecer planes de respuesta para abordar situaciones de emergencia y crisis.

Presupuesto:

La implementación de esta propuesta requiere recursos y presupuesto, por lo tanto, es importante tener en cuenta los siguientes aspectos:

Costo de los empleados:

Además de las tareas diarias, es necesario considerar que la planificación y la implementación de una propuesta metodológica para mitigar los riesgos sobre ciberataques a PYMES requiere tiempo por parte de los empleados. Esto incluye la participación en capacitaciones, la elaboración de documentos, la definición de procesos, normas y controles.

Instalación de equipos, sistemas de tecnología de información, entre otros:

Es crucial que la organización reconozca la importancia de invertir en nuevas tecnologías y herramientas para supervisar y prevenir los riesgos a los que está expuesta. Una inversión clave es la adopción de soluciones de recuperación de desastres, la cual a menudo se pasa por alto en las primeras etapas de planificación de muchas organizaciones. Un plan de recuperación

de desastres implica el uso de herramientas que aseguran la disponibilidad de datos y tecnología tanto en el entorno principal de servidores como en un centro secundario designado para situaciones de desastre. Con los avances tecnológicos, ya no es necesario contar con servidores de respaldo en ubicaciones físicas, ya que es posible utilizar servicios en la nube.

Es necesario analizar las herramientas ya disponibles y luego elaborar una lista de tecnologías a implementar:

Tabla 7. Herramientas de Prioridad

Herramientas de Prioridad 1	
Antimalware	Sw diseñado para detectar, prevenir y eliminar programas maliciosos (malware) de un sistema informático, como virus, spyware, ransomware, entre otros.
Filtro web de contenido	Una herramienta o sistema que filtra y controla el acceso a sitios web y contenido en línea, con el objetivo de bloquear o restringir el acceso a contenido no deseado, inapropiado o potencialmente peligroso.
Antispam	Sw o mecanismo utilizado para detectar y filtrar correos electrónicos no deseados o no solicitados, conocidos como spam, con el fin de reducir su impacto en la bandeja de entrada del usuario y prevenir posibles amenazas.
IDS/IPS	Un Sistema de Detección y Prevención de Intrusiones (SDPI) es una solución de seguridad diseñada para supervisar y analizar el tráfico de red en busca de actividades que sean sospechosas o maliciosas. Su objetivo es identificar intrusiones o intentos de violación de seguridad y, en consecuencia, puede tomar medidas para bloquear o prevenir dichas actividades. El SDPI está diseñado para salvaguardar la integridad y la seguridad de la red al detectar y responder de manera proactiva a posibles amenazas o ataques.
Virtual patching	Es una técnica de seguridad que consiste en aplicar medidas temporales y virtuales para proteger una aplicación o sistema

	contra vulnerabilidades conocidas, sin necesidad de aplicar un parche o actualización de software oficial. Estas medidas pueden incluir reglas de seguridad, configuraciones específicas o redireccionamiento del tráfico, con el objetivo de reducir la exposición a posibles ataques mientras se espera la solución oficial.

Fuente: Elaboración propia

Creación del plan de proyecto

Desarrollar un plan con el objetivo de lograr lo siguiente:

Crear un conjunto de directrices que guíen la ejecución del proyecto, elaborar una documentación exhaustiva de la planificación para disponer de un registro escrito, clarificar la información para respaldar la toma de decisiones, programar revisiones fundamentales que abarquen el seguimiento, el alcance, el contenido y las fechas, y establecer un punto de referencia que facilite la evaluación del progreso del proyecto a lo largo del tiempo.

Política de ciberseguridad

Políticas Generales: Estas políticas constituyen un marco global destinado a asegurar la protección de la información, la continuidad operativa y la prevención de posibles perjuicios a los activos y incidentes de seguridad de la organización de manera eficaz y eficiente. Algunos ejemplos de estas políticas incluyen la Política de Seguridad y la Política de Gestión de Riesgos. Estos documentos proporcionan directrices y directrices sobre cómo abordar y mitigar los riesgos asociados con la seguridad de la información, así como cómo mantener la continuidad de las operaciones frente a amenazas y eventos adversos. Dichas políticas establecen los principios y las directrices generales que se deben seguir en toda la organización para asegurar una gestión de seguridad y riesgos efectiva.

Políticas sobre temas específicos: La Política de Ciberseguridad establece normas y prácticas específicas relacionadas con la

protección de los activos de información y la prevención de incidentes de seguridad en el ámbito digital.

Detalladas: Estas políticas son aplicadas en sectores o temas específicos y complementan las políticas previamente mencionadas. Algunos ejemplos incluyen la Política de Control de Acceso, la Política de Uso de Internet, la Política de Destrucción de Documentos o Archivos, y la Política de Evaluación de Riesgos de Ciberseguridad y su Metodología. Estas políticas establecen directrices y procedimientos específicos para abordar aspectos particulares relacionados con la seguridad de la información y la ciberseguridad.

Es fundamental destacar que las políticas asociadas a la administración de la ciberseguridad deben estar en sintonía con la estrategia y los objetivos de la organización. Estas políticas deben incluir un compromiso de evaluación y mejora constante, no solo en lo concerniente a la gestión de riesgos cibernéticos, sino también en relación a la seguridad integral de la información.

Tabla 8. Política de ciberseguridad

Tipo	Grupo 1	Tipo	Grupo 2
Identidad y acceso	Autenticación y Autorización.	Redes	Gestión de inventario de equipos de red.
	Manejo de credenciales.		Seguridad de acceso a la red.
	Control de accesos.		Seguridad de equipos de red.
Seguridad de datos	Clasificación información.	Amenazas	Evaluaciones de ciberseguridad.
	Encriptación de datos.		Gestión de vulnerabilidades.
	Privacidad de la información		Identificación de actores de amenazas.
	Respaldo y conservación de los datos.		

Software y aplicaciones	Gestión de software.	
	Seguridad de software.	
Endpoint	Seguridad en estaciones de trabajo.	
	Seguridad en dispositivos no supervisados.	
	Seguridad en servicios de infraestructura.	

Fuente: Elaboración propia

Para este proceso se recomienda realizarlo con el siguiente flujo de trabajo y en siguiente orden:

Primero Designar un responsable para cada grupo de políticas, de acuerdo con su tipo, Segundo establecer los elementos clave de cada política e identificar a las partes involucradas, Tercero recopilar información sobre los diferentes elementos de cada política con los actores involucrados, Luego debemos redactar las secciones pertinentes, validar el contenido y la estructura. Por último, Obtener la validación final de los involucrados.

Es recomendable que, para la inicial divulgación de la política general de ciberseguridad, se notifique y, de ser posible, se obtenga la firma de todos los empleados de la organización. Además, es crucial crear conciencia en la organización y en cada nuevo empleado sobre la importancia y el cumplimiento de la política general de ciberseguridad.

Se recomienda considerar la siguiente estrategia de comunicación y sensibilización:

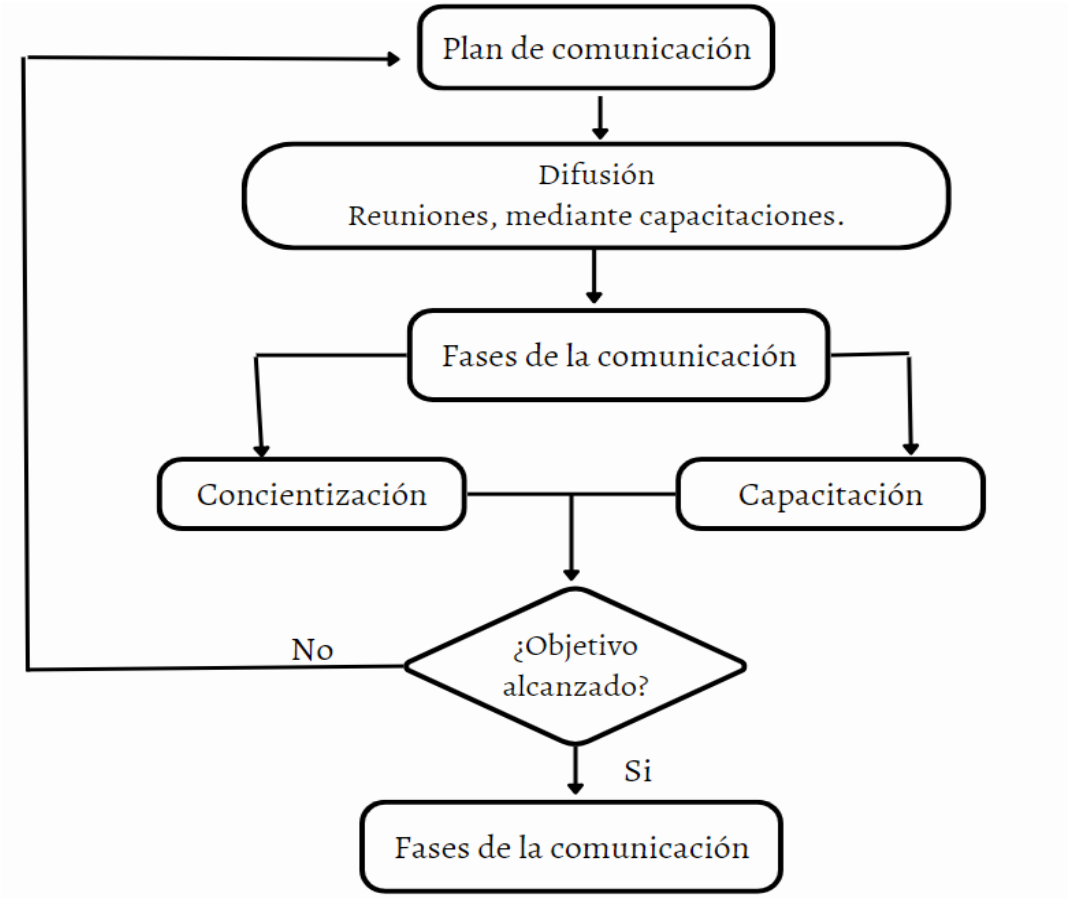

Ilustración 4. Estrategia de comunicación y sensibilización.

Fuente: Elaboración propia

Es fundamental destacar que propuesta metodológica en la organización es de vital importancia. Esta permite identificar y abordar las vulnerabilidades, reduciendo así su probabilidad de ocurrencia. Es esencial comprender que los riesgos no se eliminan, sino que se controlan, ya sea mediante la reducción de su exposición, la disminución de su probabilidad de ocurrencia o ambas acciones.

Es sumamente importante que todos los responsables y todos los niveles de la organización comprendan claramente lo mencionado anteriormente. Esto es necesario para que el equipo encargado pueda evaluar y seleccionar los controles y procesos adecuados, de acuerdo con los niveles de tolerancia de la organización respecto a la ciberseguridad.

Para lograr una gestión de riesgos adecuada, la organización debe definir su metodología y enfoque para la evaluación de riesgos, considerando metas y objetivos relacionados con la ciberseguridad.

Al realizar una evaluación de riesgos, es fundamental tener en cuenta lo siguiente:

La gestión de riesgos no es un proceso estático, sino que debe ser continuo. Esto se debe a la constante evolución de las organizaciones en términos de regulaciones y, especialmente, en relación con su ámbito de negocio. Estas evoluciones se dan a medida que las organizaciones se adentran en el mundo digital buscando procesos más ágiles y rentables. Por lo tanto, es necesario adaptarse a estos cambios en el tiempo.

Gestión del riesgo

La administración del riesgo, siguiendo la metodología NIST, se fundamenta en la categorización de niveles de implementación que brindan un contexto sobre cómo una organización aborda los riesgos y los procesos de ciberseguridad. Estos niveles se clasifican desde el Nivel 1, que es el Nivel Parcial, hasta el Nivel 4, que es el Nivel Adaptable.

Es relevante resaltar que el logro exitoso de la implementación de esta metodología basada en NIST en una organización se centra en alcanzar los resultados establecidos en el Perfil Objetivo definido por la propia organización, en lugar de enfocarse únicamente en los niveles de implementación. Aunque se sugiere que las organizaciones que se encuentren en el Nivel 1 o Parcial avancen hacia niveles superiores para obtener una mayor protección y reducción del riesgo de ciberseguridad, la decisión de progresar se basa en una evaluación específica de costo-beneficio favorable a cada organización.

Ilustración 5. Gestión del riesgo.

Fuente: Elaboración propia

Enfoque a la gestión de identificación de riesgos.

Se centra en el proceso de identificar y evaluar los riesgos que pueden afectar a la organización. Consiste en identificar las posibles situaciones que podrían tener un impacto negativo en los objetivos y actividades de la organización luego evaluar la probabilidad de que esos riesgos se materialicen y el impacto que tendrían si ocurrieran.

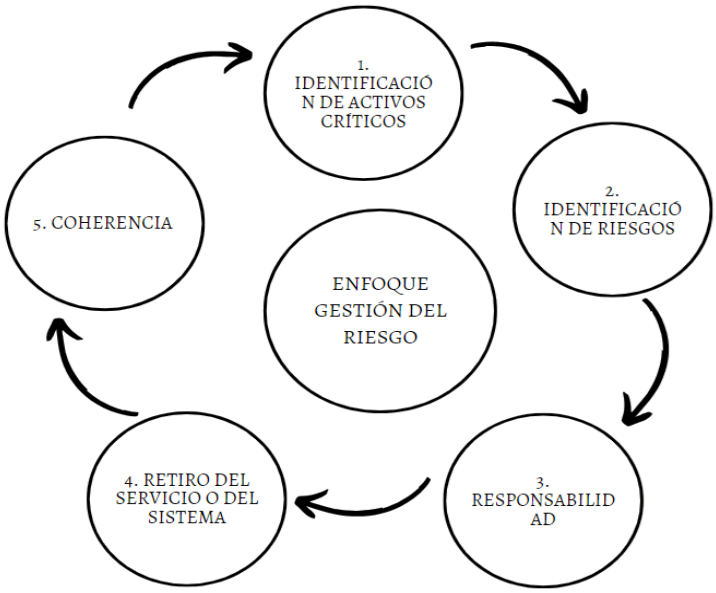

Ilustración 6. Enfoque a la gestión de identificación de riesgos.

Fuente: Elaboración propia

1. **Identificación de los activos**

Dado que proteger todos los activos puede resultar costoso para una organización y más a una pyme, es fundamental identificar de manera clara los activos críticos en colaboración con sus líderes y usuarios responsables. Esto permitirá enfocar esfuerzos, recursos en su protección y monitoreo adecuados. Al clasificar los activos, se deben considerar los siguientes aspectos:

Aspectos de negocio: Se deben analizar detalladamente los objetivos y procesos del negocio para determinar qué activos son críticos para su funcionamiento.

Tipo de información y datos almacenados: Cada activo puede contener diferentes tipos de información y datos, con distintos niveles de sensibilidad y valor.

Importancia a la continuidad del servicio: Algunos activos pueden tener un impacto significativo en la continuidad de los servicios y operaciones de la organización.

Ilustración 7. Identificación de los activos

Fuente: Elaboración propia

Para establecer la categorización de un activo como público, de uso interno o restringido, se emplea un cuestionario que evalúa el proceso de custodia y control. Dicho cuestionario se fundamenta en una evaluación individual de cada activo, tomando en consideración los siguientes criterios. La puntuación obtenida en cada criterio se pondera y se utiliza para generar la clasificación correspondiente. El objetivo es establecer un sistema objetivo y

consistente para categorizar y gestionar adecuadamente los activos, asegurando que se implementen las medidas de seguridad apropiadas según su nivel de sensibilidad y acceso permitido.

Ilustración 8. Identificación de los activos en escala

Fuente: Elaboración Propia

2. **Identificación de riesgos:**

Es un proceso que consiste en identificar, analizar y comprender los posibles eventos o situaciones que podrían tener un impacto negativo en un proyecto, una organización o cualquier actividad específica. Esto implica identificar y evaluar los diversos factores que pueden generar riesgos, como amenazas, vulnerabilidades o incertidumbres, con el objetivo de tomar medidas preventivas o correctivas para mitigarlos o eliminarlos. La identificación de riesgos es fundamental para la gestión eficaz de riesgos, ya que permite tomar decisiones informadas y desarrollar estrategias adecuadas para minimizar los impactos adversos y aprovechar las oportunidades.

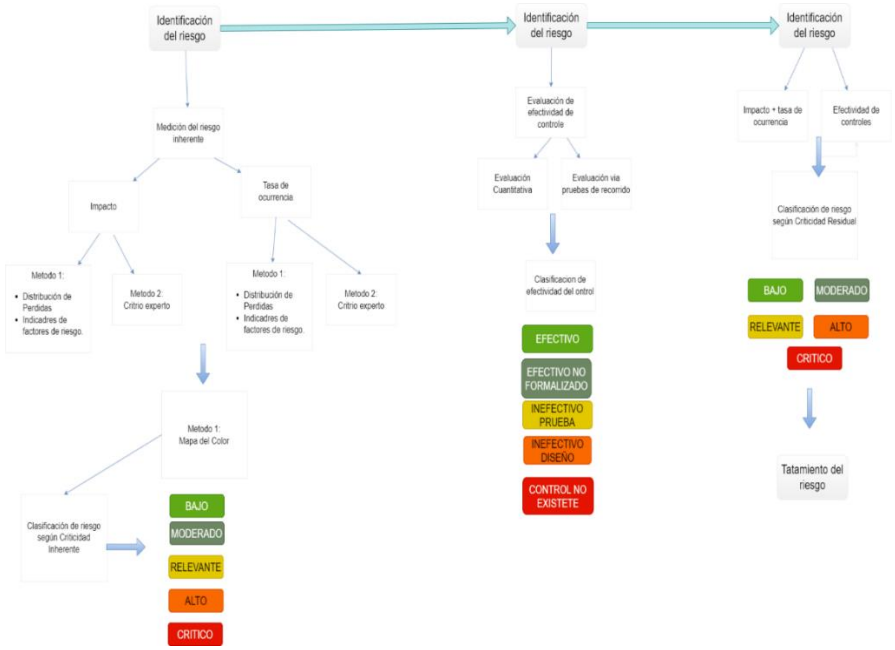

Ilustración 9. Identificación de riesgos

Fuente: Elaboración propia

Para llevar a cabo una correcta identificación de riesgos, es importante describir de manera adecuada cada uno de ellos considerando su causa, evento y consecuencia.

Causa y/o Vulnerabilidad: Este término se utiliza para describir el motivo o la razón que podría llevar a la materialización del evento identificado como riesgo. En otras palabras, se refiere a las circunstancias, condiciones o factores que podrían estar presentes y aumentar la probabilidad de que ocurra un evento adverso. Identificar y comprender las causas y vulnerabilidades es crucial para evaluar el impacto potencial y tomar medidas adecuadas para prevenir o mitigar las pérdidas para la organización.

Evento y/o Amenaza: Hace referencia al riesgo identificado en las actividades o tareas del proceso y/o sistema que está siendo evaluado. Es esencial realizar una identificación precisa del evento o amenaza específica que representa el riesgo. Al comprender claramente el evento o amenaza en cuestión, se puede evaluar adecuadamente su impacto potencial y tomar medidas apropiadas para mitigarlo. La identificación precisa del riesgo permite una gestión

eficaz y una mejor toma de decisiones en términos de implementar controles y medidas preventivas.

Consecuencia: Se refiere a la posible pérdida o materialización del evento, lo cual podría tener un impacto financiero significativo. Esto puede incluir pérdidas o daños a los activos de la organización, sanciones y multas por incumplimiento de regulaciones, litigios legales o indemnizaciones a clientes. Es importante tener en cuenta estas posibles consecuencias financieras al evaluar y gestionar los riesgos, ya que ayudará a determinar la importancia y prioridad de las medidas de control y mitigación a implementar.

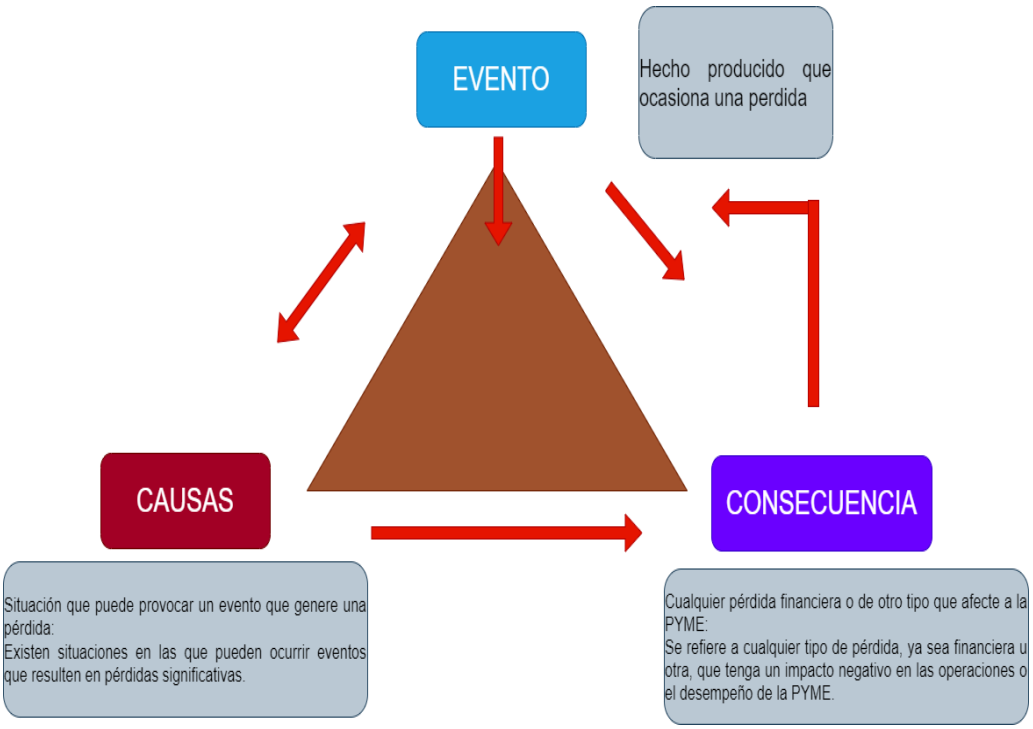

Ilustración 10. Causa, evento y consecuencia.

Fuente: Elaboración propia

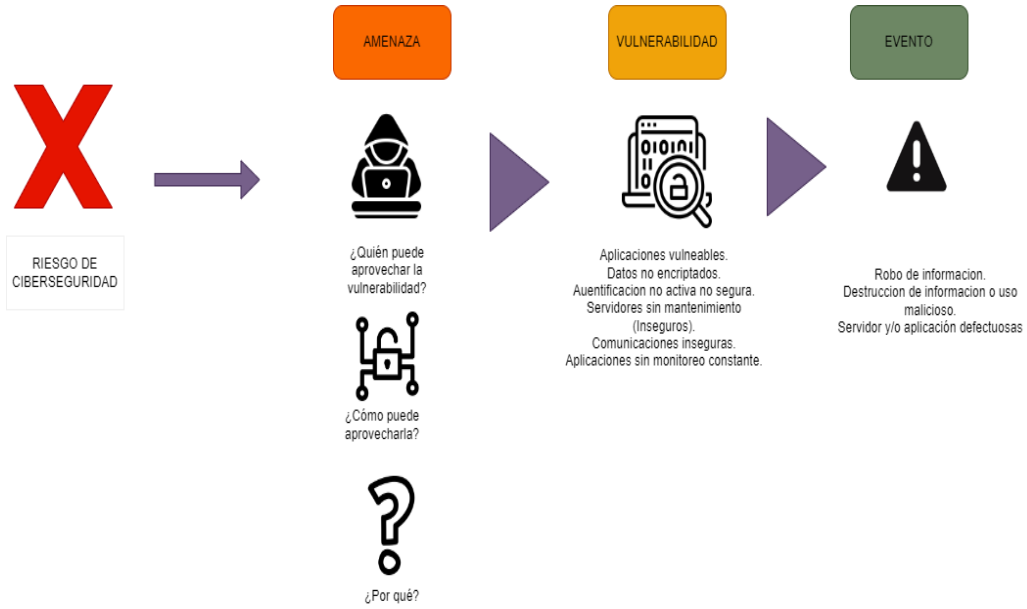

Ilustración 11. Medir Riesgo de ciberseguridad

Fuente: Elaboración propia

3. Evaluación del riesgo

Es fundamental que cualquier criterio de aceptación con niveles de riesgo deseados como objetivos. Además, se deben establecer los mecanismos necesarios para que la alta dirección y los responsables de cada riesgo los acepten y los gestionen por encima o por debajo de un nivel determinado.

Para facilitar la aceptación y la medición de los riesgos, es posible expresar los criterios en términos de la relación entre el impacto económico y la tasa de ocurrencia:

Impacto:

Se define como el grado de daño o pérdida que podría resultar de la materialización de una amenaza o incidente de seguridad en un sistema, activo o proceso de una organización. El impacto puede manifestarse en términos de daño financiero, daño a la reputación, pérdida de productividad, interrupción de servicios, violación de la privacidad, etc. La evaluación del impacto permite comprender las consecuencias potenciales de un incidente

de seguridad y tomar medidas adecuadas para mitigar los riesgos identificados.

Tasa de ocurrencia:

Se refiere a la frecuencia estimada con la que se espera que ocurra un evento o incidente de seguridad específico en un sistema o entorno dado. Representa la probabilidad de que se materialice una amenaza o se produzca un evento no deseado en un período de tiempo determinado.

La tasa de ocurrencia puede basarse en datos históricos, análisis de amenazas, estudios de vulnerabilidades u otras fuentes de información relevante. Es importante tener en cuenta que la tasa de ocurrencia no es una medida precisa y definitiva, sino una estimación basada en la información disponible. Proporciona una base para evaluar y comparar los riesgos, así como para tomar decisiones informadas sobre la asignación de recursos y la implementación de medidas de control apropiadas.

Indicador Monitoreo

Tabla 9. Indicador Monitoreo

Indicadores	**Descripción**
KPI (Key Performance Indicator)	Utilización de bases de datos y sistemas operativos que no reciben soporte. Falta de aplicar actualizaciones de seguridad en estaciones y servidores. Existencia de vulnerabilidades identificadas a través de pruebas de Ethical Hacking. Ausencia de antivirus en estaciones o servidores. Falta de validación de controles en estaciones para acceder a la red corporativa. Falta de ejecución o incumplimiento de los respaldos programados.

KRI (Key Risk Indicator)	Costos relacionados con incidentes de ciberseguridad. Pérdida de registros críticos. Tiempos de inactividad causados por incidentes de ciberseguridad.

Fuente: Elaboración propia

Tasa de Ocurrencia

Tabla 10. Tasa de Ocurrencia

Nivel	**Descripción**
Casi probable	Los eventos similares tienen una frecuencia mensual.
Probable	Los eventos similares tienen una frecuencia aproximada de cada seis meses.
Posible	Los eventos similares ocurren una vez al año.
Improbable	Los eventos similares ocurren aproximadamente cada tres años.
Raro	Los eventos similares ocurren aproximadamente cada cinco años o no hay registro conocido del evento.

Fuente: Elaboración propia

4. Amenazas y Vulnerabilidades

1.1. Amenazas

Es esencial tener un claro entendimiento de los diversos puntos de entrada para identificar las amenazas que pueden dar lugar a riesgos. Estas amenazas pueden involucrar a:

Propietarios o usuarios de los activos, Miembros del personal de la organización en todos los niveles, Proveedores de servicios, Clientes y Servidores, bases de datos y/o sistemas desactualizados o con un diseño deficiente.

Una vez que las amenazas y sus fuentes de acceso a la organización han sido identificadas, es necesario crear una base de datos que contenga la información sobre la amenaza, su fuente y los controles de mitigación correspondientes.

1.2. Vulnerabilidades

Es crucial comprender que las vulnerabilidades, aunque se identifican de manera similar a los riesgos, no causan daño por sí mismas, ya que dependen de una amenaza o riesgo real que las aproveche.

Es importante tener en cuenta que si existe una vulnerabilidad que no está vinculada a una amenaza actual, es posible que no se requiera implementar un control específico. Sin embargo, dicha vulnerabilidad debe ser reconocida y monitoreada para que, en caso de que se identifique una amenaza, se pueda implementar un plan de remediación adecuado.

Tabla 11. Vulnerabilidades

AMENAZA	**VULNERABILIDAD**	**CONSECUENCIA**
Pérdida o Robo de equipo	Almacén sin supervisión	Pérdida financiera.
Llamadas telefónicas	Línea abierta sin protección	Filtración de las llamadas
Ataque Cibernético	Escribir credenciales sin cifrado	Pérdida de información
Error de entrada de datos	Sistema complejo de utilizar	Base de Datos dañada

Fuente: Elaboración propia

2. Controles

Una vez que se han identificado los riesgos, es importante solicitar a la unidad correspondiente que incluya los controles necesarios para mitigarlos. Estos controles pueden variar desde soluciones tecnológicas hasta procedimientos manuales.

Para lograr una mayor precisión en la identificación y redacción de los controles, es fundamental que estos respondan a cuatro preguntas clave: ¿Qué?, ¿Cuándo?, ¿Quién? Y ¿Cómo? Estas preguntas ayudan a definir claramente la naturaleza del control, el momento en que debe ser implementado, la pyme responsable de su ejecución y el método o procedimiento específico que se utilizará.

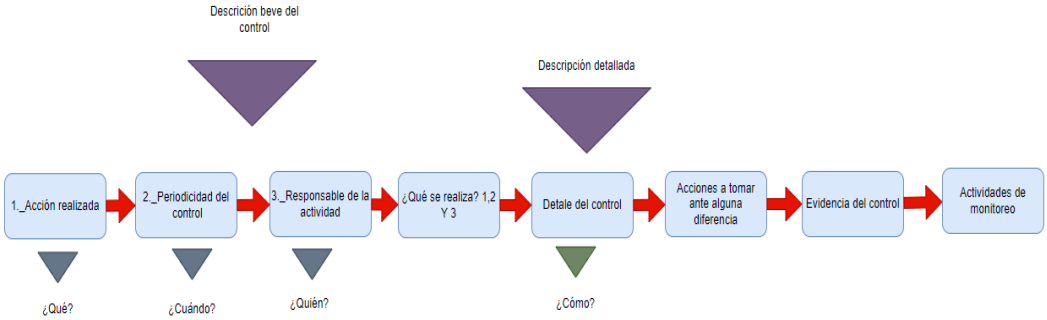

Ilustración 12. Controles

Fuente: Elaboración propia

Clasificación

Tabla 12. Clasificación

Nivel	Sub Nivel	Descripción
Preventivo	Automático	Acción preventiva que evita la ocurrencia de errores, vulnerabilidades, ataques o eventos de riesgo. Se lleva a cabo mediante la ejecución de un programa de control.

	Manual	Acción preventiva que evita la ocurrencia de errores, vulnerabilidades, ataques o eventos de riesgo. La ejecución de esta acción puede ser realizada por una persona.
Detectivo	Automático	Proceso de detección que identifica errores, vulnerabilidades, ataques o eventos de riesgo una vez que la transacción ha tenido lugar. Se utiliza un programa de control para llevar a cabo esta acción.
	Manual	Proceso de detección que identifica errores, vulnerabilidades, ataques o eventos de riesgo después de que la transacción ha tenido lugar. Esta actividad puede ser llevada a cabo por un individuo responsable de su ejecución.

Fuente: Elaboración propia

Después de haber identificado las amenazas y los correspondientes controles, es necesario crear una base de datos que permita establecer vínculos entre los riesgos y los controles. Esto facilitará el seguimiento de los riesgos a los que la organización está expuesta, clasificándolos por proceso.

Es importante tener en cuenta que si existen controles que mitigan un riesgo específico identificado, dicho riesgo se considerará residual en lugar de inherente. La clasificación de este riesgo residual dependerá de la solidez y efectividad del control implementado. Así, se establecerá una relación clara y documentada entre los riesgos identificados y los controles implementados, lo que contribuirá a una gestión efectiva de los riesgos y a evaluar la eficacia de los controles en la protección de la organización.

3. Riesgo

Las estrategias para abordar los riesgos de ciberseguridad se seleccionarán considerando el contexto y el nivel de criticidad evaluado. Existen varias estrategias comunes que se pueden emplear, como:

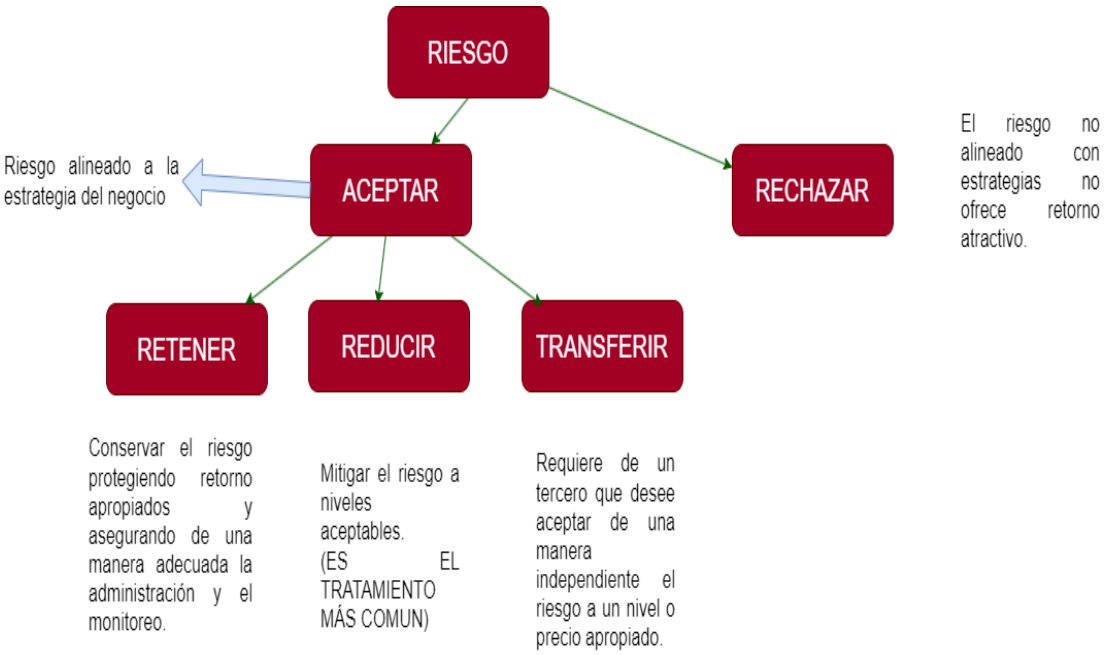

Ilustración 13. Riesgo

Fuente: Elaboración propia

El enfoque de abordaje "Mitigar" se empleará para los riesgos residuales que sean evaluados como Relevante, Alto o Crítico en términos de su nivel de criticidad. Para alcanzar el objetivo de este enfoque, es crucial identificar el riesgo y proponer planes de acción o controles adecuados. El propietario del riesgo identificado será responsable de proponer y dar seguimiento a la implementación de estos planes de acción.

4. Coherencia

Es esencial que en toda la organización se tenga una comprensión clara de que el enfoque de gestión de riesgos se aplica en todos los niveles. En este enfoque, se asignan responsabilidades tanto a los usuarios como a los proveedores, con el objetivo de llevar a cabo actividades específicas, como la planificación de situaciones de emergencia, la recuperación ante desastres y el desarrollo e implementación de programas de protección de sistemas bajo su control y/o administración.

En resumen, se estableció una estrategia de recolección de datos que involucró la recopilación de información sobre los ataques a las PYMES, se seleccionaron la metodología de investigación y el diseño más apropiados, y se aplicó la Metodología NIST para desarrollar una propuesta de medidas concretas destinadas a mitigar los riesgos de ciberataques para las PYMES.

3.6. Método de análisis de datos

Se utilizó el método de la escala de Likert para evaluar el nivel de conformidad de las pymes en cuanto a su ciberseguridad. La escala de Likert es un procedimiento de investigación que emplea una escala de calificación para determinar el grado de conocimiento de los individuos sobre un tema específico. En esta escala, los encuestados clasifican sus respuestas según su nivel de conocimiento o familiaridad con el tema.

En consecuencia, esta escala permite evaluar la conformidad de los individuos y resulta útil cuando se busca obtener una descripción detallada sobre un tema en particular (Douglas da Silva, 2020).En el primer paso, se aplicará un cuestionario que medirá la variable Ciberataques a Pymes, con sus respectivos indicadores que son: Nivel de afectación, vulnerabilidades detectadas, vulnerabilidades tratadas.

Tabla 13. Tabla de resultados de respuestas de los ítems

Conozco mucho	5
Conozco	4
Ni mucho, ni poco	3
Conozco poco	2
No conozco	1

Resultados de respuestas de los ítems correspondientes los indicadores de la variable Ciberataques a pymes.

Conozco mucho: Tiene un conocimiento profundo y detallado sobre el nivel de ciberseguridad, Conozco: Tiene un nivel de conocimiento general sobre el nivel de ciberseguridad, Ni mucho, ni poco: Tiene un conocimiento moderado sobre el nivel de ciberseguridad, Conozco poco: Tiene un conocimiento limitado sobre el nivel de ciberseguridad y No conozco: No tiene conocimiento o información sobre el nivel de ciberseguridad.

Una vez completada la fase de recopilación de datos, se transferirán las puntuaciones obtenidas en el cuestionario aplicado a las PYMES encuestadas a una hoja de cálculo en Excel 2019. Esta etapa permitirá la sistematización de la información con el objetivo de presentarla posteriormente en tablas y gráficos, según corresponda y resulte pertinente.

3.7. Aspectos éticos

En este trabajo de investigación, se han observado y respetado los principios éticos fundamentales de la investigación científica, asegurando la aplicación de los criterios de autonomía y justicia. Todos

los participantes del estudio fueron debidamente informados de que su participación era voluntaria. Además, se ha prestado especial atención al respeto de las propiedades intelectuales, asegurándose de citar y referenciar correctamente toda la información utilizada en el estudio.

IV. RESULTADOS

VARIABLE: Ciberseguridad y Metodología Nist.

Con el objetivo de evaluar los indicadores de esta variable, se utilizaron métodos descriptivos y se llevó a cabo una encuesta para su evaluación. Los instrumentos se aplicaron en una muestra, correspondientes a las pymes.

Posteriormente, se realizó un análisis y normalización de los datos, y debido al tamaño de la muestra, inferior a 50, se aplicó la prueba de Shapiro-Wilk.

OE1: Identificación de los diferentes tipos de ciberataques que enfrentan las pymes.

Indicador 1: Nivel de afectación

Los datos se obtuvieron a través de una encuesta, la cual se aplicó a cinco empresas diferentes, obteniendo el nivel de afectación, para determinar las muestras, con la que se trabajó con 1 empresa especifica.

HIPÓTESIS PARA PRUEBA DE NORMALIDAD:

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN:

Si p<0.05, se rechaza la Ho y se acepta la Ha.

Si p >=0.05, se rechaza la Ha y se acepta la Ho.

Tabla 14. Prueba de normalidad de indicador Porcentaje de Nivel de Afectación

MUESTRA	Shapiro-Wilk		
	ESTADISTICO	gl	Sig.
	0.904	40	0.003

Fuente: Elaboración propia

Debido a que el valor de significancia asintótica es inferior a 0.05, se rechaza la hipótesis nula según el nivel de significancia obtenido. Por consiguiente, se acepta la hipótesis alternativa y se recomienda aplicar la metodología en la pequeña y mediana empresa (Pyme). Este resultado sugiere que las vulnerabilidades en diversas pymes presentan problemas de seguridad, ya que muestran un alto porcentaje de afectación.

OE2: Clasificar los distintos ataques con mayor impacto a las pymes.

Indicador 2: Vulnerabilidades detectadas

Los datos se obtuvieron a través de una encuesta, la cual se aplicó a cinco empresas diferentes, obteniendo el nivel de afectación, para determinar las muestras

HIPÓTESIS PARA PRUEBA DE NORMALIDAD:

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN:

Si p<0.05, se rechaza la Ho y se acepta la Ha.

Si p >=0.05, se rechaza la Ha y se acepta la Ho.

Tabla 15. Prueba de normalidad de indicador Porcentaje de Vulnerabilidades detectadas

MUESTRA	Shapiro-Wilk		
	ESTADISTICO	gl	Sig.
	0.909	40	0.003

Fuente: Elaboración propia

Debido a que el valor de significancia asintótica es menor a 0.05, se rechaza la hipótesis nula de acuerdo al nivel de significancia obtenido. Por lo tanto, se acepta la hipótesis alternativa y se recomienda aplicar la metodología en

la pequeña y mediana empresa (Pyme). El resultado implica que las vulnerabilidades en diversas pymes presentan problemas de seguridad, ya que se han detectado un alto porcentaje de vulnerabilidades.

OE3: Mitigación de riesgos asociados a los ciberataques.

Indicador 3: Vulnerabilidades Tratadas

Los datos se obtuvieron a través de una encuesta, la cual se aplicó a cinco empresas diferentes, obteniendo el nivel de afectación, para determinar las muestras

HIPÓTESIS PARA PRUEBA DE NORMALIDAD:

Ho: Los datos tienen una distribución normal.

Ha: Los datos no tienen una distribución normal.

CRITERIO DE DECISIÓN:

Si p<0.05, se rechaza la Ho y se acepta la Ha.

Si p >=0.05, se rechaza la Ha y se acepta la Ho.

Tabla 16. Prueba de normalidad de indicador Porcentaje de Vulnerabilidades Tratadas

MUESTRA	Shapiro-Wilk		
	ESTADISTICO	gl	Sig.
	0.904	40	0.002

Fuente: Elaboración propia

Debido a que el valor de significancia asintótica es menor a 0.05, se rechaza la hipótesis nula de acuerdo al nivel de significancia obtenido. Por lo tanto, se acepta la hipótesis alternativa y se recomienda aplicar la metodología en la pequeña y mediana empresa (Pyme). El resultado implica que las vulnerabilidades en diversas pymes presentan problemas de seguridad, ya

que se ha observado un bajo porcentaje de vulnerabilidades tratadas o resueltas.

Las preguntas que generan diferenciación son las siguientes:

P1: ¿Qué tan satisfecho(a) está con la efectividad de mitigación de riegos ante ciberataques guiándose de la metodología NIST?

P4: ¿Qué tan satisfecho(a) está con la experiencia de la simulación implementada?

Para la pregunta 1 tanto en las mitigaciones riesgos ante ciberataques, a comparación de otros métodos a utilizar, esta demostró una mayor confiabilidad y facilidad de uso, sin una inversión extrema que afecte a la economía de una PYME.

Para la pregunta 2 tanto en la experiencia de la simulación, los participantes demostraron tener la confianza para implementar esa metodología en la PYME, por lo que la simulación demostró una efectividad ante estos ciberataques.

Tabla 17. Preguntas que generan diferenciación por métodos a utilizar, para el indicador Controles Aplicador.

ÍTEM 1	Shapiro-Wilk		
	ESTADÍSTICO	gl	Sig.
	0.827	8	0.056
ÍTEM 2	Shapiro-Wilk		
	ESTADÍSTICO	gl	Sig.
	0.665	8	0.001

Debido a que el valor de significancia asintótica es menor a 0.05, se rechaza la hipótesis nula de acuerdo al nivel de significancia obtenido. Por lo tanto, se acepta la hipótesis alternativa, se demostró la confiabilidad y eficacia de la Propuesta metodológica basada en NIST según la PYME, para ser utilizada en una prevención de ataques cibernéticos.

V. DISCUSIÓN

El presente proyecto de investigación, tuvo como finalidad desarrollar y aplicar una propuesta para mitigar los riesgos que generan los ciberataques en las pymes., además para lograr demostrar dicha finalidad se tuvo por objetivos específicos: Identificar los distintos tipos de ciberataques a las pymes, Clasificar los distintos ataques con mayor impacto a pymes, y Mitigación de riesgos asociados a los ciberataques.

Para ello se tomaron datos para cada uno de los indicadores que se están evaluando a través de un cuestionario aplicado a una población de 40 personas, esta población se enfocó en una muestra. Los datos obtenidos de cada resultado mostraron tener una distribución no normal usando el método de Shapiro-Wilk.

Los resultados obtenidos en esta investigación están en línea con los antecedentes seleccionados y analizados. En primer lugar, la hipótesis planteada en este estudio fue aceptada, lo que indica que la mitigación de riesgos asociados a los ciberataques es un objetivo crucial para cualquier organización o entidad que opere en el entorno digital actual.

Al analizar los resultados de cada objetivo específico de la investigación en relación con los antecedentes, se puede observar una relación positiva y coherente. Por ejemplo, la encuesta de satisfacción y confiabilidad aplicada en la metodología de la PYME arrojó respuestas muy satisfactorias, lo que respalda los hallazgos de investigaciones anteriores que también destacaron la importancia de implementar medidas de mitigación de riesgos.

Además, los resultados de esta investigación refuerzan la relevancia de los antecedentes seleccionados al demostrar la efectividad de las acciones tomadas para reducir los riesgos de ciberataques. Estos resultados respaldan y corroboran los hallazgos previos, brindando una base sólida para concluir que la mitigación de riesgos cibernéticos es esencial en el entorno digital actual.

Con los resultados obtenidos y que se detallan en el capítulo anterior de la investigación, se procedió a realizar las discusiones con respecto a una

propuesta metodológica para mitigar los riesgos sobre ciberataques a PYMES, usando la METODOLOGIA NIST.

Nivel de afectación, la discusión de los resultados reveló una media significativa de 0.003 y una desviación estándar de 0.904. Estos cálculos se basaron en el promedio de los estadísticos descriptivos de los indicadores pertenecientes a la dimensión, utilizando un peso de muestra del 40%. Estos resultados cuantitativos proporcionan una medida objetiva de la afectación experimentada por las PYMES en relación con los riesgos de ciberseguridad.

En cuanto al nivel de afectación, se utilizó una Escala de Likert para medir el impacto sufrido por las PYMES. Se determinó que un nivel de afectación del 0% al 20% se considera bajo, del 21% al 25% se considera medio y a partir del 25% se considera alto. Según los niveles de respuesta obtenidos, se observó que la PYME con mayor nivel de afectación fue la PYME 4, con un nivel de afectación del 27%, en comparación con las otras cinco PYMES entrevistadas. Por otro lado, la PYME 1 mostró un nivel de afectación del 15%, la PYME 2 del 25%, la PYME 3 del 17% y la PYME 5 del 16%. Estos resultados son consistentes con los hallazgos de Benz y Chatterjee (2022), quienes señalan que las PYMES han experimentado demoras en la adopción de tecnología y medidas de seguridad adecuadas, lo que las expone a riesgos significativos.

La discrepancia entre las medidas de afectación encontradas en esta investigación y las investigaciones anteriores resalta la importancia de que las PYMES reconozcan y aborden adecuadamente los riesgos de ciberseguridad. El hecho de que algunas PYMES presenten altos niveles de afectación indica que aún existe una brecha en la adopción de medidas de seguridad eficaces. Esta brecha puede poner en peligro la supervivencia y la capacidad de las PYMES para prosperar en el entorno digital actual.

En conclusión, los resultados obtenidos en esta investigación, respaldados por los antecedentes seleccionados, subrayan la necesidad de que las PYMES no subestimen la importancia de la ciberseguridad. Es esencial que tomen medidas proactivas para proteger sus sistemas y activos digitales, ya que esto puede

determinar su capacidad para sobrevivir y mantenerse competitivas. Las PYMES deben superar las demoras en la adopción de tecnología y medidas de seguridad adecuadas, y en su lugar, centrarse en fortalecer su postura de seguridad cibernética para enfrentar eficazmente los riesgos presentes en el entorno digital actual.

Vulnerabilidades detectadas, los resultados obtenidos revelaron una media significativa de 0.003 y una desviación estándar de 0.909, obtenidos a partir del promedio de los estadísticos descriptivos de los indicadores que conforman la dimensión, utilizando un peso de muestra del 40%.

En relación al nivel de vulnerabilidades detectadas, se utilizó una Escala de Likert para medir el impacto. Se determinó que un nivel de detección del 0% al 20% se considera bajo, del 21% al 25% se considera medio y a partir del 25% se considera alto, lo cual indica que una PYME con un nivel de afectación alto es candidata para aplicar la metodología propuesta. Al analizar los niveles de detección de las pymes entrevistadas, se encontró que la PYME 4 presentó el mayor nivel de detección, con un 27%. En contraste, la PYME 1 tuvo un nivel de detección del 19%, la PYME 2 del 24%, la PYME 3 del 15% y la PYME 5 también del 15%. Debido a que la PYME 4 mostró el nivel más alto de vulnerabilidades detectadas, se decidió trabajar con ella en el desarrollo de la metodología.

En relación a los antecedentes, se ha identificado que existen diferentes tipos de ciberataques. Uno de ellos son los virus informáticos, que son programas maliciosos diseñados para infectar archivos y causar daños en el sistema informático afectado (Norton LifeLock, 2021). Otro tipo es el correo no deseado o SPAM, que consiste en el envío masivo de mensajes no solicitados con intenciones perjudiciales para el receptor (Francisco J. Urueña Centeno, 2015). También está el spoofing, que es un método en el cual el atacante oculta su identidad para obtener acceso a recursos en otro sistema confiando en la dirección IP del host suplantado, representando una amenaza para organizaciones de cualquier tipo.

Estos antecedentes resaltan la importancia de abordar los riesgos asociados a los ciberataques, ya que estos pueden manifestarse a través de diferentes formas y representar una amenaza para la seguridad de las PYMES. La detección de vulnerabilidades en la PYME 4 refuerza la necesidad de aplicar la metodología propuesta, ya que se ha identificado que existen riesgos significativos que deben ser mitigados para proteger los sistemas y activos digitales de la organización.

En resumen, los resultados obtenidos en esta investigación revelan la presencia de vulnerabilidades y riesgos de ciberseguridad en la PYME 4, respaldando la necesidad de implementar medidas de mitigación. Estos hallazgos están en línea con los antecedentes que describen los diferentes tipos de ciberataques y sus consecuencias. La combinación de estos resultados y antecedentes subraya la importancia de tomar medidas proactivas para proteger los sistemas y activos digitales de las PYMES en el entorno digital actual.

Vulnerabilidades tratadas, los resultados obtenidos revelaron una media significativa de 0.002 y una desviación estándar de 0.904, obtenidos mediante el promedio de los estadísticos descriptivos de los indicadores que conforman la dimensión, utilizando un peso de muestra del 40%.

En relación al nivel de vulnerabilidades detectadas, se utilizó una Escala de Likert para medir el impacto. Se determinó que un nivel de detección del 0% al 20% se considera bajo, del 21% al 25% se considera medio y a partir del 25% se considera alto, lo cual indica que una PYME con un nivel de afectación bajo es candidata para aplicar la metodología propuesta. Al analizar los niveles de vulnerabilidades tratadas en las PYMES entrevistadas, se encontró que la PYME 4 presentó el nivel más bajo de vulnerabilidades tratadas, con un 18%. En contraste, la PYME 1 mostró un nivel de vulnerabilidades tratadas del 20%, la PYME 2 del 21%, la PYME 3 del 22% y la PYME 5 del 19%.

En cuanto a la metodología NIST, esta se fundamenta en tres pasos: evaluación del peligro, estudio y evaluación de soluciones. Según Arias y Llanos (2012), esta metodología puede ser aplicable a la evaluación de sistemas. Asimismo, Avalos Serrano (2007) señala que es fundamental contar con el respaldo y

colaboración de todos los miembros de la organización para lograr una adecuada administración de riesgos y alcanzar las metas y objetivos establecidos.

Estos antecedentes y resultados indican que, si bien algunas PYMES han tratado un porcentaje bajo de vulnerabilidades, es necesario implementar una metodología como la propuesta por NIST para evaluar y gestionar los riesgos de manera efectiva. Además, se destaca la importancia de contar con la colaboración de todos los miembros de la organización para asegurar el éxito de la administración de riesgos.

En resumen, los resultados obtenidos en esta investigación muestran que algunas PYMES presentan un bajo nivel de vulnerabilidades tratadas, lo cual indica la necesidad de aplicar una metodología como la propuesta por NIST. Esta metodología, respaldada por los antecedentes mencionados, proporciona un enfoque estructurado para evaluar y gestionar los riesgos de manera efectiva. Sin embargo, es fundamental involucrar a todos los miembros de la organización en este proceso para asegurar el éxito en la administración de riesgos y alcanzar los objetivos establecidos.

VI. CONCLUSIONES

En cuanto al primer objetivo específico, identificar los distintos tipos de ciberataques a las pymes, de acuerdo a los resultados obtenidos, se concluyó que hay muchas PYMES han sido afectadas al menos por un tipo de ciberataque, según los instrumentos aplicados arrojan un porciento alto de PYMES que no tienen con el conocimiento de tener una prevención en caso de ser víctimas de ciberdelincuentes, en los últimos años según análisis del diario gestión 5 de cada 10 pymes sufren de al menos un ataque cibernético, por lo que no le toman la importancia, mientras que las grandes empresas que aplican NIST, comprende un conjunto de estándares y buenas prácticas, para así gestionar los riesgos de seguridad cibernética, esto proporciona una base sólida para diseñar estrategias de mitigación específicas y efectivas.

Por otra parte, el segundo objetivo específico, clasificar los distintos ataques con mayor impacto a pymes, la investigación permitió agrupar los distintos tipos de ciberataques con mayor impacto mediante el instrumento aplicado, dio a conocer que más de un PYME ha sido víctima de un ciberataque, por lo que nos enfocamos mediante antecedentes, para ver los ciberataques más frecuentes y con mayor impacto para poder clasificarlos, para así establecer medidas de seguridad y controles adecuados para prevenir, detectar y responder a los ciberataques, reduciendo así la probabilidad de incidentes y mitigando su impacto en las PYMES.

Finalmente, con el tercer y último objetivo específico, gracias a los resultados obtenidos se demostró la efectividad de una disminución de posibles ataques cibernéticos. Estos resultados respaldan la importancia de implementar medidas de mitigación de riesgos en las PYMES, especialmente en aquellas que operan en el entorno digital. La encuesta de satisfacción y confiabilidad aplicada en la a la PYME arrojó respuestas muy satisfactorias, lo que demuestra que las acciones tomadas para

reducir los riesgos de ciberataques fueron efectivas también la mitigación de riesgos asociados a los ciberataques es un objetivo crucial para cualquier organización o entidad que opere en el entorno digital actual.

De acuerdo con resultados de los indicadores, también se llegó a la conclusión que una PYME no tiene el tiempo de abordar cada uno de los controles de la metodología, ya que cuenta con recursos limitados, y querrá aplicar su esfuerzo donde tenga mayor impacto.

Dada la creciente sofisticación y frecuencia de los ciberataques, es fundamental implementar estrategias efectivas de mitigación para proteger los activos digitales de las PYMES, preservar la integridad de los datos y garantizar la continuidad de las operaciones.

VII. RECOMENDACIONES

Implementar medidas de seguridad en todas las capas de la organización: Asegurándonos de que las medidas de seguridad estén implementadas en todos los niveles de la pyme, incluyendo la infraestructura de red, los sistemas operativos, las aplicaciones y la concienciación de los empleados. Esto ayudará a fortalecer la seguridad de la información y a mitigar los riesgos de ciberataques.

Realizar evaluaciones periódicas de vulnerabilidades: Llevar a cabo evaluaciones regulares de las vulnerabilidades en los sistemas y la infraestructura de las PYMES. Esto permitirá identificar posibles brechas de seguridad y tomar medidas preventivas antes de que se conviertan en puntos de entrada para los ciber atacantes.

Establecer un plan de respuesta ante incidentes: Desarrollar un plan de respuesta ante posibles ciberataques que contenga los pasos a seguir en caso de detección de un incidente. Esto incluye la notificación de las partes relevantes, la preservación de pruebas y la restauración de la operatividad normal de la empresa. Contar con un plan de respuesta bien definido facilitará la mitigación de los riesgos y minimizará el impacto de los ciberataques en las PYMES.

REFERENCIAS

acm. 2017. [En línea] 2017. https://dl.acm.org/doi/abs/10.1145/3102304.3109812.

Alexandra Kianid, Cezar Scarlatr and Gheorghe Militaru. 2002. books.google. [En línea] 2002. https://books.google.com.pe/books?hl=es&lr=&id=74k9DwAAQBAJ&oi=fnd&pg=PA307&dq=Cyber+attacks+on+SMEs&ots=RlGe-HthH4&sig=2KnheoSGM6djuEEo4M8cORpCTAA#v=onepage&q=Cyber%20attacks%20on%20SMEs&f=false.

Al-Herwi, Somaya JALAL. 2019. Researchgate. [En línea] 2019. https://www.researchgate.net/publication/332539278_What_are_SMEs#:~:text=small%20and%20medium%2Dsized%20enterprise,of%20long%2Dterm%20economic%20growth..

Alphaenginyeria. 2021. [En línea] 2021. https://alphaenginyeria.com/ciberataques-ciberaseguridad-y-pymes.

alphaenginyeria. 2022. alphaenginyeria. [En línea] 2022. https://alphaenginyeria.com/ciberataques-ciberaseguridad-y-pymes.

B.V., Elsevier. 2021. sciencedirect. [En línea] 2021. https://www.sciencedirect.com/science/article/abs/pii/S0167923621000907.

Berger, George Casella Y Roger L. 2015. [En línea] 2015. https://mybiostats.files.wordpress.com/2015/03/casella-berger.pdf.

Centeno, Francisco J. Urueña. 2015. ieee. [En línea] 2015. https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.

Chatterjee, Michael Benz y Dave. 2022. sciencedirect. [En línea] 2022. https://www.sciencedirect.com/science/article/abs/pii/S0007681320300392.

ciberseguridad. 2018. ciberseguridad. [En línea] 2018. https://ciberseguridad.blog/como-implantar-el-framework-nist/.

compartiendoconocimiento. 2021. compartiendoconocimiento. [En línea] 2021. https://compartiendoconocimiento.elmundo.es/vivencias-empresariales/las-pymes-objetivo-principal-de-una-gran-parte-de-los-ciberataques.

deloitte. 2019. deloitte. [En línea] 2019. https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/press/20190619%20Un%2032%20porciento%20de%20empresas%20locales%20report%C3%B3%20ciberataques%20en%20los%20%C3%BAltimos%2024%20meses.pdf.

elperuano. 2022. elperuano. [En línea] 2022. https://elperuano.pe/noticia/168541-pymes-en-la-mira-de-la-ciberdelincuencia#:~:text=12%2F07%2F2022%20Entre%20enero,al%20Protocolo%20de%20Escritorio%20Remoto..

—. 2021. elperuano.pe. [En línea] 2021. https://elperuano.pe/noticia/133055-pymes-tienen-dificultades-para-invertir-en-seguridad-digital-segun-estudio.

—. 2022. elperuano.pe. [En línea] 2022. https://elperuano.pe/noticia/168541-pymes-en-la-mira-de-la-ciberdelincuencia#:~:text=12%2F07%2F2022%20Entre%20enero,al%20Protocolo%20de%20Escritorio%20Remoto..

—. elperuano.pe. [En línea] https://elperuano.pe/noticia/168541-pymes-en-la-mira-de-la-ciberdelincuencia#:~:text=12%2F07%2F2022%20Entre%20enero,al%20Protocolo%20de%20Escritorio%20Remoto..

Empresarial, Business. 2021. Businessempresarial. [En línea] 2021. https://www.businessempresarial.com.pe/peru-sufrio-mas-de-4-700-millones-de-intentos-de-ciberataques-en-el-primer-semestre-del-ano/.

esan. 2021. esan.edu.pe. [En línea] 2021. https://www.esan.edu.pe/conexion-esan/ciberseguridad-para-pymes-que-hacer-cuando-se-tiene-un-presupuesto-limitado#:~:text=Seg%C3%BAn%20un%20estudio%20realizado%20por,de%204700%20millones%20de%20intentos..

Frett, Nahun. 2015. nahunfrett. [En línea] 2015. http://nahunfrett.blogspot.com/2015/06/otro-ciberataque.html#more.

gestion. 2022. gestion.pe. [En línea] 2022. https://gestion.pe/economia/mercados/ciberataques-cuantos-hay-en-el-peru-y-como-se-protegen-las-empresas-noticia/.

gestion.pe. 2022. gestion. [En línea] 2022. https://gestion.pe/economia/mercados/ciberataques-cuantos-hay-en-el-peru-y-como-se-protegen-las-empresas-noticia/.

Grant, Kenneth. 2011. books.google. [En línea] 2011. https://books.google.com.pe/books?hl=es&lr=&id=4HiKP9dDoc8C&oi=fnd&pg=PA62&dq=Cyber+attacks+on+SMEs&ots=oh7eKlwJTB&sig=rG1H3o6KtKlpO6185Yx7CiR2Vv8#v=onepage&q=Cyber%20attacks%20on%20SMEs&f=false.

Grinblatt. 2002. virtual.urbe.edu. [En línea] 2002. https://virtual.urbe.edu/tesispub/0091897/cap02.pdf.

itdatum. 2021. itdatum.com. [En línea] 2021. https://itdatum.com/ciberseguridad_para_empresas_en_peru/.

Kajtazi, Milos Zec and Miranda. 2015. books.google. [En línea] 2015. https://books.google.com.pe/books?hl=es&lr=&id=zyNoCwAAQBAJ&oi=fnd&pg=PA231&dq=Cyber+attacks+on+SMEs&ots=nKcMf32V-X&sig=pP_BpDevuM-wvI4OTPjGhtIMu8A#v=onepage&q=Cyber%20attacks%20on%20SMEs&f=false.

Kaspersky. 2022. [En línea] 2022. https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/.

kaspersky. 2022. kaspersky. [En línea] 2022. https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/.

moneseguros. 2022. moneseguros. [En línea] 2022. https://moneseguros.com/blog/tipos-ciberataque-empresa.

peru21. 2022. peru21.pe. [En línea] 2022. https://peru21.pe/cheka/tecnologia/digitalizacion-ciberseguridad-pymes-como-digitalizar-una-pyme-cinco-aspectos-a-considerar-para-mantenerse-en-la-competencia-noticia/.

piranirisk. 2022. piranirisk. [En línea] 2022. https://www.piranirisk.com/es/blog/ciberataques-pymes-latinoamericanas.

—. 2022. piranirisk. [En línea] 2022. https://www.piranirisk.com/es/blog/ciberataques-pymes-latinoamericanas.

—. 2022. piranirisk.com. [En línea] 2022. https://www.piranirisk.com/es/blog/marco-ciberseguridad-nist-que-es#:~:text=El%20Marco%20de%20Ciberseguridad%20o,adopci%C3%B3n%20voluntaria%2C%20ofrece%20diferentes%20ventajas..

pmg-ssi. 2021. pmg-ssi. [En línea] 2021. https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/#:~:text=La%20metodolog%C3%ADa%20NIST%20SP800%2D30%20est%C3%A1%20compuesta%20por%20nueve%20fases,de%20motivaci%C3%B3n%20de%20las%20mismas..

pressperu. 2121. pressperu.com. [En línea] 2121. https://pressperu.com/las-pymes-ya-no-consideran-la-ciberseguridad-algo-complementario/.

rrhhdigital. 2022. rrhhdigital. [En línea] 2022. https://www.rrhhdigital.com/secciones/pymes/153261/Los-ciberataques-a-pymes-crecen-en-2022.

ruralvia. 2022. ruralvia. [En línea] 2022. https://blog.ruralvia.com/ciberataques-mas-populares-en-empresas/.

tarlogic. 2022. tarlogic.com. [En línea] 2022. https://www.tarlogic.com/es/blog/guias-nist-ciberseguridad/.

welivesecurity. 2021. welivesecurity. [En línea] 2021. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf.

zendesk. 2020. zendesk. [En línea] 2020. https://www.zendesk.com.mx/blog/que-es-escala-de-likert/#:~:text=La%20escala%20de%20likert%20es,s%C3%AD%E2%80%9D%20o%20%E2%80%9Cno%E2%80%9D.

ANEXOS

Anexo 1: Matriz De Consistencia

MATRIZ DE CONSISTENCIA										
TITULO	Pregunta General	Objetivo General	Preguntas Especificas	Objetivos Específicos	VARIABLE	Definición Conceptual	Definición operacional	Dimensiones	Indicador	Escala de medición
Propuesta metodológica para mitigar los riesgos sobre ciberataques a PYMES, usando la METODOLOGÍA NIST	¿De qué manera los riesgos de ciberataques a PYMES se mitigan usando una metodología basada en Nist?	Aplicar una propuesta para mitigar los riesgos que generan los ciberataques en las pymes.	¿Cuáles son los problemas de la gestión de la ciberseguridad en la Pymes? ¿Cómo mitigar los riesgos de los ciberataques en las pymes?	Identificar los distintos tipos de ciberataques a las pymes. Clasificar los distintos ataques con mayor impacto a pymes. Mitigación de riesgos asociados a	Ciberataques a pymes.	Acción de impulsar la implantación de la normativa sobre la protección de infraestructuras críticas y de las capacidades necesarias para la protección de los servicios esenciales (Presidencia del gobierno de España, 2013)	Los datos son obtenidos a través de diversas técnicas e instrumentos de recolección de información tales como la técnica de encuesta, y antecedentes de Frecuencia de Ataques Cibernéticos anuales.	Nivel de Ciberseguridad	Nivel de afectación Vulnerabilidades detectadas Vulnerabilidades tratadas Conocimiento	Razón / Continua

				los ciberataques.	Metodología NIST	Es fundamental que las organizaciones tengan en cuenta esta metodología para proteger su información, debido a que actualmente es la que más trascendencia tiene, inclusive tenemos la posibilidad de nombrar que la organización no solo debería proteger su capital, sino también la información como un bien de la compañía por esa razón debería ser completa la información, disponible para los individuos correctos y lo	Este marco de ciberseguridad consta de 5 funciones: 1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar	Rendimiento	Controles aplicados	Razón / Continua

						más relevante confidencial. (Roxana & Yesenia, 2013).				

Anexo 2. Indicadores de variables

OBJETIVO ESPECÍFICO	INDICADOR	DESCRIPCIÓN	TÉCNICA / INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CÁLCULO
Identificar los distintos tipos de ciberataques a las pymes.	Nivel de afectación	Nivel de afectación de los ataques cibernéticos a pymes.	Encuestas y/o antecedentes.	1 mes	Evaluación según el criterio del investigador. Se mide en una escala de Likert que va desde Totalmente en desacuerdo, En desacuerdo, Ni poco, ni mucho, De acuerdo y Totalmente de acuerdo
Clasificar los distintos ataques con mayor impacto a pymes	Vulnerabilidades detectadas	Según la clasificación de los distintos ataques, se verá que vulnerabilidades son detectadas en las pymes.	Encuestas y/o antecedentes.	1 mes	Evaluación según el criterio del investigador. Se mide en una escala de Likert que va desde Totalmente en desacuerdo, En desacuerdo, Ni poco, ni mucho, De acuerdo y Totalmente de acuerdo
Mitigar los riesgos de los ciberataques a las pymes.	Vulnerabilidades tratadas	Calcular el tiempo en el cual se puede mitigar los riegos de un ataque cibernético a pyme.	Encuestas y/o antecedentes.	1 mes	Evaluación según el criterio del investigador. Se mide en una escala de Likert que va desde Totalmente en desacuerdo, En desacuerdo, Ni poco, ni mucho, De acuerdo y Totalmente de acuerdo
Generar una propuesta de solución para combatir los ataques cibernéticos a las pymes.	Controles aplicados	Es lo que aplicaremos para detectar si hay cambio o no.	Encuestas y/o antecedentes.	1 mes	Obtenidos mediante la evaluación según el criterio del investigador, para concretar el resultado final.

Fuente: Elaboración propia de los autores.

Anexo 3. Matriz de operacionalización de variables

VARIABLE DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN	COMO MEDIRLO	TÉCNICA/ INSTRUMENTO
Ciberseguridad	La acción consiste en fomentar la implementación de regulaciones relacionadas con la protección de infraestructuras críticas, así como promover el desarrollo de habilidades básicas para garantizar la seguridad de los servicios esenciales.(Presidencia del gobierno de España, 2013)	La información se recopila utilizando distintas técnicas e instrumentos de recolección de datos, como encuestas y análisis de antecedentes sobre la frecuencia de ataques cibernéticos en años anteriores.	Nivel de Ciberseguridad	Nivel de afectación	Ordinal	Escala de Likert	Encuesta
				Vulnerabilidades detectadas	Ordinal	Escala de Likert	
				Vulnerabilidades tratadas			

VARIABLE DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN	COMO MEDIRLO	TÉCNICA/ INSTRUMENTO
Metodología NIST	Es fundamental que las orgEs fundamental que las organizaciones tengan en cuenta esta metodología para proteger su información, debido a que actualmente es la que más trascendencia tiene, inclusive tenemos la posibilidad de	Este marco de ciberseguridad consta de 5 funciones: 1. Identificar 2. Proteger 3. Detectar 4. Responder 5. Recuperar	Nivel de Ciberseguridad	Controles aplicados	Ordinal	Escala de Likert	Encuesta
			Rendimiento				

	nombrar que la organización no solo debería proteger su capital, sino también la información como un bien de la compañía por esa razón debería ser completa la información, disponible para los individuos correctos y lo más relevante confidencial. (Roxana & Yesenia, 2013).						

Anexo 4. Instrumento de recolección de datos – Encuesta

<table>
<tr><th colspan="5">Ficha de registro determinar el nivel ciberseguridad en la que se encuentra la empresa</th></tr>
<tr><td>Investigadores</td><td colspan="2">Berrú Escajadillo Sergio André
Yarleque Golles Luis Fernando</td><td>Tipo de prueba</td><td>Aplicada</td></tr>
<tr><td>Institución</td><td colspan="4">Universidad Privada César Vallejo</td></tr>
<tr><td>Dimensión</td><td colspan="4">Nivel de Ciberseguridad</td></tr>
<tr><td>Fecha de Inicio</td><td colspan="2">02/10/2022</td><td>Fecha final</td><td>16/12/2022</td></tr>
<tr><th>Variable</th><th colspan="2">Indicador</th><th colspan="2">Técnica</th></tr>
<tr><td>Ciberataques a pymes</td><td colspan="2">● Nivel de afectación
● Vulnerabilidades detectadas
● Vulnerabilidades tratadas</td><td colspan="2">● Encuesta</td></tr>
</table>

Item	Preguntas	Valoración	Nivel	Resultado
Nivel de afectación				
1	¿Conoce los pasos que el departamento de Tecnología de la Información (TI) sigue para recuperarse después de sufrir un ataque o evento cibernético?			
2	¿Comprende la importancia de que una empresa tenga un Plan de Contingencia y Continuidad de Negocio?			
3	¿Conoce si la pyme ha sido víctima de ataques cibernéticos			

	y/o robo de información?			
Vulnerabilidades detectadas				
5	¿Conoce las medidas de control que debe tomar en caso de detectar actividades inusuales en alguno de los dispositivos electrónicos asignados por la pyme			
6	¿Consideran que la capacitación y concientización sobre ciberseguridad es una prioridad en su empresa para reducir las vulnerabilidades detectadas?			

7	¿Cuentan con políticas y procedimientos claros para abordar las vulnerabilidades detectadas en materia de ciberseguridad?			
8	¿Conoce si la pyme tiene un plan y herramientas de detección para prevenir posibles ataques cibernéticos de forma anticipada?			
Vulnerabilidades tratadas				
9	¿Conoce si la empresa cuenta con algún repositorio dónde usted pueda acceder e informarse sobre los tipos de			

	ataques cibernéticos, suplantaciones de identidad (phishing), etc.?			
10	¿Crees que es necesario tener bloqueados los puertos USB de tu laptop y/o PC?			
11	¿Tienes confianza en que el equipo de Soporte de TI cuenta con personal capacitado que realiza revisiones adecuadas para prevenir futuros ataques cibernéticos?			
12	¿Conoce las herramientas de			

	supervisión utilizadas para identificar ataques informáticos en una pyme?			
Conocimiento				
13	¿Está informado/a sobre si su empresa tiene algún programa de capacitación para prevenir convertirse en víctima de ataques cibernéticos?			
14	¿Tiene conocimiento de algún programa de concienciación sobre ciberseguridad que su pyme haya llevado a cabo?			

15	¿Está informado/a con los controles utilizados para acceder a las instalaciones de la pyme?			
16	¿Está informado/a si la pyme tiene un plan destinado a mejorar la detección de ataques cibernéticos?			

Fuente: Elaboración propia del autor

Ficha de registro determinar el nivel de confianza en la que se encuentra ante la empresa				
Investigadores		Berrú Escajadillo Sergio André Yarleque Golles Luis Fernando	**Tipo de prueba**	Aplicada
Institución		Universidad Privada César Vallejo		
Dimensión		Nivel de Ciberseguridad		
Fecha de Inicio		14/01/2023	**Fecha final**	14/05/2023
Variable		**Indicador**	**Técnica**	
Metodología NIST		● Controles Aplicados	● Encuesta	
Item	**Preguntas**	**Valoración**	**Nivel**	**Resultado**
Controles Aplicados				
1	**¿Qué tan satisfecho(a) está con la efectividad de mitigación de riegos ante**			

	ciberataques guiándose de la metodología NIST?			
2	**¿Qué tan satisfecho(a) está con la experiencia de la simulación implementada?**			

Fuente: Elaboración propia del autor

Anexo 5. Carta de autorización

CARTA DE AUTORIZACION DE USO DE INFORMACIÓN DE EMPRESA

Yo JOSE ALBERTO BERRU GUERRERO, identificado con el DNI 02621749, en mi calidad de GERENTE GENERAL de la empresa Think Solutions con R.U.C N° 20602772625, ubicada en la ciudad de Piura.

OTORGO LA AUTORIZACIÓN,

A los señores BERRU ESCAJADILLO SERGIO ANDRE, identificado con el DNI N° 74301581, y YARLEQUE GOLLES LUIS FERNANDO, identificado con el DNI N° 75537311, estudiantes del decimo semestre de la carrera profesional de Ingeniería de Sistemas de la Universidad César Vallejo filial Piura, para que utilice la siguiente información necesaria de la empresa con la finalidad de que pueda desarrollar su Trabajo de Investigación para optar al grado de Bachiller. Confidencial.

Firma y sello del Representante Legal de la empresa.

El Egresado/Bachiller declara que los datos emitidos en esta carta y en el trabajo de Investigación, en la Tesis son auténticos.

Firma y sello del Egresado.
YARLEQUE GOLLES LUIS FERNANDO

Firma y sello del Egresado.
BERRU ESCAJADILLO SERGIO ANDRE

Piura, 20 de mayo del 2023

Anexo 6. Contrato de confidencialidad

CONTRATO DE CONFIDENCIALIDAD, TRATAMIENTO Y PROTECCION DE DATOS

Este contrato de Confidencialidad, Tratamiento y Protección de Datos (en adelante, el "Contrato") se realiza entre:

Berru Escajadillo Sergio André identificado con el DNI N° 74301581, y YARLEQUE GOLLES LUIS FERNANDO, identificado con el DNI N° 75537311, estudiantes del ultimo semestre de la carrera profesional de Ingeniería de Sistemas en la Universidad Cesar Vallejo filial Piura (en adelante, "El Investigador"), por una parte, y la empresa Think Solutions con R.U.C N° 20602772625(en adelante, "La Empresa"), por otra parte.

Ambas partes, conjuntamente conocidas como "Las Partes".

CONSIDERANDO:

1. El Investigador esta llevando a cabo una tesis de investigación que implica la utilización de instrumentos y metodologías desarrolladas por él/ella misma en La Empresa.
2. La Empresa posee información y datos de carácter confidencial relacionados con su actividad y operaciones comerciales, que deben ser protegidos adecuadamente.
3. Las Partes desean establecer los términos y condiciones para garantizar la confidencialidad, tratamiento y protección de datos y la información relevante en la relación con la ejecución de la tesis en La Empresa.

Por lo tanto, ambas partes acuerdan comprometerse a mantener en estricta confidencialidad toda la información y datos proporcionados por La Empresa, ya sea verbalmente, por escrito, electrónicamente o en cualquier otro formato, que sean considerados como confidenciales.

Anexo 7. TABLA DE VALIDACIÓN DEL INSTRUMENTO DE EXPERTOS:

TITULO DE TESINA

Propuesta metodológica para mitigar los riesgos sobre ciberataques a PYMES, usando la METODOLOGIA NIST

Nombre del experto:

Ing. Romero Nishiki Hernán Rafael

Berru Escajadillo, Sergio André

Yarleque Golles, Luis Fernando

Mediante la tabla de evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con "X" en las columnas de SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre el control de inventario dirigido a emprendedores.

		APRECIA		
ITEMS	PREGUNTAS	SI	NO	OBSERVACIONES
1	¿El instrumento de medición cumple con el diseño adecuado?	X		
2	¿El instrumento de recolección de datos tiene relación con el título de investigación?	X		
3	¿En el instrumento de recolección de datos se mencionan las variables de investigación?	X		
4	¿En el instrumento de recolección de datos, facilitara el logro de los objetivos de la investigación?	X		
5	¿El instrumento de recolección de datos se relaciona con las variables de estudio?	X		
6	¿La redacción de las preguntas es con sentido coherente?	X		
7	¿Cada una de las preguntas del instrumento de medición, se relacionan con cada uno de los elementos de los indicadores?	X		
8	¿El diseño del instrumento de medición facilitará el análisis y procesamiento de datos?	X		
9	¿Del instrumento de medición, son entendibles sus alternativas de respuesta?	X		
10	¿El instrumento de medición será accesible a la población sujeto a estudio?	X		
11	¿El instrumento de medición es clara, precisa, y sencilla para que contestes y de esa manera obtener los datos requeridos?	X		
	TOTAL	11		

SUGERENCIAS:

.....

Firma de experto:

TITULO DE TESINA

Propuesta metodológica para mitigar los riesgos sobre ciberataques a PYMES, usando la METODOLOGIA NIST

Nombre del experto:

Ing. Romero Nishiki Hernán Rafael

Berru Escajadillo, Sergio André

Yarleque Golles, Luis Fernando

Mediante la tabla de evaluación de expertos, usted tiene la facultad de evaluar cada una de las preguntas marcando con "X" en las columnas de SI o NO. Asimismo, le exhortamos en la corrección de los ítems indicando sus observaciones y/o sugerencias, con la finalidad de mejorar la coherencia de las preguntas sobre el control de inventario dirigido a emprendedores.

ITEMS	PREGUNTAS	SI	NO	OBSERVACIONES
1	¿Qué tan satisfecho(a) está con la efectividad de mitigación de riegos ante ciberataques guiándose de la metodología NIST?	X		
2	¿Qué tan satisfecho(a) está con la experiencia de la simulación in	X		
	TOTAL	2		

SUGERENCIAS:

.....

Firma de experto:

Anexo 8. Figuras referencias:

La situación problemática según antecedentes ESET aplico un reporte de seguridad en donde las PYMES de Latinoamérica EN EL 2021 se ven afectadas, entre ellas se encuentra Perú con un 8.9%.

Infecciones de malware por país

Ilustración 14. Infecciones de malware por país

Fuente: (ESET_security_report_LATAM2022).

Asimismo, se aplicó otro reporte por ESET sobre ciberataques de códigos espías maliciosos (SPYWARE) en el 2022, el país más afectado es Perú con el 40%.

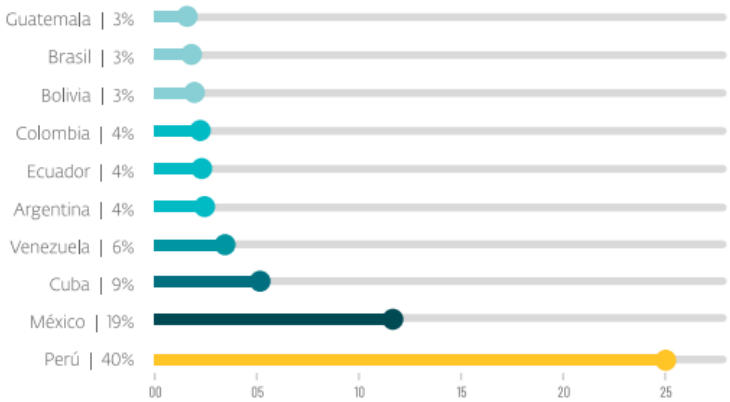

Ilustración 15. Ciberataques de códigos espías maliciosos (SPYWARE)

Fuente: (ESET_security_report_LATAM2022).

Las vulnerabilidades mediante TROYANOS dejan a Perú en tercer puesto de vulnerables antes estos ataques en países Latinoamericanos.

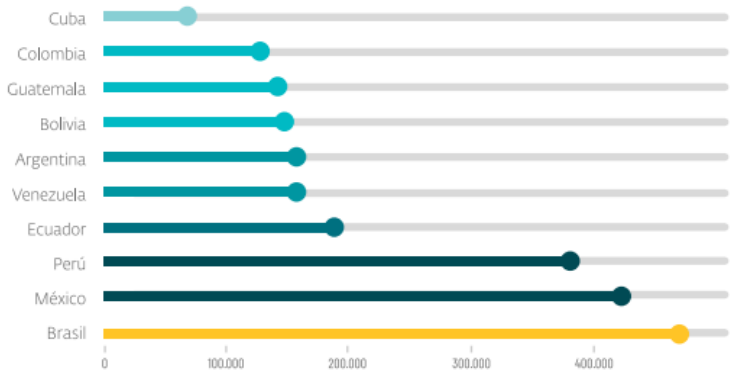

Ilustración 16. TROYANOS: AMENAZAS EN AMENAZAS

Fuente: (ESET_security_report_LATAM2022).

Por lo que también es importante analizar y conocer la situación que presenta nuestro país ante la ciberseguridad. Por ejemplo, en el diario “El Peruano”, se puede observar una publicación del presente año 2022, donde se muestran que las Pymes sufren mucho de ciberataques

Ilustración 17. Noticias actuales sobre ciberataques a pymes.

Fuente: (El_Peruano_Diario_Oficial_Del_Bicentenario).

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, TAVARA RAMOS ANTHONY PAUL, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - PIURA, asesor de Tesis titulada: "Propuesta Metodológica para mitigar los Riesgos sobre Ciberataques a Pymes, usando la Metodología NIST", cuyos autores son BERRU ESCAJADILLO SERGIO ANDRE, YARLEQUE GOLLES LUIS FERNANDO, constato que la investigación tiene un índice de similitud de 18.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

PIURA, 26 de Junio del 2023

Apellidos y Nombres del Asesor:	**Firma**
TAVARA RAMOS ANTHONY PAUL **DNI:** 40784283 **ORCID:** 0000-0002-4159-930X	Firmado electrónicamente por: ATAVARAR el 05-07-2023 11:22:58

Código documento Trilce: TRI - 0551673

INVESTIGA UCV