UNIVERSIDAD AUTÓNOMA DE CIUDAD JUÁREZ

Instituto de Ingeniería y Tecnología

Departamento de Ingeniería Eléctrica y Computación

FRAMEWORK DE CIBERSEGURIDAD PARA PYMES

Reporte Técnico de Investigación presentado por:

Eduardo Santana Valverde Guereca 167975

Requisito para la obtención del título de:

INGENIERO EN SISTEMAS COMPUTACIONALES

ASESOR:

Dr. Víctor Manuel Morales Rocha

Mtro. Adrian Hernandez Rivas

Ciudad Juárez, Chihuahua 11 de noviembre de 2024

Ciudad Juárez, Chihuahua, a 11 de Noviembre de 2024

Asunto: Liberación de Asesoría

Dra. Nelly Gordillo Castillo
Jefa del Departamento de Ingeniería
Eléctrica y Computación
Presente.-

Por medio de la presente me permito comunicarle que, después de haber realizado las asesorías correspondientes al reporte técnico FRAMEWORK DE CIBERSEGURIDAD PARA PYMES, del alumno Eduardo Santana Valverde Guereca de la Licenciatura en Ingeniería en Sistemas Computacionales, considero que lo ha concluido satisfactoriamente, por lo que puede continuar con los trámites de titulación intracurricular.

Sin más por el momento, reciba un cordial saludo.

Atentamente:

Dr. Víctor Manuel Morales Rocha

Profesor Investigador

Ccp: Dr. Josué Domínguez Guerrero
Coordinador del Programa de Sistemas Computacionales
Eduardo Santana Valverde Guereca
Archivo

Ciudad Juárez, Chihuahua, a 11 de Noviembre de 2024

Asunto: Autorización de publicación

C. Eduardo Santana Valverde Guereca

Presente.-

En virtud de que cumple satisfactoriamente los requisitos solicitados, informo a usted que se autoriza la publicación del documento de FRAMEWORK DE CIBERSEGURIDAD PARA PYMES, para presentar los resultados del proyecto de titulación con el propósito de obtener el título de Licenciado en Ingeniería en Sistemas Computacionales.

Sin otro particular, reciba un cordial saludo.

Dr. Gilberto Rivera Zarate

Profesor Titular de Seminario de Titulación II

Declaración de Originalidad

Yo, Eduardo Santana Valverde Guereca declaro que el material contenido en esta publicación fue elaborado con la revisión de los documentos que se mencionan en el capítulo de Bibliografía, y que la solución obtenida es original y no ha sido copiada de ninguna otra fuente, ni ha sido usada para obtener otro título o reconocimiento en otra institución de educación superior.

Eduardo Santana Valverde Guereca

Agradecimientos

[Sustituye este texto escribiendo tus agradecimientos. La sección de agradecimientos reconoce la ayuda de personas e instituciones que aportaron significativamente al desarrollo de la investigación. No te debes exceder en los agradecimientos; agradece sólo las contribuciones realmente importantes, las menos importantes pueden agradecerse personalmente. El nombre de la agencia que financió la investigación y el número de la subvención deben incluirse en esta sección. Generalmente no se agradecen las contribuciones que son parte de una labor rutinaria o que se reciben a cambio de pago.

Las contribuciones siguientes ameritan un agradecimiento pero no justifican la coautoría del artículo: ayuda técnica de laboratorio, préstamo de literatura y equipo, compañía y ayuda durante viajes al campo, asistencia con la preparación de tablas e ilustraciones o figuras, sugerencias para el desarrollo de la investigación, ideas para explicar los resultados, revisión del manuscrito y apoyo económico".]

Dedicatoria

[Aquí escribe tu dedicatoria.]

Resumen

El presente proyecto de titulación comprende el desarrollo de un Framework de ciberseguridad para las pequeñas y medianas empresas, esto debido a la necesidad de brindar medidas de protección ante los riesgos de amenazas digitales. El Framework consiste en seguir una metodología de cascada para implementar soluciones de seguridad utilizando controles apegados bajo las directrices de las PYMES.

Palabras claves: PYMES, ciberseguridad, Framework

Índice general

Índice de figuras

Índice de tablas

Introducción

La falta de conciencia en seguridad digital, junto a la carencia de recursos y protocolos de protección adecuados, son algunos elementos que hacen que las pequeñas y medianas empresas (PYMES) sean vulnerables a las amenazas digitales. En la actualidad, estas amenazas se han vuelto más frecuentes debido al creciente uso de tecnologías digitales por parte de las empresas. Por lo tanto la ciberseguridad es importante porque es una medida para proteger la información sensible y los activos de las empresas. En las PYMES, sin medidas de ciberseguridad adecuadas, están en riesgo de sufrir robos de datos, interrupciones en sus servicios, o incluso pérdidas económicas que pueden afectar su estabilidad y reputación en el mercado.

En la Figura 1, se muestra el indice por país de ataques de ransomware en 2024, uno de los ataques digitales mas comunes y graves porque no solo interrumpe los servicios de la empresa sino que también roba información confidencial.

Las empresas de mayor tamaño suelen contar con recursos económicos y tecnológicos que les permiten implementar soluciones avanzadas de ciberseguridad, contratar personal especializado y establecer protocolos de protección robustos, por otro lado las PYMES enfrentan limitaciones en estos aspectos, los recursos, así como la falta de conciencia en ciberseguridad,las hace más vulnerables [2]. Basado en esto, se pretende ofrecer una solución de ciberseguridad mediante el desarrollo de un marco de trabajo (Framework) para apoyar a las PYMES a protegerse ante las amenazas digitales.

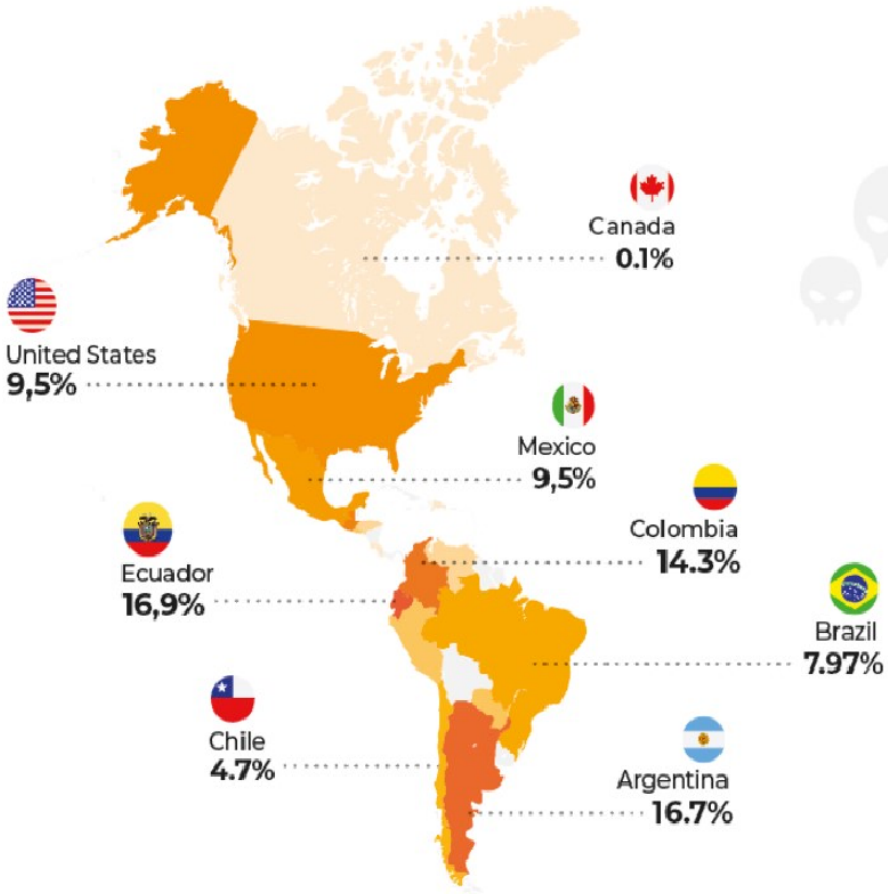

Figura 1: Detección de ataques de ransomware *BlackSuit* por país, en 2024 [1].

Los siguientes capítulos del presente trabajo están organizadas de la siguiente manera: en el Capítulo 1 se presenta el planteamiento del problema, que comprende los antecedentes, los objetivos del proyecto, la justificación, así como los alcances y limitaciones. El Capítulo 2 presenta el marco teórico, que muestra la información que fue necesaria investigar, creando bases sólidas para el desarrollo del Framework. El Capítulo 3 describe el desarrollo del proyecto, que incluye la propuesta de solución y la metodología. Los resultados y discusiones se encuentran en el Capítulo 4, donde se analizan los efectos de la aplicación del Framework. Finalmente, en el Capítulo 5 se presentan las conclusiones, en las que se evalúa el cumplimiento del objetivo.

Capítulo 1
Planteamiento del Problema

En el primer Capítulo se presenta de manera detallada la investigación realizada para reunir las bases y los datos necesarios para el desarrollo del proyecto. Se llevó a cabo un análisis de los antecedentes relacionados con el proyecto, así como la definición del problema, la descripción de los objetivos, tanto general como específico, la justificación y los alcances y limitaciones.

1.1. Antecedentes

Los Frameworks son estructuras conceptuales que proporcionan una base sólida para desarrollar y estructurar soluciones en áreas específicas, facilitando las tareas de quienes los utilizan [3]. En el ámbito de la ciberseguridad, los Frameworks ofrecen un conjunto de directrices, herramientas y buenas prácticas diseñadas para identificar, evaluar y gestionar riesgos de seguridad de manera efectiva.

Saeed et al. [4], presentan un Framework de cuatro niveles, diseñado para guiar la preparación en ciberseguridad de las organizaciones durante la transformación digital. Este modelo enfatiza la necesidad de comenzar con evaluaciones de seguridad básicas y progresar hacia políticas estratégicas y medidas preventivas avanzadas, como las pruebas de penetración y el escaneo de vulnerabilidades.

Complementando este enfoque, Bruno Azinheira et al. [5], introducen una metodología enfocada en PYMES en Portugal, la cual mapea las capacidades mínimas de ciberseguridad requeridas (RMCSC), alineándolas con la norma ISO 27001:2013. Esta metodología sigue una estructura de tres fases que permite a las PYMES evaluar sus capacidades de ciberseguridad y prepararse para la autoevaluación, construyendo una base sólida para la implementación de buenas prácticas. Asimismo, Miguel Angel López et al. [6], abordan la protección de las PYMES frente a ataques digitales complejos como DDoS, SQLi y DGA, aplicando tecnologías de Machine Learning y blockchain para desarrollar una arquitectura de seguridad robusta. Aunque los resultados iniciales son satisfactorios, este estudio destaca la importancia de emplear tecnología avanzada para enfrentar amenazas sofisticadas. Aunque estas soluciones son especialmente para PYMES, su implementación puede resultar compleja y demandante en términos de recursos y tiempo.

Adicionalmente, Arunabha Mukhopadhyay et al. [7], proponen un Framework específico para combatir el ransomware, el Modelo de Gestión de Riesgos de Ransomware (RRRM), que abarca desde la evaluación hasta la mitigación de riesgos. Este enfoque ofrece una herramienta integral que, en conjunto con los estudios anteriores, permite a las organizaciones no solo establecer medidas de ciberseguridad básicas, sino también fortalecer su capacidad de respuesta ante amenazas específicas como el ransomware.

Finalmente, Muriel Figueredo Franco et al. [8], presentan el Framework SECProject, que se estructura en seis pilares y cubre desde la identificación de necesidades hasta la ejecución de estrategias en ciberseguridad.

A pesar de los beneficios que ofrecen estos Frameworks, pueden requerir inversiones en tecnologías de seguridad avanzadas; estos componentes suelen ser costosos y a veces inaccesibles para muchas PYMES.

1.2. Definición del problema

Las PYMES se encuentran vulnerables debido a su escasa capacidad de inversión en recursos y personal especializado en ciberseguridad. Según datos de la empresa de seguridad Kaspersky, el 77 % de las empresas ha experimentado al menos una violación de ciberseguridad en los últimos años [9]. El 68 % de los incidentes se originaron por errores humanos, como la descarga de malware, el uso de contraseñas débiles, la visita a sitios web no seguros y la utilización de sistemas no autorizados para compartir datos. Estas cifras evidencian la falta de concienciación del personal en cuanto a los riesgos cibernéticos, lo que hace a estas empresas más susceptibles a ataques de malware, phishing, ransomware y otras amenazas cibernéticas. Muchas empresas subestiman los riesgos cibernéticos o asumen erróneamente que son demasiado pequeñas para ser blanco de ataques cibernéticos. Esto acción puede alentar a los ciberdelincuentes y dejar a la empresa vulnerable, con consecuencias devastadoras, como brechas de datos, pérdida de reputación y pérdidas financieras que pueden ascender hasta los US$155 mil dólares en un solo ataque [10].

La carencia de Frameworks de ciberseguridad que proporcionen directrices ajustadas a la escala y recursos de las PYMES, impide que estas adopten las mejores prácticas para hacer frente a las amenazas que ponen en riesgo la confidencialidad, integridad y privacidad de sus datos. Este problema es relevante en un mundo cada vez más interconectado y digitalizado, donde las empresas, enfrentan constantes desafíos de seguridad cibernética.

1.3. Objetivo general

Desarrollar un Framework de ciberseguridad para pequeñas y medianas empresas, mediante el uso de políticas y controles de estándares internacionales de ciberseguridad, que permitan proteger la integridad y confidencialidad de los datos dentro de estas organizaciones.

1.3.1. Objetivos específicos

- Realizar un análisis de las características de las PYMES para definir las soluciones a implementar.
- Diseñar la arquitectura del Framework para tener una visión general.
- Elaborar plantillas para la correcta implementación del Framework, incluyendo ejemplos de mejores prácticas basados en los estándares internacionales de ciberseguridad.
- Desarrollar un caso de uso mediante la simulación de una PYME para probar el Framework.

1.4. Justificación

Es pertinente abordar la seguridad cibernética para las PYMES debido a su relevancia económica. Según datos de la Organización Mundial del Comercio (WTO, por sus siglas en inglés), las PYMES representan más del 90 % del total de las empresas a nivel mundial, contribuyendo al crecimiento económico [11]. En México, existen alrededor de 4 millones de PYMES que generan 7 de cada 10 empleos formales y aproximadamente el 50 % del Producto Interno Bruto [12]. Sin embargo, estas empresas están expuestas ante la ciberdelincuencia; solo en 2022, México reportó 323,434 detecciones de ataques digitales [10]. Esta cifra resalta la urgencia de proteger a las PYMES, pero en ocasiones carecen de los recursos y la experiencia necesarios para protegerse. Según el estudio de Marsh, el 43 % de las empresas encuestadas indicó que la ciberseguridad es una de las principales preocupaciones de las PYMES [13]. A pesar de ello, en ocasiones se opta por no implementar ninguna medida de seguridad debido a la complejidad de las soluciones de seguridad disponibles, que por lo general son diseñadas para las grandes empresas, esto deja a las PYMES expuestas a riesgos.

Por lo tanto, este trabajo contribuirá al diseño e implementación de un Framework de ciberseguridad específicamente adaptado para las PYMES, lo cual es fundamental, ya que ayudará a proteger los activos y la información confidencial de estas empresas frente a ataques digitales, evitando así pérdidas financieras y daños a su reputación. Además, fortalece la capacidad de las PYMES de protegerse frente a las amenazas cibernéticas, lo que les permite continuar operando de manera segura y eficiente.

1.5. Alcances y limitaciones

Alcances:

- Se llevará a cabo una investigación detallada sobre las demandas de seguridad cibernética de las pequeñas y medianas empresas, identificando las amenazas y vulnerabilidades prevalentes del entorno empresarial.
- El diseño está orientado para las pequeñas y medianas empresas debido a su limitada capacidad que tienen para invertir en sistemas costosos.
- Se realizarán pruebas para asegurar la eficacia de las medidas de ciberseguridad.

Limitaciones:

- El Framework está orientado a PYMES que se ajusten a las características de las mismas.

Capítulo 2
Marco Teórico

A continuación, se proporciona el fundamento conceptual más importante de la propuesta, que a su vez brinda validez a la investigación.

2.0.1. Ciberseguridad

La ciberseguridad consiste en proteger sistemas, redes y programas contra amenazas digitales [14]. Por lo general, las amenazas buscan acceder, modificar o eliminar información confidencial, extorsionar a los usuarios o interrumpir la continuidad del negocio. Esto destaca lo fundamental que es asegurar que la información y los servicios críticos para individuos, empresas y organizaciones estén protegidos en cuanto a su confidencialidad, integridad y disponibilidad.

2.0.2. Pequeñas y medianas empresas

En términos de tecnología [15], las pequeñas y medianas empresas (PYMES), se refieren a entidades que pueden no estar formalmente constituidas como empresas pero se caracterizan por tener un número reducido de empleados y un volumen de ingresos moderado que operan con recursos limitados. Cualquier emprendimiento o actividad económica constante puede ca-

lificarse como PYME, ya que el factor determinante es la actividad económica y no la estructura jurídica. Esto incluye a trabajadores autónomos, empresas familiares, asociaciones, sociedades y cualquier otra entidad que realice una actividad económica de manera regular. En términos de infraestructura cada empresa puede variar dependiendo del tamaño y la cantidad de empleados. En general, algunas consideraciones comunes incluyen que una PYME podría tener entre 1 y 50 computadoras o más, dependiendo de su escala y crecimiento, al menos 1 o 2 switches para conectar todas las computadoras y otros dispositivos y 1 router principal para la conexión a internet y, en algunos casos, routers adicionales para segmentar la red.

2.0.3. Tipos de amenazas a la ciberseguridad.

Malware. De acuerdo con McAfee [16], el malware, es un tipo de programa informático malicioso creado con el objetivo de infectar y dañar el sistema de un usuario legítimo. El malware se infiltra en las redes aprovechando vulnerabilidades. Los criminales cibernéticos suelen emplearlo para obtener información que luego utilizan para extorsionar a sus víctimas y así obtener beneficios financieros. Esta información puede incluir datos financieros, historiales médicos, correos electrónicos personales y contraseñas. La variedad de información que puede ser comprometida es cada vez mayor.

Phishing. Como señala Cisco [17], el phishing es el tipo de ataque cibernético más frecuente, comúnmente los cibercriminales lo utilizan para enviar correos electrónicos fraudulentos que parecen provenir de fuentes confiables con el fin de obtener información confidencial, como los números de tarjetas de crédito y datos de acceso. Esta amenaza utiliza técnicas de ingeniería social para engañar a los usuarios y hacer que revelen información personal. Según Kaspersky, en 2023 se registraron 286 millones bloqueos de intento de phishing en el último año, lo que representa un aumento del 617 % en comparación con los 12 meses anteriores y un promedio de 544 ataques por minuto.

En la Figura 2.1, se muestra un mapa de los países mas afectados correspondiente a mensajes falsos.

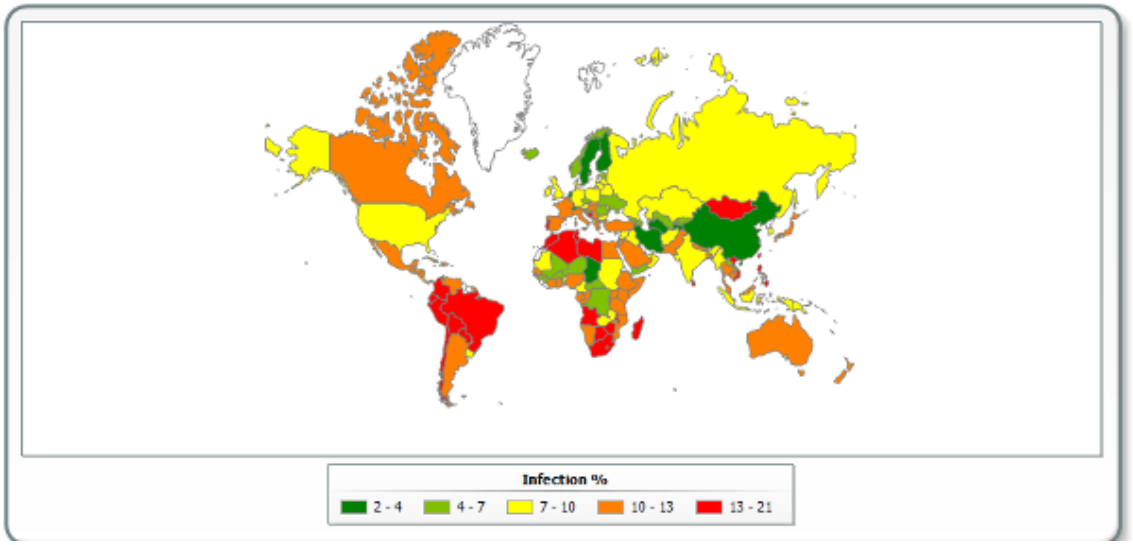

Figura 2.1: Mapa de los países mas atacados por mensajes falsos [18].

Ransomware. Según IBM [19], el ransomware es una forma de software malicioso que bloquea los datos o dispositivos de una persona y la amenaza con mantenerlos bloqueados a menos que pague un rescate al atacante. El pago del rescate no garantiza que se recuperen los archivos o se restaure el sistema. El 17 por ciento de todos los ataques digitales en 2022 fueron perpetrados mediante ransomware [20].

En la Figura 2.2, se presenta una gráfica de X-Force, donde realizó un análisis de los ataques de ransomware entre 2022 y 2023 para determinar si hubo cambios en el tiempo que tarda un atacante en ejecutar un ataque de ransomware. La duración promedio de un ataque de ransomware empresarial (es decir, el tiempo entre el acceso inicial y la implementación del ransomware) se redujo levemente a 92.21 horas (3.84 días) en 2023 desde 92.48 horas (3.85 días) en 2022.

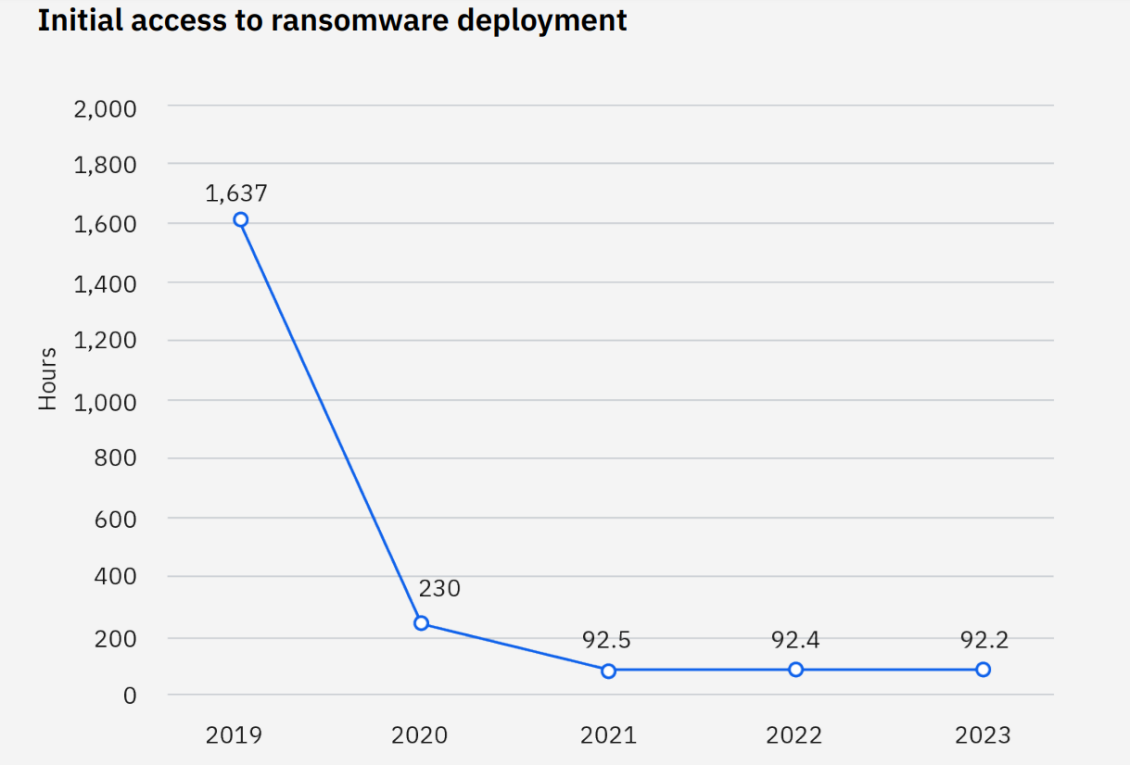

Figura 2.2: Tiempo entre el acceso inicial y el ransomware [21].

2.0.4. Concienciación en ciberseguridad

La formación y concienciación en ciberseguridad se refiere a un conjunto de acciones y prácticas diseñadas para que los usuarios conozcan y pongan en práctica una serie de iniciativas para contribuir a garantizar la seguridad de una organización. La sensibilización en ciberseguridad desempeña un papel crucial en la manera en que un usuario o empleado afronta posibles fraudes en la red, reduciendo el impacto de amenazas como el phishing, el malware, entre otros. Independientemente de las medidas que una organización pueda tener implementadas, como un firewall, un sistema antivirus o copias de seguridad de la información. Principalmente se utiliza la concienciación para disminuir los riesgos de ciberseguridad que están directamente relacionados con el comportamiento de los usuarios de las organizaciones. El usuario sigue

siendo el punto más vulnerable de una organización [22].

2.0.5. Framework

Un Framework es una estructura o modelo que proporciona una base para desarrollar un proyecto con metas específicas, funcionando como una plantilla inicial para organizar y crear software. El uso de frameworks puede hacer que una tarea o proceso sea mucho más sencillo. Un Framework es útil para llevar a cabo un proyecto en menos tiempo, especialmente en el campo de la programación, ya que permite escribir un código más ordenado y coherente de forma rápida y eficiente. El uso de Frameworks permite acelerar el proceso de desarrollo al poder reutilizar herramientas o módulos. La facilidad para escribir código o desarrollar aplicaciones también contribuye a una mejor organización y control del trabajo realizado, permitiendo su reutilización en el futuro [3].

2.0.6. NIST

El NIST es un Framework que proporciona controles de ciberseguridad. Está basado en un núcleo, que incluye tres capas: el marco, niveles de implementación y los perfiles como se muestran en la Figura 2.3.

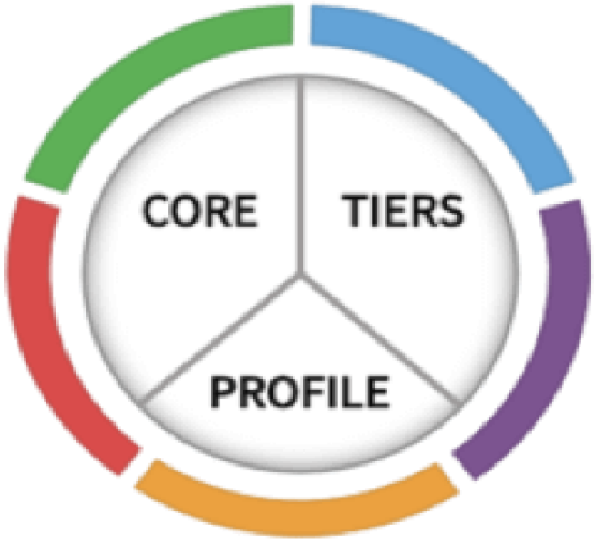

Figura 2.3: Núcleo del NIST.

El marco(core) presenta cinco funciones que son el centro de la implementación de los controles de ciberseguridad.

- **Identificar:** Permite analizar los sistemas y activos de la organización
- **Proteger:** Permite implementar las medidas de ciberseguridad.
- **Detectar:** Permite monitorear eventos y anomalías en ciberseguridad.
- **Responder:** Permite reaccionar frente a un evento de ciberseguridad identificado.
- **Recuperar:** Permite reaccionar después de un incidente.

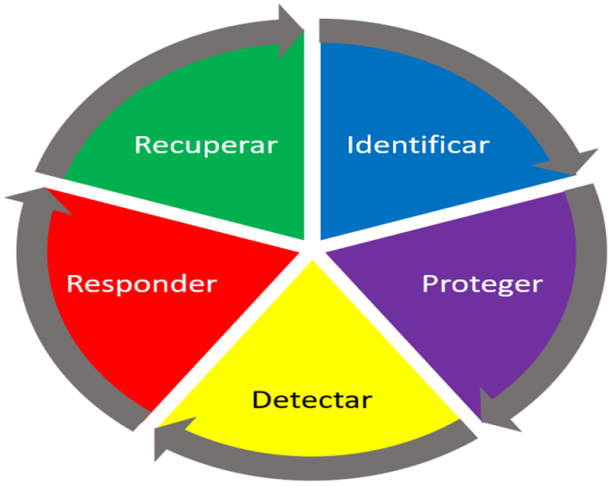

Figura 2.4: Funciones del NIST.

Los niveles de implementación (tiers) permiten a la organización clasificarse en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa [23].

En la Figura 2.5 se muestra los niveles que utiliza el NIST para clasificación.

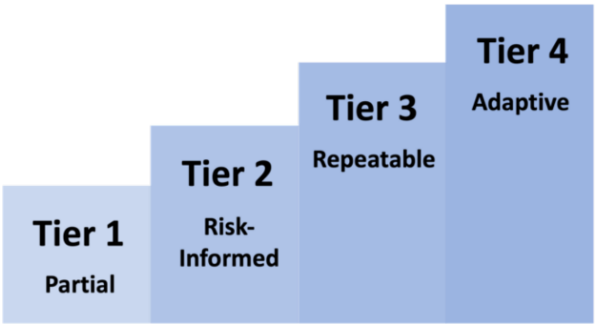

Figura 2.5: Marco del NIST.

Los perfiles (profile) se emplean para describir el estado actual y el estado objetivo de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la iden-

tificación de brechas que deben gestionarse para cumplir con los objetivos de gestión de riesgos [23].

Figura 2.6: Perfiles del NIST.

2.0.7. ISO 27001

ISO 27001 es un estándar internacional para la gestión de la seguridad de la información. Su objetivo es ayudar a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de su información mediante un sistema de gestión de seguridad de la información (SGSI).

El SGSI es un conjunto de políticas, procesos, controles y procedimientos diseñados para gestionar los riesgos de seguridad de la información. Esto incluye la protección de datos sensibles, la gestión de acceso y el manejo de incidentes de seguridad [24].

En la Figura 2.7 se muestran las fases de implementación del SGSI.

Figura 2.7: Implementación del SGSI del ISO 27001 [25].

Capítulo 3
Desarrollo del Proyecto

En este Capítulo se presenta el desarrollo de un Framework, el cual presenta a las PYMES una solución para protegerse ante amenazas digitales y fomentar una cultura en términos de ciberseguridad.

Se considera que este proyecto es un desarrollo perteneciente al área de ciberseguridad y responde a la necesidad de abordar la vulnerabilidad que enfrentan las PYMES frente a las amenazas digitales, derivada de la carencia de recursos y la falta de directrices adaptadas a sus características.

Para una mayor comprensión del proyecto, a continuación se presenta de manera visual la arquitectura de cada una de las fases en la Figura 3.1.

Figura 3.1: Arquitectura general del Framework.

3.1. Producto propuesto

La solución propuesta esta basada en desarrollar un Framework que proporcione las directrices necesarias para mejorar la ciberseguridad en las PYMES, de manera que puedan mantener la integridad y confidencialidad de sus datos. Este Framework explica paso a paso las acciones

a implementar, facilitando la adopción de buenas prácticas de ciberseguridad, que protejan los activos digitales de la empresa y promuevan un entorno seguro para sus operaciones.

3.2. Descripción de la metodología

El enfoque metodológico para el desarrollo de este trabajo utiliza el modelo en cascada, estructurado en cuatro fases: análisis, diseño, implementación y mejora continua. Este enfoque secuencial garantiza una planificación detallada y un orden en el desarrollo del Framework. Este modelo esta representado en la Figura 3.2, donde se muestra cada fase, lo cual constituirá la parte inicial del Framework.

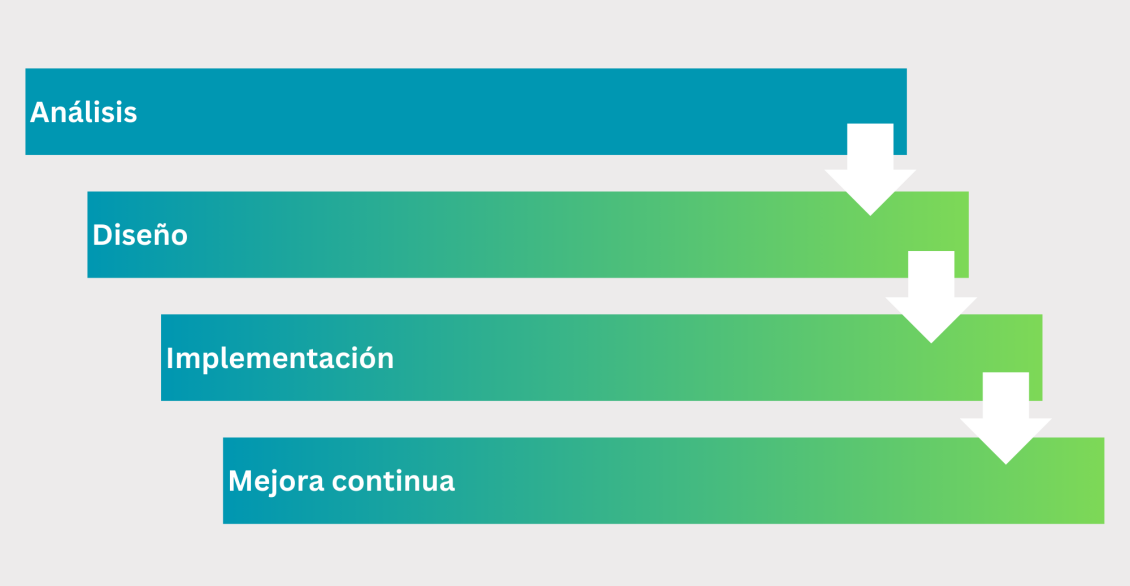

Figura 3.2: Metodología en cascada usada para el desarrollo del Framework.

Cada fase del Framework incluye secciones, como se muestra en la Tabla 3.1, que sirven como una base general para establecer procesos claros, comenzando desde el análisis de la empresa para tener una visión de la misma, el diseño de políticas, roles y responsabilidades,

pasando por la implementación de medidas de ciberseguridad en la redes, la gestion de los datos y conseguir una cultura de concienciación entre el personal, y por último mantener la mejora continua al hacer uso de una auditoría y definir el rumbo de la empresa en términos de seguridad.

Fase	Sección
Análisis	**Requisitos**
	Perfil actual y objetivo
	Gestión de activos
	Gestión de comunicaciones
Diseño	**Políticas**
	Roles y responsabilidades de seguridad
Implementación	**Plan de riesgos**
	Seguridad de los datos
	Seguridad de la red
	Conciencia y capacitación
	Plan ante incidentes
Mejora continua	**Auditoría**
	Actualización de estrategias

Tabla 3.1: Fases y secciones del Framework.

Cada sección tiene prácticas especificas por realizar,. En esta parte se define lo que se debe hacer para mantener una buena práctica de ciberseguridad, basadas en las características de la empresa. Se obtiene un perfil actual y objetivo, que determina la situación actual y las metas a alcanzar como organización. De la misma manera se debe realizar un inventario de activos para gestionar la empresa y analizar las formas de comunicación existentes, identificando lo que se necesita proteger. Una vez teniendo claro los objetivos de la empresa, se definen tanto las políticas como los roles y responsabilidades de quienes las aplicaran. Con los elementos a

proteger identificados, se procede a tomar medidas que ayudaran a la empresa a proteger y mantener la integridad y disponibilidad de los datos. Tras completar esta parte, el siguiente paso es hacer una auditoría interna para comprobar si se ha logrado el objetivo y actualizar las estrategias según sea necesario.

Fase	Sección	Práctica
Análisis	**Requisitos**	Definir PYME
	Perfil actual y objetivo	Definir perfil actual y objetivo
	Gestión de activos	Inventariar Infraestructura: activos hardware y software
	Gestión de comunicaciones	Gestionar las comunicaciones
Diseño	**Políticas**	Definir las políticas de ciberseguridad de la organización
	Roles y responsabilidades de seguridad	Definir los roles y las responsabilidades de seguridad
Implementación	**Plan de riesgos**	Desarrollar un plan de riesgos a través de una evaluación
	Seguridad de los datos	Implementar medidas de protección de los datos
	Seguridad de la red	Implementar medidas de protección de la red
	Conciencia y capacitación	Implementar una cultura de ciberseguridad
	Plan ante incidentes	Desarrollar un plan para mitigar incidentes
Mejora continua	**Auditoría**	Realizar auditoría de ciberseguridad
	Actualización de estrategias	Actualizar las estrategias de seguridad

Tabla 3.2: Framework de ciberseguridad para PYMES.

3.3. Análisis de la empresa

En esta fase la empresa debe hacer un análisis profundo de forma interna para identificar las características de valor en el entorno. Este proceso conlleva una revisión de diferentes aspectos de la organización.

En la Tabla 3.3, se presentan los entregables que sirven como guía en el proceso de la etapa de análisis.

Práctica	**Entregable**
Definir PYME	Se detallan las características de una PYME
Definir perfil actual y objetivo	Plantilla que proporciona los niveles de madurez
	Plantilla para definir el perfil actual y objetivo de la empresa
Inventariar Infraestructura activos hardware y software	Plantilla para gestionar inventarios
Gestionar las comunicaciones	Plantilla de gestor de comunicación

Tabla 3.3: Entregables de la etapa de análisis.

3.3.1. Requisitos de las PYMES

En esta sección se define lo que es una PYME, es importante tener en cuenta que características tiene la empresa, en términos de tamaño e infraestructura, para saber si este Framework aplicara para la misma.

Definir PYME

Las PYMES suelen tener entre 1 y 200 empleados [26]. Basado en esto, las PYMES necesitan recursos tecnológicos esenciales que les permitan operar de manera eficiente.

En 2024, toda PYME requiere, como mínimo, acceso a internet para conectarse al mundo digital. La conectividad de red es fundamental, por lo que es necesario establecer una red local (LAN), un switch para la conexión de los equipos de cómputo y un router para gestionar el acceso a internet. También se recomienda contar con una red Wi-Fi que permita el acceso inalámbrico a dispositivos móviles y visitantes.

Además, una PYME debe disponer de hardware adecuado, que incluya entre 1 a 50 computadoras y dispositivos móviles para el personal, impresoras y, en algunos casos, un servidor, ya sea local o en la nube, para alojar aplicaciones y almacenar datos de manera segura y eficiente.

A nivel de software, una PYME cuenta con sistemas operativos en cada dispositivo y aplicaciones de productividad, como procesadores de texto y hojas de cálculo, que faciliten las tareas diarias. Para la comunicación y el intercambio de información, el uso de servicios de correo electrónico es común. En la actualidad, muchas PYMES optan por soluciones basadas en la nube, que no solo ofrecen almacenamiento seguro, sino que también facilitan el uso compartido de archivos y la colaboración en tiempo real.

3.3.2. Perfil actual y objetivo

Esta sección se basa en la evaluación que realiza el NIST para medir la seguridad de la empresa [27]. Consiste en establecer un perfil actual y un perfil objetivo, con el fin de saber en qué nivel de ciberseguridad se encuentra la organización y hacia dónde se desea llegar. Esto permite definir las prioridad en la implementación.

La siguiente plantilla proporciona los niveles de madurez, esto nos ayudara a definir una

base para poder implementar las prácticas de ciberseguridad. Estos niveles muestran el estatus de seguridad de la empresa.

Nivel	**Descripción**
Nivel 1: Inicial (Bajo)	La práctica no se ha implementado.
Nivel 2: Básico	La práctica se ha analizado.
Nivel 3: Intermedio	La práctica se está implementando.
Nivel 4: Avanzado	La práctica se está perfeccionando.
Nivel 5: Óptimo (Alto)	La práctica se ha implementado.

Tabla 3.4: Nivel de madurez.

En la siguiente plantilla se definen el perfil actual y el perfil objetivo, los cuales se completan mediante un análisis de las medidas que se han implementado dentro de la organización.

Práctica	Perfil Actual	Perfil Objetivo
Definir PYME	Nivel de madurez	Nivel de madurez
Definir perfil actual y objetivo	Nivel de madurez	Nivel de madurez
Inventariar infraestructura: activos de hardware y software	Nivel de madurez	Nivel de madurez
Gestionar las comunicaciones	Nivel de madurez	Nivel de madurez
Definir las políticas de ciberseguridad de la organización	Nivel de madurez	Nivel de madurez
Definir los roles y las responsabilidades de seguridad	Nivel de madurez	Nivel de madurez
Desarrollar un plan de riesgos a través de una evaluación	Nivel de madurez	Nivel de madurez
Implementar medidas de protección de los datos	Nivel de madurez	Nivel de madurez
Implementar medidas de protección de la red	Nivel de madurez	Nivel de madurez
Implementar una cultura de ciberseguridad	Nivel de madurez	Nivel de madurez
Desarrollar un plan para mitigar incidentes	Nivel de madurez	Nivel de madurez
Realizar auditoría de seguridad	Nivel de madurez	Nivel de madurez
Actualizar las estrategias de seguridad	Nivel de madurez	Nivel de madurez

Tabla 3.5: Perfil actual y objetivo.

3.3.3. Gestión de activos

La infraestructura de una empresa incluye todos los recursos tecnológicos que utiliza para llevar a cabo sus operaciones. Esto abarca hardware, software, dispositivos de red y cualquier otro activo tecnológico. Elaborar un inventario detallado permite identificar los recursos disponibles, las necesidades y cómo el componente aporta a la seguridad general de la organización.

Para realizar un inventario, se consideran los siguientes pasos:

- Realizar un listado de todos los activos tecnológicos, clasificándolos por tipo (hardware,

software, dispositivos de red, etc).

- Incluir detalles como ubicación, descripción y propietario del activo.

Activo	Tipo	Ubicación	Descripción	Propietario del activo
Nombre del activo	Tipo de activo	Ubicación del activo	Función del activo	Nombre de quien opera el activo

Tabla 3.6: Inventario de activos.

3.3.4. Gestión de comunicaciones

La comunicación dentro de una organización es importante para su correcto funcionamiento. Mapear los métodos de comunicación utilizados por diferentes departamentos y sistemas contribuye a identificar áreas de mejora y posibles vulnerabilidades.

La plantilla propuesta se visualiza en la Tabla 3.7

Departamento	Método de Comunicación
Área de la empresa	Cómo el departamento se comunica

Tabla 3.7: Gestor de comunicación.

3.4. Diseño de políticas, roles y responsabilidades

En esta fase se diseñan las políticas, así como los roles y responsabilidades que serán de utilidad para que las PYMES se guíen en cuanto a las acciones y decisiones de la empresa en términos de ciberseguridad. Ademas, se asignan roles específicos y responsabilidades a cada miembro del equipo, asegurando que todos comprendan su papel en la protección de los activos digitales de la organización.

En la Tabla 3.8, se presentan los entregables que sirven como guía en el proceso de la etapa de diseño.

Práctica	Entregable
Definir las políticas de ciberseguridad de la organización	Plantilla del documento que proporciona las políticas
Definir los roles y las responsabilidades de seguridad	Plantilla para definir los roles y responsabilidades

Tabla 3.8: Entregables de la etapa de diseño.

3.4.1. Políticas

Para esta sección se toma como base el estándar ISO 27001 para el diseño de políticas [28]. La empresa deberá definir las políticas de ciberseguridad, considerando las características de las PYMES se consideran las siguientes:

1. **Política de control de acceso**

   Objetivo: Establecer medidas para controlar el acceso a sistemas y datos sensibles.

2. **Política de uso aceptable de recursos**

   Objetivo: Definir las reglas sobre el uso adecuado de los recursos de tecnología de la empresa.

3. **Política de protección de datos**

   Objetivo: Establece normas para la recolección, almacenamiento y manejo de datos sensibles.

4. **Política de seguridad de la red**

Objetivo: Establece medidas para proteger la red de la empresa contra ataques externos e internos.

5. **Política de concienciación y capacitación en Seguridad**

   Objetivo: Promueve la concienciación y capacitación continua en ciberseguridad para todos los empleados.

6. **Política de seguridad física**

   Objetivo: Proteger el acceso físico a los sistemas y datos sensibles de la empresa.

7. **Política de auditoria**

   Objetivo: Realiza auditorias de ciberseguridad continuamente para evaluar la empresa.

Estas políticas son la base para la ciberseguridad en las PYMES y pueden actualizarse en función de las necesidades de la organización.

Con base a las políticas establecidas, se elabora un documento que actúa como una guía formal que detalla los principios y directrices necesarias para proteger la información. En la Figura 3.3, se presenta una plantilla de dicho documento.

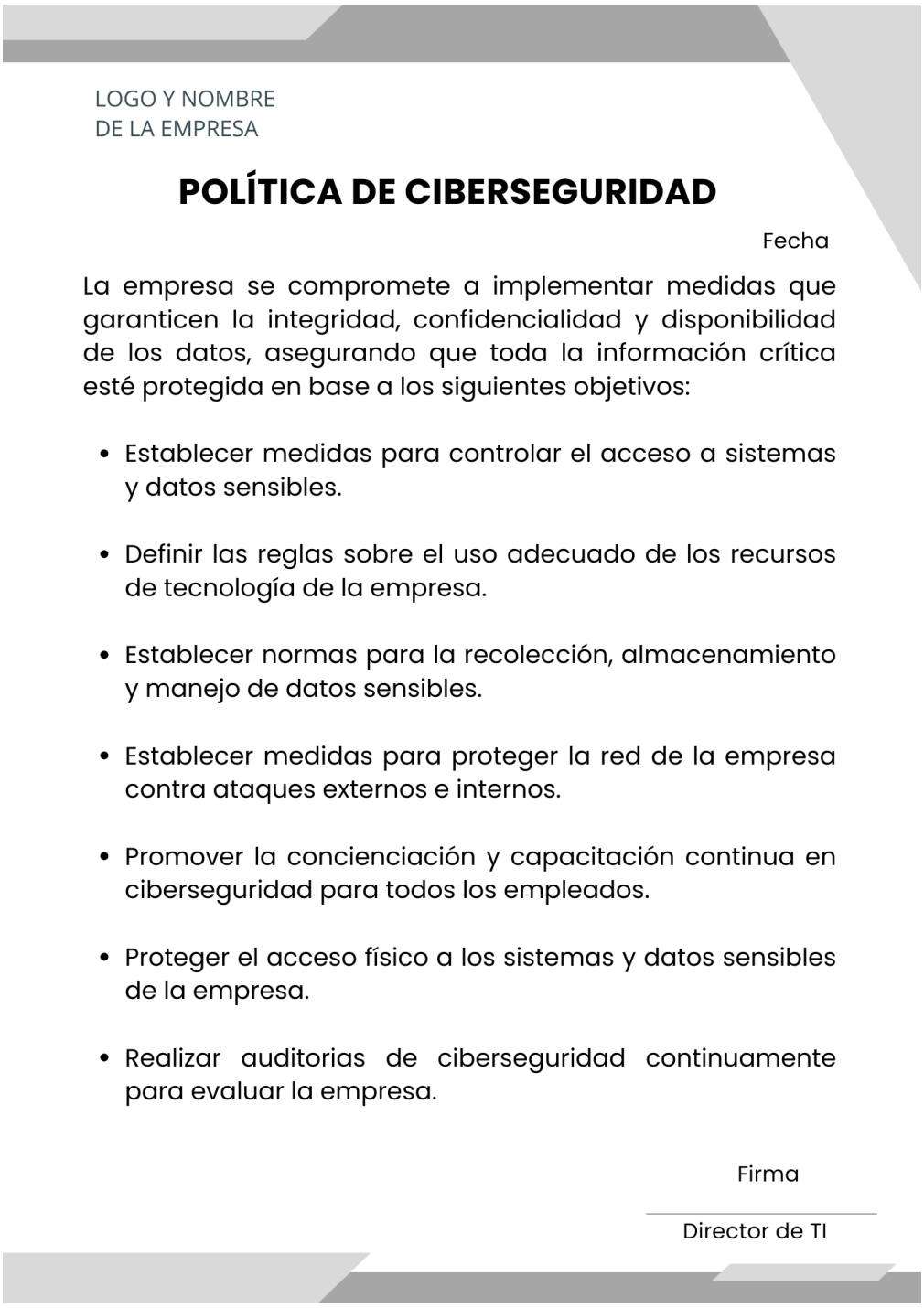

Figura 3.3: Plantilla del documento de políticas de ciberseguridad.

3.4.2. Roles y las responsabilidades

Definir roles y responsabilidades en seguridad de la información es fundamental para asegurar que todos en la organización comprendan su función en la protección de los activos digitales y en la prevención de incidentes. Este proceso incluye identificar y registrar las tareas y responsabilidades específicas de seguridad para cada puesto relevante, desde la alta dirección hasta los usuarios comunes. Los roles clave pueden incluir encargados de la seguridad de la información, administradores de sistemas, gestores de riesgos y personal general, cada uno con funciones ajustadas a su nivel de acceso y responsabilidades dentro de la organización. Esto permite una asignación clara de funciones, promueve la responsabilidad y facilita una respuesta coordinada y eficiente ante posibles amenazas o incidentes de seguridad.

La Tabla 3.9 funciona como base para lograr el objetivo planteado.

Rol	Responsabilidades
Director de TI	Supervisa la implementación y cumplimiento de las políticas de seguridad.
Gerente de Seguridad	Desarrolla y revisa las políticas y controles de ciberseguridad.
Administrador de Sistemas	Mantiene y protege los sistemas críticos, asegurando su disponibilidad.
Empleado	Cumple con las políticas establecidas, reportando cualquier incidente o actividad sospechosa.

Tabla 3.9: Roles y responsabilidades de seguridad.

3.5. Implementación de medidas de ciberseguridad

La fase de implementación es donde se llevan a cabo las acciones de las soluciones de ciberseguridad, abarcando el plan de riesgos, la seguridad de los datos, la seguridad de la red,

el plan de concienciación para el personal y el plan de mitigación de incidentes.

Los entregables de la etapa se definen en la Tabla 3.10.

Práctica	Entregable
Desarrollar un plan de riesgos a través de una evaluación	Plantilla plan de riesgos de activos
	Plantilla plan de riesgos de comunicaciones
Implementar medidas de protección de los datos	Bases de seguridad de los datos
Implementar medidas de protección de la red	Bases de seguridad en la red
Implementar una cultura de ciberseguridad	Bases de concientización
Desarrollar un plan para mitigar incidentes	Plantilla plan de mitigación de incidentes

Tabla 3.10: Entregables de etapa de implementación.

3.5.1. Plan de riesgos

Realizar un plan de riesgos es importante, ya que identifica las posibles amenazas o vulnerabilidades que pueden afectar a una organización. En base a los activos de la empresa se deben analizar los riesgos potenciales que podrían afectar directamente al activo y determinar el impacto que tendría en la empresa si sucediera. De igual manera, se atribuye una probabilidad de que pueda pasar, y se propone una solución que detalla cómo se va a mitigar el riesgo y se asigna a un responsable quien llevara a cabo la implementación de la solución.

La siguiente Tabla 3.11 muestra de manera detallada cómo realizar la implementación para los activos de la empresa.

Activo	Tipo	Riesgos Potencia-les	Impacto	Probabilidad	Prevención	Responsable
Nombre del activo	Hardware /Software /Disposi-tivo /Otro	Posibles amenazas	Muy Bajo /Bajo /Medio /Alto /Extre-mo	Baja /Media /Alta /Extrema	Forma de prevenir el riesgo	Encargado de llevar a cabo el plan

Tabla 3.11: Plan de riesgos activos.

De la misma manera en que se evalúan los activos y se realiza el plan de riesgo, es necesario aplicar el análisis para las comunicaciones de la empresa. Para ello, se presenta la plantilla en la Tabla 3.12. Las comunicaciones, deben ser evaluadas para identificar posibles riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información transmitida.

Departamento	Método de Comunicación	Riesgos Potenciales	Prevención	Responsable
Área de la empresa	Cómo el departamento se comunica	Posibles amenazas	Forma de prevenir el riesgo	Encargado de llevar a cabo el plan

Tabla 3.12: Plan de riesgo de comunicaciones.

3.5.2. Seguridad de los datos

Basado en las políticas definidas se establece la implementación de medidas de seguridad para la protección de los datos, asegurando la confidencialidad, integridad y disponibilidad de la información. Mejorar la seguridad de los datos implica controlar el acceso a la información sensible; por ello, es fundamental aplicar buenas prácticas de ciberseguridad, tales como la autenticación multifactor (MFA) y la asignación de permisos según los roles asignados. También

es recomendable realizar respaldos de manera seguida y gestionar adecuadamente los datos críticos como contraseñas de los usuarios, para reforzar la protección de la información en todo momento.

3.5.3. Seguridad de la red

En esta sección se implementan medidas de seguridad para la protección de la red, ya que proteger de red es fundamental para cualquier empresa. Una red comprometida puede permitir acceso no autorizado a datos sensibles y afectar la disponibilidad de los sistemas. Para ello, se debe asegurar que el tráfico de datos esté controlado y protegido contra amenazas externas e internas. Para realizar la seguridad de la red en las PYMES, implica establecer barreras y controles que limiten el acceso no autorizado; aplicar buenas prácticas, como la segmentación de la red en zonas de seguridad y el uso de cortafuegos (firewalls) configurados con reglas específicas. Es recomendable hacer uso de herramientas de código abierto (open source) por su flexibilidad, escalabilidad y accesibilidad. Estas herramientas pueden adaptarse a las necesidades específicas de la empresa, proporcionando funcionalidades avanzadas sin la carga de licencias costosas. Implementar sistemas de detección y prevención de intrusos (IDS/IPS) sirve para identificar y mitigar posibles ataques en tiempo real, así como mantener la infraestructura de red actualizada con parches de seguridad. Estas medidas deben complementarse con la política de auditoría constante para asegurar la detección temprana de cualquier anomalía en el tráfico de red.

3.5.4. Conciencia y capacitación

La concienciación y capacitación tienen como objetivo fomentar una cultura de ciberseguridad en la empresa. Aumentar el conocimiento sobre los riesgos cibernéticos ayuda a reducir los errores humanos, que son una de las causas más comunes de incidentes, como los ataques

de phishing. Para lograrlo es importante implementar un programa de capacitación periódica que fomente a los empleados en términos de ciberseguridad y conozcan sus roles para aplicar practicas seguras. Este programa deberá contar con actualizaciones regularmente para incluir nuevas tendencias y amenazas de ciberseguridad, permitiendo que el personal esté preparado para enfrentar los futuros riesgos.

3.5.5. Plan de mitigación de incidentes

La empresa debe contar con un plan de respuesta ante incidentes, detallando específicamente las acciones a seguir en caso de un ataque o anomalía. Este plan debe incluir procedimientos para detener el incidente, minimizar el impacto en las operaciones de la empresa y restaurar la normalidad de manera segura.

La redacción de los incidentes debe estructurarse como sigue:

- **Incidente:**

  Objetivo: Se describe el incidente identificado.

- **Mitigación:**

  Objetivo: Se describe la forma de mitigar el incidente.

- **Responsable:**

  Objetivo: Se informa quien es el encargado de mitigarlo.

3.6. Mejora continua en las funciones de ciberseguridad

En esta fase se promueve la mejora continua de las prácticas de ciberseguridad mediante una auditoría que evalué el cumplimiento de las practicas y políticas para detectar vulnerabilidades.

Además, la actualización de estrategias de seguridad es importante para adaptarse a los cambios en el entorno digital y a las nuevas técnicas de ataque.

Práctica	Entregable
Realizar auditoría de seguridad	Plantilla de auditoría interna
Actualizar estrategias de seguridad	Bases de actualización de estrategias

Tabla 3.13: Prácticas y Entregables.

3.6.1. Auditoría

Se realiza una auditoría interna para evaluar el avance que se ha llevado a cabo sobre las prácticas de ciberseguridad. Esta auditoria tiene como objetivo analizar el nivel de madurez actual alcanzado de cada practica y compararlo con el nivel objetivo definido al inicio del Framework, para identificar áreas de mejora.

La Tabla 3.14, presenta una plantilla que facilita el proceso de auditoría. En esta plantilla, cada práctica de ciberseguridad, ademas de las columnas de perfil actual y objetivo que definen el nivel de madurez en el que se encuentra cada práctica, incluye una columna de avance, donde se registra el porcentaje de progreso alcanzado.

Práctica	Perfil Actual	Perfil Objetivo	Avance
Definir PYME	Nivel de madurez	Nivel de madurez	Porcentaje
Definir perfil actual y objetivo	Nivel de madurez	Nivel de madurez	Porcentaje
Inventariar infraestructura: activos de hardware y software	Nivel de madurez	Nivel de madurez	Porcentaje
Gestionar las comunicaciones	Nivel de madurez	Nivel de madurez	Porcentaje
Definir las políticas de ciberseguridad de la organización	Nivel de madurez	Nivel de madurez	Porcentaje
Definir los roles y las responsabilidades de seguridad	Nivel de madurez	Nivel de madurez	Porcentaje
Desarrollar un plan de riesgos a través de una evaluación	Nivel de madurez	Nivel de madurez	Porcentaje
Implementar medidas de protección de los datos	Nivel de madurez	Nivel de madurez	Porcentaje
Implementar medidas de protección de la red	Nivel de madurez	Nivel de madurez	Porcentaje
Implementar una cultura de ciberseguridad	Nivel de madurez	Nivel de madurez	Porcentaje
Desarrollar un plan para mitigar incidentes	Nivel de madurez	Nivel de madurez	Porcentaje
Realizar auditoría de seguridad	Nivel de madurez	Nivel de madurez	Porcentaje
Actualizar las estrategias de seguridad	Nivel de madurez	Nivel de madurez	Porcentaje

Tabla 3.14: Auditoría interna de prácticas de ciberseguridad.

3.6.2. Actualización de estrategias

Una vez completado todas las prácticas, es importante estar actualizando las estrategias de ciberseguridad, ya que las amenazas y vulnerabilidades siguen incrementando. Por lo tanto, es necesario revisar y ajustar regularmente las prácticas y políticas de seguridad hacia la PYME.

Además, las actualizaciones deben incluirse en las reuniones de capacitación continua del personal, ya que los empleados son de suma importancia en la defensa y prevención de ataques. Cuando surgen nuevas amenazas, es fundamental que los empleados conozcan y estén informados sobre cómo reconocer y responder a situaciones de riesgo.

3.7. Prueba del Framework

Para probar el funcionamiento del Framework, se ha realizado un caso de uso mediante la simulación de una PYME. El caso de uso se describe de la siguiente manera: se trata de una empresa con poco conocimiento en ciberseguridad, con siete empleados, cada uno con un equipo de cómputo conectado a una red LAN. La infraestructura de red incluye un router y un switch que conecta todos los equipos, representando la configuración básica de una pequeña empresa. Para sus operaciones diarias, la empresa también utiliza medios de comunicación como el correo electrónico.

Para modelar la topología de la red se utilizó GNS3, un software de código abierto que permite simular redes y emular dispositivos. Esta herramienta permitió recrear la infraestructura de una PYME. En la Figura 3.4, se ve representada la topología.

A esta empresa se le aplicaron las prácticas de ciberseguridad propuestas en el Framework, con el fin de evaluar su eficacia y garantizar una protección adecuada en un entorno típico de pequeña empresa.

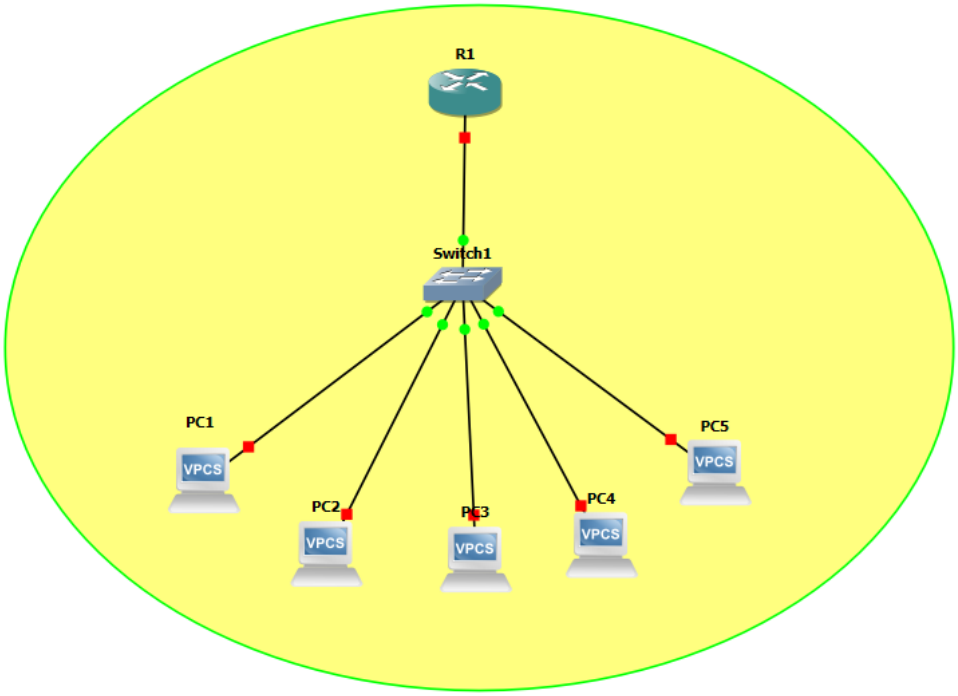

Figura 3.4: Topología de red de la PYME simulada en GNS3.

Capítulo 4
Resultados y discusiones

4.1. Resultados

En este Capítulo se presentan los resultados obtenidos en la implementación del Framework de ciberseguridad. El proceso de evaluación se llevó a cabo mediante una simulación de una PYME en GNS3 descrita en el capitulo anterior, donde se analizaron diferentes prácticas y políticas de seguridad aplicadas en la empresa. Los resultados se describen en función de la capacidad de la PYME para implementar el Framework, asegurando la protección de los datos sensibles de la organización y el aumento de la ciberseguridad de la empresa.

Para un mejor análisis, los resultados de la auditoría interna descrita en la fase de mejora continua se representan en la Tabla 4.1. Al inicio de la implementación la PYME tenía poco conocimiento en ciberseguridad por lo que al definir el perfil actual y objetivo el resultado de nivel de madurez era bajo.

Una vez finalizada la implementación del Framework estos niveles aumentaron a un nivel alto, en función de las prácticas implementadas.

Práctica	Perfil Actual	Perfil Objetivo	Avance
Definir PYME	Alto	Alto	100 %
Definir perfil actual y objetivo	Alto	Alto	100 %
Inventariar infraestructura: activos de hardware y software	Alto	Alto	100 %
Gestionar las comunicaciones	Alto	Alto	100 %
Definir las políticas de ciberseguridad de la organización	Alto	Alto	100 %
Definir los roles y las responsabilidades de seguridad	Alto	Alto	100 %
Desarrollar un plan de riesgos a través de una evaluación	Alto	Alto	100 %
Implementar medidas de protección de los datos	Alto	Alto	100 %
Implementar medidas de protección de la red	Alto	Alto	100 %
Implementar una cultura de ciberseguridad	Alto	Alto	100 %
Desarrollar un plan para mitigar incidentes	Alto	Alto	100 %
Realizar auditoría de seguridad	Alto	Alto	100 %
Actualizar las estrategias de seguridad	Alto	Alto	100 %

Tabla 4.1: Auditoría interna de prácticas de ciberseguridad en la PYME simulada.

4.2. Discusiones

Los resultados obtenidos en este proyecto permiten visualizar los avances logrados en función de cada objetivo específico.

En primer lugar, respecto al análisis de las características de las PYMES para definir las soluciones a implementar, los hallazgos muestran que las pequeñas y medianas empresas suelen carecer de sistemas de ciberseguridad sólidos debido a limitaciones de recursos y conocimiento en ciberseguridad. Además, permitió definir el tamaño de las PYMES de acuerdo con el número de empleados y la infraestructura con la que cuentan. Este análisis permitió identificar

necesidades clave, lo cual guió la selección de las soluciones específicas implementadas en el Framework.

En cuanto al objetivo de diseñar la arquitectura del Framework para tener una visión general, los resultados muestran que la estructura del Framework es efectiva para abordar los desafíos de ciberseguridad en las PYMES. La arquitectura propuesta permite una implementación escalonada, facilitando su adaptación en entornos con diferentes niveles de madurez en ciberseguridad. Esto confirma que la arquitectura diseñada puede ser una base sólida para implementar políticas de seguridad en empresas con infraestructura y recursos limitados.

Para el objetivo de elaborar plantillas de implementación que incluyan ejemplos de mejores prácticas basadas en estándares internacionales de ciberseguridad, los resultados destacan la importancia de contar con directrices claras. Las plantillas desarrolladas proporcionan pasos concretos y ejemplos de buenas prácticas que se alinean con estándares reconocidos, como ISO 27001 y NIST, permitiendo a las PYMES implementar procedimientos de seguridad de manera estructurada. Estas plantillas no solo facilitan la implementación, sino que también ofrecen una referencia práctica para futuras actualizaciones y mejoras en las políticas de seguridad.

Finalmente, en relación con el objetivo de realizar un caso de uso mediante la simulación de una PYME para probar el Framework, la simulación en GNS3 permitió evaluar la efectividad del Framework en un entorno controlado. En esta simulación los resultados mostraron que se implementó de manera correcta el Framework experimentando una mejora notable en las prácticas de ciberseguridad y una disminución de incidentes de seguridad, así como una mejora en la detección y respuesta ante amenazas digitales. Esto resalta la efectividad del Framework como una herramienta práctica y accesible para fortalecer la ciberseguridad para las PYMES.

Capítulo 5
Conclusiones

En capítulos anteriores se ha presentado un análisis detallado de las características, diseño y pruebas de implementación del Framework de ciberseguridad para PYMES. En este capítulo se verá de forma objetiva lo que el proyecto consiguió aportar y si este mismo alcanzó el objetivo principal.

5.1. Con respecto al objetivo general

Este trabajo se centró en el desarrollo de un Framework de ciberseguridad orientado a PYMES, con el objetivo de proteger la integridad y confidencialidad de los datos brindando una estructura que fortalezca sus defensas contra amenazas de ciberseguridad en entornos con recursos limitados.

El Framework desarrollado mostró resultados importantes que demuestran que el Framework no solo cumple con los objetivos específicos planteados, sino que también ofrece un enfoque adaptable y escalable para las necesidades de ciberseguridad de las PYMES.

5.2. Recomendaciones para trabajo a futuro

Se sugiere que en futuras investigaciones evalúe el Framework en entornos de producción reales, en diversas PYMES de distintos sectores y que se exploren posibles optimizaciones en cuanto a las medidas de ciberseguridad e implementación.

Bibliografía

[1] L. Technologies, "Lumu compromise report 2024," tech. rep., 2024. Accessed: 2024-10-28.

[2] C. Paulsen and P. Toth, "Small business information security: The fundamentals," Tech. Rep. NIST IR 7621 Revision 1, 2021.

[3] U. FP, "Framework: qué es, para qué sirve y algunos ejemplos | UNIR FP — unirfp.unir.net." `https://unirfp.unir.net/revista/ingenieria-y-tecnologia/framework/`. [Accessed 19-03-2024].

[4] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, 2023.

[5] B. Azinheira, M. Antunes, M. Maximiano, and R. Gomes, "A methodology for mapping cybersecurity standards into governance guidelines for sme in portugal," *Procedia Computer Science*, vol. 219, pp. 121–128, 2023. CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022.

[6] M. López, J. M. Lombardo, M. López, C. M. Alba, S. Velasco, M. A. Braojos, and M. Fuentes-García, "Intelligent detection and recovery from cyberattacks for small and medium-sized enterprises," *IJIMAI*, vol. 6, no. 3, pp. 55–62, 2020.

[7] A. Mukhopadhyay and S. Jain, "A framework for cyber-risk insurance against ransomware: A mixed-method approach," *International Journal of Information Management*, vol. 74, p. 102724, 2024.

[8] M. F. Franco, F. M. Lacerda, and B. Stiller, "A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises," *Gestão e Projetos: GeP*, vol. 13, no. 3, pp. 10–37, 2022.

[9] Kaspersky, "Redefining the Human Factor in Cybersecurity — kaspersky.com." `https://www.kaspersky.com/blog/human-factor-360-report-2023/`, 2023. [Accessed 21-04-2024].

[10] Kaspersky, "Las PyMEs de América Latina enfrentan un creciente número de ciberataques — latam.kaspersky.com." `https://latam.kaspersky.com/blog/pymes-latam-enfrentan-creciente-numero-ciberataques/24950/`, 2022. [Accessed 21-04-2024].

[11] W. T. Organization, "OMC | Grupo de Trabajo Informal sobre las Microempresas y las Peque&xF1;as y Medianas Empresas (Mipymes) — wto.org." `https://www.wto.org/spanish/tratop_s/msmes_s/msmes_s.htm`. [Accessed 21-04-2024].

[12] I. N. de Estadística y Geografía (INEGI), "Encuesta nacional sobre productividad y competitividad de las micro, pequeñas y medianas empresas 2018," 2018.

[13] Marsh, "Primer estudio de riesgos para empresas nacionales y familiares latinoamericanas 2023-2024," 2023.

[14] Kaspersky, "¿Qué es la ciberseguridad? — latam.kaspersky.com." https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed 19-03-2024].

[15] Mexicoemprende, "Qué son las pymes, clasificación y ejemplos — mexicoemprende.org.mx." https://www.mexicoemprende.org.mx/que-son-las-pymes/. [Accessed 21-05-2024].

[16] McAfee, "¿Qué es malware?." https://www.mcafee.com/es-mx/antivirus/malware.html. [Accessed 18-03-2024].

[17] Cisco, "¿Qué es la ciberseguridad? — cisco.com." https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html. [Accessed 19-03-2024].

[18] kaspersky, "Panorama en América Latina 2023 — latam.kaspersky.com." https://latam.kaspersky.com/blog/panorama-amenazas-latam-2023/26586/. [Accessed 29-10-2024].

[19] IBM, "¿Qué es el ransomware? | IBM — ibm.com." https://www.ibm.com/mx-es/topics/ransomware. [Accessed 19-03-2024].

[20] IBM, "IBM Security X-Force Threat Intelligence Index 2024 — ibm.com." https://www.ibm.com/reports/threat-intelligence. [Accessed 19-03-2024].

[21] I. Security, "Ibm x-force threat intelligence index 2024," 2024.

[22] G. ICA, "La Concienciación en Ciberseguridad es clave para garantizar la seguridad en cualquier organización - Web Corporativa Grupo ICA - Grupo ICA — grupoica.com." https://www.grupoica.com/blog/-/blogs/. [Accessed 19-03-2024].

[23] D. Acosta, "Guía rápida para entender el marco de trabajo de ciberseguridad del NIST." https://www.deacosta.com/

guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/. [Accessed 30-10-2024].

[24] I. 27001, "ISO 27001 - Certificado ISO 27001 punto por punto." https://www.normaiso27001.es/. [Accessed 30-10-2024].

[25] ExpertSoft, "ISO 27001 — expertsoft.e." https://expertsoft.es/servicios/consultoria/iso-27001/. [Accessed 30-10-2024].

[26] BBVA, "Qué es una pyme y cuándo una empresa es pequeña o mediana — bbva.com." https://www.bbva.com/es/salud-financiera/que-es-una-pyme-y-cuando-se-considera-que-una-empresa-es-pequena-o-mediana/. [Accessed 30-10-2024].

[27] National Institute of Standards and Technology, "Nist sp 1301: Framework for improving critical infrastructure cybersecurity," Special Publication 1301, National Institute of Standards and Technology, Gaithersburg, MD, 2022. Accessed: 2024-10-30.

[28] I. 27001, "ISO 27002 punto a punto - A5 Políticas de Seguridad de la Información — normaiso27001.es." https://www.normaiso27001.es/a5-politicas-de-seguridad-de-la-informacion/. [Accessed 30-10-2024].

Apéndice A
Nombre del apéndice

[Sustituye este texto. En esta sección opcional se deberá incluir información secundaria o material importante que es muy extenso. El apéndice se coloca después de la literatura citada. Ejemplos de información que puede colocarse en el apéndice: una lista de universidades visitadas; los datos obtenidos de todas las repeticiones del experimento; derivaciones matemáticas extensas; todos los resultados del análisis estadístico (incluyendo quizás los no significativos) y mapas de distribución para cada fenómeno estudiado; listados completos de código fuente; etc.]

Apéndice B
Nombre del apéndice

[Sustituye este texto. En esta sección opcional se deberá incluir información secundaria o material importante que es muy extenso. El apéndice se coloca después de la literatura citada. Ejemplos de información que puede colocarse en el apéndice: una lista de universidades visitadas; los datos obtenidos de todas las repeticiones del experimento; derivaciones matemáticas extensas; todos los resultados del análisis estadístico (incluyendo quizás los no significativos) y mapas de distribución para cada fenómeno estudiado; listados completos de código fuente; etc.]