UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

CENTRO UNIVERSITARIO UAEM ATLACOMULCO

"Gestión de riesgos y estrategias de mitigación ante ataques del *ransomware* Medusa"

T E S I N A

Que para obtener el Título de:

Ingeniera en Computación

Presenta:

Andrea Piña Contreras

Director:

Dr. Everardo Efrén Granda Gutiérrez

Atlacomulco, México; abril del 2026

RESUMEN

Medusa es una de las amenazas de *ransomware* más agresivas de los últimos cinco años, debido a la implementación de tácticas como la doble extorsión y la exposición pública de datos. Este tipo de ataque secuestra la información de una organización y exige un rescate para liberarla. En contraste con la mayoría de los operadores de ransomware, se encuentra en la web superficial, junto con actividades tradicionales en la web oscura.

Medusa es una variante de *ransomware* identificada inicialmente en 2021 y que ganó notoriedad a partir de 2023 por su agresiva estrategia de doble extorsión: cifra los archivos de los sistemas comprometidos, pero también filtra información confidencial y amenaza con publicarla si no se paga el rescate. Este *ransomware* utiliza cifrado simétrico para bloquear el acceso a los datos, lo que permite realizar el proceso de cifrado y descifrado de forma rápida y eficiente, siempre que se cuente con la clave correspondiente.

Además, Medusa opera bajo el modelo de *ransomware* como servicio, lo que significa que los desarrolladores del *malware* lo alquilan a afiliados o atacantes, quienes lo utilizan para ejecutar campañas maliciosas a cambio de una parte del rescate. Esta estructura facilita su expansión global y la diversidad de los vectores de ataque.

En este documento se analizan los antecedentes y las características técnicas de Medusa, así como su impacto en organizaciones de distintos sectores. Además, como contribución fundamental, se propone una arquitectura de gestión de ciberseguridad que mejora la prevención, la respuesta y la recuperación frente a este tipo de ataques.

A partir de encuestas a profesionales del sector TI, entrevistas a expertos que han estado en contacto directo con el *ransomware* Medusa, así como del soporte basado en estándares internacionales de seguridad de la información, se desarrolla un protocolo de respuesta ante un incidente de *ransomware* Medusa. El estudio se basa en el análisis de experiencias y percepciones de expertos en ciberseguridad y de profesionales de TI, con el propósito de contribuir al fortalecimiento de la resiliencia organizacional frente al *ransomware.*

Palabras clave: *Ransomware,* Medusa, gestión de riesgos, ciberseguridad, estrategias de mitigación.

ABSTRACT

Medusa is one of the most aggressive cyber threats in recent years. This type of attack hijacks an organization's data and demands a ransom for its release. In contrast to most ransomware operators, Medusa has established a presence on the surface web, in addition to traditional activities on the dark web.

Medusa is a ransomware variant first identified in 2021 that gained notoriety from 2023 onward for its aggressive double extortion strategy: encrypting files on compromised systems, exfiltrating confidential information, and threatening to publish it unless the ransom is paid. This ransomware uses symmetric encryption to lock access to data, enabling fast, efficient encryption and decryption when the correct key is available.

Operating under a *Ransomware-as-a-Service (RaaS)* model, Medusa's developers lease the malware to affiliates or attackers, who then conduct malicious campaigns in exchange for a share of the ransom. This structure facilitates global expansion and a diverse set of attack vectors.

This document analyzes the background and technical characteristics of the Medusa ransomware and its impact across sectors. As a core contribution, an architectural cybersecurity management framework is proposed to enhance prevention, response, and recovery from such attacks.

Based on surveys of IT professionals, interviews with experts who have had direct contact with Medusa, and international information security standards, a protocol for responding to a Medusa Ransomware attack was developed. The study generates new practical knowledge for the profession, aimed at strengthening organizational resilience against ransomware from a strategic perspective.

Keywords: Ransomware, Medusa, risk management, cybersecurity, mitigation strategies.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN

Este proyecto de investigación surge de la creciente preocupación por los ataques de *ransomware,* en particular la variante Medusa, que ha demostrado ser una amenaza significativa para las organizaciones (Parvini, 2025). El análisis preliminar de varios casos documentados reveló que, aunque existen medidas técnicas para mitigar estos ataques, muchas empresas carecen de estrategias administrativas y organizacionales efectivas para gestionar adecuadamente la prevención, la respuesta y la recuperación.

La motivación de este estudio proviene del reconocimiento de la falta de un enfoque administrativo integral en ciberseguridad y de la necesidad de mejorar la gestión organizacional para mitigar los riesgos asociados al *ransomware.* Este trabajo ofrece una propuesta aplicable y práctica que integra la gestión de incidentes dentro de un marco administrativo, permitiendo así que las organizaciones puedan reaccionar ante los ataques, y también fortalecer su resiliencia frente a futuras amenazas.

Se ha optado por desarrollar este trabajo bajo la modalidad de tesina, debido a su enfoque aplicado, orientado al análisis documental y a la sistematización de experiencias profesionales, lo que permite proponer estrategias prácticas sin requerir la formulación de hipótesis ni el desarrollo experimental.

Se desarrolla en el ámbito de la ingeniería en computación, al proponer un protocolo técnico y administrativo de mitigación de riesgos ante el *ransomware* Medusa, fundamentado en la infraestructura de redes, sistemas y medidas de ciberseguridad, además de la recopilación y el tratamiento de datos mediante encuestas a personal del sector tecnológico y entrevistas a expertos en ciberseguridad.

La presente propuesta es innovadora respecto del estado del arte, en el que se observó que la mayoría de los enfoques actuales se centran exclusivamente en soluciones técnicas, como la implementación de sistemas de seguridad (Cordova, 2025). Sin embargo, faltan enfoques administrativos que guíen las decisiones organizacionales ante incidentes de ciberseguridad, especialmente en relación con *ransomware* como Medusa.

El *ransomware* Medusa se distingue por su capacidad para extraer datos, ejercer una doble extorsión y realizar un desplazamiento lateral sofisticado, que potencia tanto el efecto operativo como el daño a la reputación de las entidades afectadas. Esta situación resalta que la ciberseguridad debe considerarse no solo desde una óptica tecnológica, sino también como un aspecto estratégico en la administración empresarial.

En este proyecto se propone la elaboración de un protocolo administrativo integral, basado en estándares internacionales como ISO/IEC 27001, NIST SP 1800-26 e ITIL 4, con el objetivo de ofrecer directrices definidas para la prevención, identificación, respuesta, recuperación y mejora continua ante incidentes de *ransomware.* Además, se incluyen una lista de evaluación de la madurez organizacional y un diagrama de acciones inmediatas ante incidentes, con el propósito de facilitar la toma de decisiones y mitigar el impacto.

Es relevante mencionar que la investigación se enfocó en las pequeñas y medianas empresas debido a su participación en la economía y a su vulnerabilidad, consecuencia de recursos escasos y de la ausencia de estrategias formales de ciberseguridad. La propuesta busca abordar esta situación mediante una alternativa práctica adaptable a diversas realidades empresariales.

Finalmente, esta tesina representa una aportación al ámbito de la ingeniería en computación, al evidenciar que la gestión administrativa y la ciberseguridad pueden fusionarse para reforzar la resiliencia organizacional ante amenazas como Medusa. De esta manera, se establecen los fundamentos para futuras investigaciones orientadas a la mejora continua de los protocolos de ciberseguridad en las empresas.

2 PLANTEAMIENTO DEL PROBLEMA

El *ransomware* Medusa ha sido identificado como una amenaza disruptiva para las organizaciones debido a su rapidez para cifrar archivos, su capacidad para evadir medidas de seguridad y su enfoque en la doble extorsión (Dubec, 2025). Esto es, al comprometer los sistemas, impide el acceso a la información mediante cifrado y también filtra datos confidenciales, sometiendo a presión a las víctimas mediante la publicación de dicha información si no se cumple con el pago.

La variante distribuida bajo el modelo de *Ransomware* como Servicio (RaaS, por sus siglas en inglés, *Ransomware-as-a-Service*) permite que atacantes con distintos niveles de experiencia accedan a la herramienta y desplieguen campañas dirigidas, ampliando su alcance y efectividad (Blancaflor, Bauson, Cruz, & Escandor, 2025). Esta descentralización de su operación vuelve más compleja su contención y su seguimiento.

Ante este panorama, resulta prioritario que las organizaciones inviertan en su infraestructura tecnológica y la evalúen, pero también fortalezcan la gestión administrativa de la ciberseguridad: políticas claras, procedimientos de respuesta, respaldos seguros y formación del personal. Esta evaluación busca analizar el nivel de preparación actual frente a amenazas como Medusa y detectar posibles áreas de mejora para reducir el riesgo organizacional.

2.1 Definición del problema

El *ransomware* Medusa representa una amenaza creciente para organizaciones y entidades gubernamentales debido a su capacidad para cifrar datos críticos. El *modus operandi* de los atacantes consiste en exigir pagos en criptomonedas a cambio de supuestamente proporcionar las claves de cifrado, sin garantía alguna de que así sea. Esto afecta la continuidad operativa de las empresas, generando pérdidas económicas y daños a su reputación.

En el ámbito administrativo, la falta de estrategias efectivas de prevención, respuesta y recuperación ante ataques de *ransomware* se traduce en vulnerabilidades significativas en los planes de seguridad de la información.

El problema central para resolver en este proceso investigativo radica en la ausencia de un marco eficiente de gestión de riesgos que permita a las organizaciones mitigar el impacto de un ataque de *ransomware* Medusa. Actualmente, las estrategias de ciberseguridad suelen centrarse en soluciones tecnológicas, dejando de lado la importancia de una gestión integral de la seguridad de la información. La investigación busca identificar cómo cerrar la brecha entre las prácticas administrativas y las técnicas de ciberseguridad, y proponer un modelo de gestión que optimice la toma de decisiones ante incidentes de *ransomware.*

2.2 Objetivos de investigación

Objetivo General

Diseñar una arquitectura de gestión para la prevención, mitigación y respuesta ante ataques de *ransomware* Medusa en organizaciones, principalmente pymes (pequeñas y medianas empresas), que permita identificar los principales vectores de ataque, incorporar las mejores prácticas de gestión de riesgos y establecer un modelo integral basado en metodologías reconocidas, con el fin de fortalecer la resiliencia organizacional frente a amenazas cibernéticas.

Objetivos Específicos

1. Identificar los principales vectores de ataque empleados por el *ransomware* Medusa mediante el análisis de incidentes previos, estudios de casos y fuentes académicas, con el propósito de localizar al menos tres métodos o canales de propagación que las organizaciones deben prevenir para mitigar los riesgos asociados.
2. Evaluar las mejores prácticas de gestión de riesgos frente a ataques de *ransomware* con el fin de proponer al menos cinco estrategias clave basadas en informes de expertos, estudios de ciberseguridad y análisis de casos reales que han demostrado ser eficaces para prevenir, detectar y mitigar estos incidentes en las organizaciones.

3. Definir un modelo de respuesta administrativa a incidentes de Medusa, basado en metodologías reconocidas como ITIL (*Information Technology Infrastructure Library*), NIST (*National Institute of Standards and Technology*) e ISO 27001 (*International Organization for Standardization*), que incluya al menos cuatro fases: preparación, detección, respuesta y recuperación, con el fin de ofrecer un enfoque integral para fortalecer la resiliencia organizacional frente a ataques cibernéticos.

2.3 Preguntas de investigación

- ¿Cuáles son los principales vectores de ataque empleados por el *ransomware* Medusa?
- ¿Cómo contribuye la gestión de riesgos a la respuesta organizacional ante ataques de *ransomware?*
- ¿Qué estrategias administrativas pueden implementarse para prevenir, detectar y mitigar los ataques de *ransomware* en las organizaciones?

2.4 Meta de ingeniería

Como resultado de este proyecto en Ingeniería de Computación, se desarrollan productos que contribuyen directamente a la gestión de la ciberseguridad, a la seguridad de la información en las pequeñas y medianas empresas. Uno de los elementos más sobresalientes es una arquitectura de gestión administrativa, diseñada según las mejores prácticas de NIST, ISO/IEC 27001 e ITIL, que establece procesos y controles para la gestión del riesgo asociado al *ransomware* Medusa. Además, una matriz de indicadores de gestión de ciberseguridad que permitirá evaluar el nivel de madurez y la efectividad de los controles administrativos de ciberseguridad en las organizaciones, proporcionando métricas que facilitan la toma de decisiones y la mejora continua de la resiliencia operativa.

2.5 Justificación

De acuerdo con (NIST Special Publication, 2025) existe un creciente número de ataques de *ransomware* a nivel mundial respecto al año 2024. La falta de estrategias administrativas integrales para gestionar eficazmente estos incidentes constituye uno de los principales motivos para realizar este estudio. A diferencia de los enfoques puramente técnicos, esta investigación pone énfasis en la gestión organizacional y la toma de decisiones desde un marco administrativo, reconociendo que la ciberseguridad no es solo un asunto tecnológico, sino también de gobernanza.

Con este enfoque, la investigación busca contribuir a mejorar la preparación institucional mediante la propuesta de criterios administrativos que fortalezcan la prevención, la respuesta y la recuperación ante amenazas como el *ransomware* Medusa. De este modo, se busca mejorar la resiliencia empresarial frente a ciberataques, promoviendo una cultura organizacional más consciente, estratégica y proactiva en materia de ciberseguridad.

2.6 Impactos

- Científico: Contribuir al conocimiento sobre la relación entre la administración y la ciberseguridad, desarrollando metodologías aplicables a distintos sectores.
- Tecnológico: Proveer recomendaciones para mejorar las herramientas de gestión de riesgos y la respuesta ante incidentes de ataques cibernéticos, como el *ransomware* Medusa.

3 MARCO TEÓRICO

En este apartado se presentan las bases teóricas y conceptuales indispensables para el desarrollo de la investigación documental que integra este proyecto. El propósito principal es presentar los antecedentes y las bases del diseño del marco administrativo en relación con el *ransomware* Medusa.

3.1 Ransomware

Las Tecnologías de la Información (TI) abarcan esencialmente todos los aspectos de la informática dentro de la empresa, incluyendo el estudio, la conceptualización, el desarrollo, la implementación y el soporte de los sistemas de información (ServiceNow, 2025). El término TI se utiliza para referirse al departamento encargado de la instalación y el mantenimiento de los sistemas de redes informáticas en una empresa.

Ransomware se define como un tipo de software dañino diseñado para restringir el acceso a sistemas o información con fines de extorsión cibernética, y está compuesto por "*ransom*" y "*software*" que se traducen como "*software* de rescate". Este *malware* se ha convertido en una preocupación para los profesionales de TI (Pérez Castro, 2020). En términos simples, es una aplicación creada y difundida por delincuentes cibernéticos que puede infectar un sistema y encriptar sus archivos mediante un potente algoritmo de cifrado, con el objetivo de extorsionar al administrador pidiéndole un pago para recuperar sus datos.

Existen diversos tipos de *ransomware,* dentro de los que destacan los siguientes (Baker, 2025):

- *Ransomware* criptográfico o cifradores: Este tipo cifra los archivos y datos de un sistema, haciendo que el contenido quede inaccesible sin una clave de descifrado.
- Taquillas: Los bloqueos impiden el acceso al sistema, por lo que los archivos y aplicaciones quedan inaccesibles. Una pantalla de bloqueo muestra la exigencia de un rescate, posiblemente con una cuenta regresiva para aumentar la urgencia e incitar a las víctimas a actuar.

- *Scareware*: es software falso que afirma haber detectado un virus u otro problema en la computadora y solicita un pago para solucionarlo. Algunos tipos de scareware bloquean la computadora, mientras que otros simplemente inundan la pantalla de alertas emergentes sin dañar los archivos.
- *Doxware:* software de fugas: amenaza con distribuir información confidencial, personal o empresarial en línea, y muchas personas, presas del pánico, pagan el rescate para evitar que sus datos privados caigan en manos indebidas o se hagan públicos.
- RaaS (*Ransomware* como servicio): se trata de un tipo de *malware* en el que un ciberdelincuente con experiencia desarrolla y mantiene el modelo, encargándose de toda la infraestructura del ataque (difusión, gestión de pagos y soporte a víctimas). Otros atacantes, con menos conocimientos técnicos, pueden utilizar este servicio para ejecutar ataques y entregar al creador un porcentaje de las ganancias obtenidas.

3.2 Extorsión cibernética

La extorsión cibernética es una categoría de delito cibernético que consiste en amenazar o coaccionar digitalmente a alguien para que haga algo en contra de su voluntad (Treviño, Cutler, & Guccione, 2025). Es una conducta en la que los actores crean amenazas y explotan vulnerabilidades de seguridad para atacar sistemas de seguridad digital y obtener acceso no autorizado a activos valiosos. Entre los principales tipos de extorsión se encuentran los siguientes (Paloalto Networks, 2025):

Doble extorsión: Además de cifrar los archivos de la víctima, el *ransomware* de doble extorsión añade una segunda capa al ciberataque: el operador del *ransomware* filtra los archivos y amenaza con publicar los datos de la víctima a menos que se pague el rescate. Esta amenaza aumenta la presión sobre la víctima para que pague el rescate a tiempo y dificulta que se niegue a pagar.

Los ataques de *ransomware* de doble extorsión pueden ser particularmente dañinos porque interrumpen la capacidad de la víctima de acceder a sus propios datos y, al mismo tiempo, exponen potencialmente información sensible o confidencial al público.

Triple extorsión: Implica otra capa de ataque, además del cifrado de archivos y del robo de datos. Un vector de ataque común es la interrupción del servicio (por ejemplo, un ataque DDoS, *distributed denial-of-service)*. Además de la pérdida y la exposición de datos, la víctima podría verse también amenazada por operaciones críticas.

Otra capa de ataque que está ganando popularidad entre los grupos de *ransomware* es la extorsión a socios externos o terceros vinculados a la organización víctima. En este ejemplo de triple extorsión, el atacante extiende las amenazas y las exigencias de rescate a los clientes, proveedores u otros socios de la víctima original.

3.3 Tipos de cifrados

El cifrado en ciberseguridad consiste en la conversión de datos de un formato legible a otro codificado. Los datos cifrados solo pueden leerse o procesarse después de descifrarlos. Hay dos variantes principales de cifrado: el simétrico y el asimétrico. El cifrado simétrico se caracteriza por utilizar una clave única para cifrar y descifrar los datos. Cuando se deben cifrar rápidamente grandes cantidades de datos, el cifrado simétrico suele ser la opción preferida (Gitlan, 2025). Algunos algoritmos populares de encriptación simétrica son:

- **AES (Estándar de Cifrado Avanzado)**: Conocido por su alta seguridad y velocidad, el AES se utiliza ampliamente en aplicaciones gubernamentales, militares y comerciales. El uso de algoritmos como AES en *ransomware* como Medusa evidencia un alto nivel de sofisticación, lo que dificulta la recuperación de la información sin la clave correspondiente.
- **DES (Estándar de Cifrado de Datos)**: Aunque fue sustituido en gran medida por AES debido a su menor seguridad, DES sentó las bases de muchos sistemas de cifrado.
- ***Blowfish***: Un método de encriptación rápido y compacto que se utiliza con frecuencia en aplicaciones de software en las que la alta velocidad es fundamental.

Para comprender cómo se protege la información en las redes actuales, es necesario conocer dos protocolos fundamentales. El primero, *Secure Sockets Layer* (SSL), es un protocolo de comunicación, o conjunto de reglas, que establece una conexión segura entre dos dispositivos o aplicaciones de una red. En comparación, el segundo protocolo se basa en la seguridad de la capa de transporte (TLS), es la versión mejorada de SSL donde ya están corregidas las vulnerabilidades (Amazon Web Services, Inc., 2025).

SSL y TLS son protocolos que protegen la comunicación cifrando la información que circula entre servidores, aplicaciones, usuarios y otros sistemas. Su función es verificar la identidad de ambas partes conectadas a la red y permitir el intercambio de datos de forma segura.

Una forma de encriptación se realiza mediante clave asimétrica, que utiliza una clave pública y otra privada para encriptar y desencriptar datos. Este método elimina la necesidad de compartir la misma clave, ya que la clave pública se utiliza para cifrar y la clave privada para descifrar. El cifrado asimétrico, también conocido como criptografía de clave pública, se utiliza habitualmente para comunicaciones en línea seguras, firmas digitales y protocolos SSL/TLS para establecer conexiones seguras entre navegadores web y servidores.

Por otro lado, el descifrado es el proceso inverso del cifrado. Consiste en transformar los datos previamente codificados a su formato original, de modo que la información vuelva a ser legible y utilizable por los usuarios autorizados. Este proceso depende del tipo de cifrado empleado, tal como se mencionó anteriormente.

3.4 Medusa

Medusa es un servicio de *ransomware* del tipo RaaS que surgió a finales de 2021 y cobró notoriedad en 2022 al enfocarse en entornos de Windows. MedusaLocker, la variante predecesora, apareció en septiembre de 2019; ambos son tipos de *ransomware* que cifran los archivos de la víctima y exigen un rescate para descifrarlos (Lakshmanan, 2024).

Se trata de un tipo de software malicioso que bloquea o cifra los archivos de un usuario, impidiendo el acceso a ellos, y posteriormente exige el pago de un rescate a cambio de

restaurar su disponibilidad. Utilizan AES-256, una técnica de cifrado simétrico que vuelve los archivos ilegibles si no se cuenta con la clave, y es tan segura que hace casi imposible recuperarlos sin ella. Además, emplea la técnica de doble extorsión: no solo cifra los datos para impedir el acceso, sino que también los extrae (exfiltración). Posteriormente, exige un pago tanto para restaurar la información como para evitar que los datos robados sean publicados, vendidos o filtrados, ya sea en internet o en la web oscura.

En la etapa final del ciclo de vida de un ataque de Medusa, los atacantes identifican y sustraen información confidencial, que envían a sus servidores de comando y control. Este proceso, conocido como *callback*, puede ocultarse mediante puertos de comunicación comunes y técnicas, como registros DNS de texto o paquetes ICMP, con el objetivo de evadir los mecanismos de detección de seguridad tradicionales.

En 2023, Medusa comprometió a más de 74 organizaciones en todo el mundo, afectando a sectores como la tecnología, la educación, la manufactura y las telecomunicaciones. Su presencia también se hizo notar en Latinoamérica, donde se registraron incidentes importantes, como el ataque masivo en Colombia en septiembre de ese año, el caso de la Comisión Nacional de Valores en Argentina en noviembre de 2023 y un presunto ataque dirigido a una empresa de telecomunicaciones en Venezuela, lo que refleja su creciente expansión en la región.

Hasta febrero de 2025, tanto los desarrolladores como los afiliados de Medusa habían comprometido a más de 300 organizaciones pertenecientes a distintos sectores de la infraestructura crítica, incluidos la medicina, la educación, el derecho, los seguros, la tecnología y la manufactura (Cibersecurity & Infraestructure Security Agency , 2025).

Medusa es un RaaS que actúa mediante la exfiltración de datos; es decir, tras ingresar al sistema, roba los datos y no solo amenaza con publicarlos en un portal llamado “Medusa Blog” en la Dark Web, sino que lo hace y pide un rescate en criptomonedas, que, aunque se pague, no garantiza la integridad de los datos. Según lo señalado por Castillo G. 2025 (comunicación personal, 27 de julio de 2025), la siguiente sección muestra la cadena de infección y el impacto que genera, información que se detalla en la Tabla 3.1.

Tabla 3.1 Cadena de infección Medusa

Fase	**Qué hace**
Infección inicial	Phishing, RDP, Explotación de vulnerabilidades
Ejecución y persistencia	Descarga payload, instalación
Escalamiento de privilegios y movimiento lateral	Elevación de privilegios, movimiento lateral
Cifrado de Archivos	Uso de AES/RSA, eliminación de copias, cifrado masivo, notas de rescate.
Comunicación con C2	Envía información, recibe órdenes, exfiltración de datos
Extorsión	Amenazas con filtración de datos, pago en criptomonedas
Recuperación de datos	Restauración parcial o total, o pérdida de información

En la Figura 3.1 se presenta un gráfico tipo "Medusa" que muestra las palabras clave asociadas a este ransomware, lo que permite visualizar de forma gráfica los conceptos más relevantes. Esta representación destaca los términos que aparecen con mayor frecuencia en la investigación, facilitando la identificación de temas clave como infección, cifrado, impacto, vectores de ataque y medidas de mitigación. El propósito es ofrecer una perspectiva rápida y contextual del comportamiento y alcance de este tipo de amenaza, ayudando a comprender de qué trata y cuáles son los elementos fundamentales que lo caracterizan.

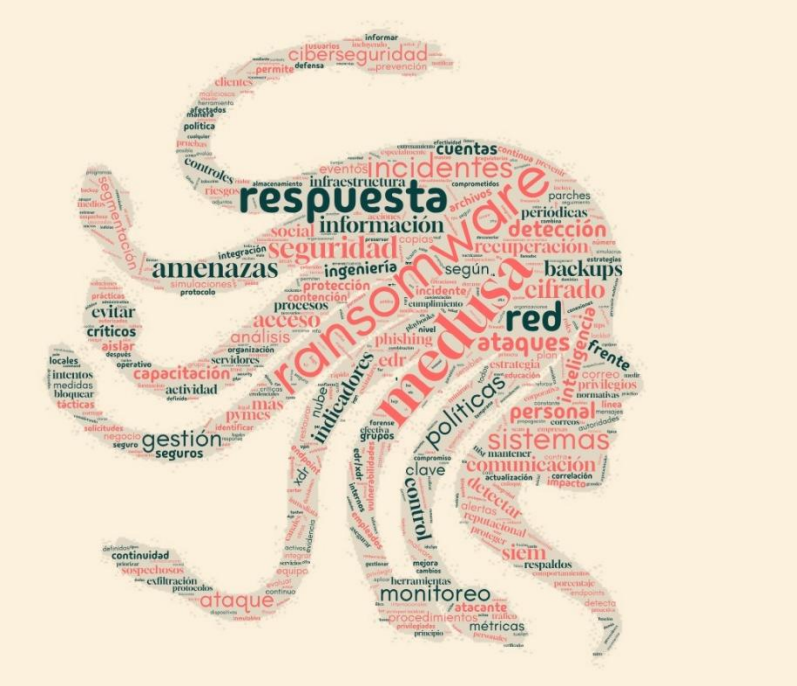

Figura 3.1. Nube de palabras relacionadas con el ransomware Medusa (elaboración propia).

3.5 Gestión de riesgos en ciberseguridad

En esta sección se presentan algunos aspectos sobre los riesgos en ciberseguridad, destacando los conceptos y técnicas más conocidas sobre la identificación y análisis de amenazas, los métodos más conocidos sobre evaluación de riesgos y también las estrategias de mitigación y reducción de riesgos

3.5.1 Identificación y análisis de amenazas

La identificación y el análisis de amenazas son el primer paso en la gestión de riesgos en ciberseguridad. Este proceso implica identificar posibles amenazas que puedan afectar la infraestructura de TI, como *malware*, ataques de *phishing* y *ransomware.* Además, es crucial realizar un análisis detallado para comprender cómo estas amenazas podrían explotar vulnerabilidades y qué impacto tendrían en la organización. El análisis de amenazas es fundamental para priorizar las acciones de mitigación y prevención.

3.5.2 Métodos para evaluar riesgos

Evaluar riesgos implica determinar la probabilidad de que una amenaza se materialice y el impacto potencial de dicha amenaza en los activos de la organización. Los métodos comunes de evaluación de riesgos incluyen la matriz de riesgos, que clasifica los riesgos según su probabilidad e impacto, y el análisis cualitativo y cuantitativo de riesgos, que evalúa la severidad y la probabilidad de un riesgo con base en datos históricos y modelos matemáticos.

Uno de los marcos más utilizados es el *NIST Risk Management Framework* (RMF), que ofrece un enfoque detallado para evaluar y gestionar riesgos. El Marco de Ciberseguridad del NIST (CSF) 2.0 proporciona orientación para gestionar los riesgos de ciberseguridad al ayudar a las organizaciones a comprender, evaluar, priorizar y comunicar de manera consistente los esfuerzos de ciberseguridad, incluidos los relacionados con la fuerza laboral en ciberseguridad (NIST Special Publication, 2025).

El NIST reconoce que los riesgos de ciberseguridad son solo una parte de los riesgos empresariales globales y deben gestionarse en conjunto, y que se deben contemplar riesgos negativos como pérdidas, daños, reputación, interrupciones, pero también, los riesgos positivos, como lo son las oportunidades derivadas de activos empresariales dentro del portafolio global de riesgos.

Uno de los principales puntos que destaca el NIST son las brechas de personal, entre las cuales se encuentran las habilidades y las competencias, ya que en la ciberseguridad constituyen riesgos en sí mismas. Esto implica que la estrategia de personas, procesos y tecnología debe considerarse para alcanzar niveles aceptables de riesgo.

Tomar en cuenta que la evaluación de riesgos globales también es importante, no solo los riesgos técnicos; en cuanto a la gestión de talento es importante tener en cuenta ciertos puntos como las habilidades, los roles y las brechas de conocimiento; la alineación entre negocio, ciberseguridad y recursos humanos, todo esto con la finalidad de abarcar aquellos puntos vulnerables que no siempre se tienen en cuenta y que son puntos blancos para atacar.

3.5.3 Estrategias de mitigación y reducción de riesgos

Según la información publicada por el National Institute of Standards and Technology - NIST (2024), las estrategias de mitigación y reducción de riesgos buscan disminuir la probabilidad de que ocurra un riesgo o minimizar su impacto. Estas estrategias pueden abarcar la implementación de controles técnicos, como cortafuegos y sistemas de detección de intrusiones, así como la realización periódica de copias de seguridad, y la aplicación de controles administrativos, como la capacitación del personal en buenas prácticas de ciberseguridad.

También es común emplear enfoques de defensa en profundidad, que integran múltiples capas de protección para asegurar que, si un control falla, otros controles estén disponibles para proteger la información.

La defensa en profundidad (DiD) es un enfoque de ciberseguridad que combina diversas medidas y buenas prácticas para salvaguardar la infraestructura de red, los servicios en línea y los activos de una organización. También se conoce como “seguridad por capas”, ya que integra controles de distintos tipos: físicos, tecnológicos y administrativos, para reducir el riesgo de que los atacantes accedan a sistemas protegidos o a información sensible (Cloudflare, 2025).

3.6 Marco Normativo y Estándares de Seguridad

La adopción de un modelo de ciberseguridad basado en las metodologías ISO 27001 y NIST fortalece la gestión de incidentes cibernéticos. Su implementación ha permitido un manejo eficiente de estos incidentes, que abarca la identificación, investigación, análisis, contención y eliminación de amenazas, así como la recuperación óptima de los sistemas afectados (Jimenez Huaman, 2024).

3.6.1 ISO 27001: Gestión de la seguridad de la información

Es un estándar internacional para la gestión de la seguridad de la información. Establece un sistema de gestión que protege la confidencialidad, la integridad y la disponibilidad de

los datos mediante un enfoque basado en la evaluación y mitigación de riesgos, que integra políticas, controles y procesos organizacionales.

Además, ISO 27001 enfatiza la implementación de controles preventivos y planes de continuidad que permiten mitigar el impacto de incidentes, como los ataques de ransomware, mediante políticas de respaldo, cifrado de la información y gestión de incidentes.

3.6.2 NIST Cybersecurity Framework: Identificación, protección, detección, respuesta y recuperación

Proporciona un conjunto de directrices para gestionar y reducir el riesgo cibernético. Se basa en cinco funciones clave: identificación, protección, detección, respuesta y recuperación, que ayudan a las organizaciones a anticiparse, prevenir y enfrentar incidentes de seguridad.

Cada función puede implementarse con medidas concretas para enfrentar el *ransomware:*

- Identificación: inventario de activos críticos y evaluación de riesgos.
- Protección: autenticación multifactor (MFA), firewalls y políticas de control de acceso.
- Detección: monitoreo continuo, análisis de logs y alertas del SIEM/EDR.
- Respuesta: planes de contención, comunicación de incidentes y análisis forense.
- Recuperación: restauración de sistemas, recuperación de datos y lecciones aprendidas.

3.6.3 NISTIR 8374 National Institute of Standards and Technology Interagency Report 8374

Es una guía oficial del NIST, titulada "*Ransomware Risk Management: A Cybersecurity Framework Profile*", que ayuda a las organizaciones a prevenir, detectar, responder y recuperarse de ataques de *ransomware.*

NISTIR 8374 proporciona directrices para adaptar el NIST CSF específicamente frente a ataques de *ransomware,* fortaleciendo la capacidad de anticipar, contener y recuperarse

de incidentes de cifrado malicioso. Permite priorizar los controles de prevención, la detección temprana, la respuesta rápida y la recuperación, lo que aumenta la resiliencia organizacional frente a amenazas como Medusa.

3.6.4 Regulaciones como GDPR y Leyes de Protección de Datos

Exigen a las organizaciones que gestionen y protejan la información personal de manera segura. Establecen principios como la transparencia, el consentimiento, la minimización de datos y el derecho a la eliminación, aplicables principalmente a las organizaciones que gestionan datos de ciudadanos de la Unión Europea.

En territorio mexicano, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) regula cómo las empresas, organizaciones o personas físicas deben recopilar, usar, almacenar y proteger los datos personales de cualquier individuo. Su objetivo principal es proteger los datos personales de los individuos, garantizando la privacidad, el derecho a la autodeterminación informativa y la seguridad de la información.

La LFPDPPP establece cómo deben tratarse los datos personales, cubriendo la recolección y el propósito, el uso correcto, ya que no pueden usarse con fines distintos a los informados, el almacenamiento seguro mediante medidas administrativas, técnicas y físicas y, por último, la transferencia de los datos, informando si se compartirán con terceros. Incluye los Derechos ARCO: derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales (Gobierno de México, 2025)

A pesar de la robustez de estos marcos, su implementación en pequeñas y medianas empresas presenta limitaciones debido a la falta de recursos, de personal especializado y de madurez organizacional, lo que dificulta su adopción completa en contextos reales, como el de un ataque de *ransomware* Medusa.

3.7 Plan de Respuesta a Incidentes

Las fases de gestión de incidentes son: detección, análisis, contención, erradicación y recuperación. Ante una respuesta a incidentes, existen herramientas fundamentales que

deben tenerse como barreras, entre ellas, se identifican principalmente XDR y MDR, que se detallan enseguida.

3.7.1 XDR

Detección y Respuesta Extendidas (XDR, por sus siglas en inglés) es una plataforma integrada de gestión de incidentes de seguridad que aprovecha la inteligencia artificial y la automatización para detectar, analizar y responder a las amenazas de manera más rápida y eficiente, proteger frente a ciberataques avanzados y responder a ellos (Microsoft, 2025).

A diferencia de la Detección y Respuesta de puntos de Conexión (EDR, por sus siglas en inglés), esta plataforma incrementa la capacidad de defensa frente a ciberataques avanzados al combinar herramientas de detección, análisis y respuesta, y abarca diversos entornos como *endpoints*, identidades híbridas, aplicaciones y cargas de trabajo en la nube.

XDR y EDR impulsan la eficiencia en las operaciones de seguridad (SecOps). Además, contribuyen a frenar los ciberataques al unificar de manera eficiente distintas herramientas de seguridad en una sola plataforma, superando los enfoques aislados tradicionales y fortaleciendo la protección, que abarca:

- Investigación centrada en incidentes: recopila alertas dispersas y las relaciona con incidentes específicos, ofreciendo una visión integral de cada posible ataque cibernético. Esto elimina la necesidad de revisar fragmentos de información aleatorios, aumentando la eficiencia y acelerando la respuesta.

Interrupción automática de ataques avanzados: mediante el uso de señales de seguridad de alta precisión y automatización integrada, identifica ataques en curso y ejecuta acciones de respuesta efectivas, como el aislamiento de dispositivos comprometidos.

-Visibilidad de la cadena de ciberataques: los analistas pueden ver la cadena completa de ciberseguridad de un ataque sofisticado.

-Reparación automática de activos afectados: restaura los recursos comprometidos por *ransomware, phishing* y campañas de correo empresarial a un estado seguro. Incluye acciones de recuperación como la finalización de procesos maliciosos, la eliminación de

reglas de reenvío no autorizadas y la contención de cuentas de usuario, liberando al equipo de tareas repetitivas y manuales.

-Aprendizaje automático e IA: escalable y eficiente. Detección, respuesta y mitigación automáticas. Permite crear perfiles de comportamiento sospechoso y marcarlos para su revisión.

¿Cómo funciona?

1. Recopila y normaliza datos: limpia, organiza y estandariza.
2. Analiza y correlaciona datos: identifica automáticamente y localiza un ciberataque en tiempo real.
3. Facilita la gestión de incidentes: da prioridad según la gravedad y proporciona más contexto.
4. Ayuda a prevenir incidentes en el futuro: información detallada relevante, como técnicas de ciberataque y acciones recomendadas.

Ventajas:

- Más visibilidad.
- Detección y respuesta de amenazas aceleradas
- Flujos de trabajo de SecOps simplificados
- Reducción de complejidad operativa
- Priorización de incidentes mejoradas
- Conclusiones de SOC más rápidas.

Componentes:

- Herramientas de detección y respuesta de puntos de conexión: EDR
- Aprendizaje automático e IA: detección de anomalías.
- Motor de análisis de seguridad

Casos de uso

- Búsqueda de ciberamenazas
- Investigación sobre incidentes de seguridad

- Analíticas e inteligencia sobre amenazas
- Suplantación de identidad y *malware* por correo electrónico.
- Amenazas internas

3.7.2 MDR

Detección y Respuesta Gestionadas (MDR), por sus siglas en inglés, se trata de un servicio de ciberseguridad diseñado para proteger de manera proactiva a las organizaciones frente a amenazas digitales, combinando capacidades de detección avanzada con respuestas rápidas ante incidentes (Microsoft, 2025).

MDR funciona mediante el monitoreo continuo de la red, los *endpoints* y los sistemas para detectar amenazas de forma temprana. Cuando se identifica un incidente, el equipo especializado responde rápidamente para contenerlo y mitigarlo. Además, proporciona informes y recomendaciones para fortalecer la seguridad de la organización.

Supervisión y respuesta a ciberamenazas; detección de amenazas realizada por especialistas; implementación de medidas para impedir la expansión de ataques cibernéticos; acciones de respuesta para neutralizar las amenazas; análisis de la causa raíz para prevenir recurrencias; y generación de informes de ciberseguridad. A diferencia de la detección y respuesta a amenazas (TDR), este es un servicio dirigido por humanos que administra las herramientas de ciberseguridad y los datos que proporcionan para buscar, investigar, corregir y neutralizar dichos datos.

Beneficios:

- Cobertura ininterrumpida: supervisión y protección continuas.
- Riesgo reducido: buscar, detectar y responder.
- Ciberseguridad eficiente en costos: permite proteger la organización sin necesidad de aumentar el personal de seguridad a tiempo completo.
- Optimización del cumplimiento: facilita la elaboración de informes y el seguimiento de normas y regulaciones.
- Disminución de la carga de TI

- Experiencia en seguridad mejorada: acceso rápido a analistas de seguridad altamente cualificados.

Casos de uso:

- Malware: detectar proactivamente las infecciones por software malicioso en los sistemas internos de la organización y aplicar medidas para mitigarlas.
- Suplantación de identidad: detección de ataques más complejos, como AiTM (ataque de intermediario), y de ataques que comprometen el correo electrónico empresarial.
- Cumplimiento normativo
- Ciber amenazas en la nube
- Ciberataques de movimiento lateral
- Ciberataques de red

3.7.3 Comparación entre MDR, XDR, MXDR, EDR y MSSP

MDR: es un servicio administrado que combina tecnología y experiencia humana.

XDR: (Detección y Respuesta Extendidas): solución SaaS que unifica productos y datos de seguridad en una plataforma simplificada. Está diseñada para organizaciones con entornos híbridos y multinube, pero no incluye un equipo de analistas humanos, a diferencia de los servicios MDR.

MXDR (Detección y Respuesta Extendidas Administradas): evolución de los servicios MDR. Es un servicio gestionado que combina tecnología XDR con experiencia humana, ampliando la protección en múltiples entornos de TI y ofreciendo una respuesta más rápida y eficaz que la MDR tradicional.

EDR (Detección y Respuesta de Puntos de Conexión): supervisa el comportamiento y los incidentes en los *endpoints*, utilizando automatización basada en reglas para responder a amenazas. Cuando detecta anomalías, envía alertas al equipo de seguridad para su investigación, apoyándose en el aprendizaje automático, el análisis de comportamiento e integraciones con otras herramientas.

MSSP (Proveedor de Servicios de Seguridad Gestionados): antecesor de MDR, que ofrece supervisión y gestión de los sistemas de seguridad de una organización. Monitorea la red y los *endpoints*, enviando alertas al equipo interno de seguridad, pero sin intervenir activamente contra las amenazas.

3.7.4 SIEM

La Administración de Eventos e Información de Seguridad (SIEM) es una herramienta de seguridad que permite a las organizaciones identificar, analizar y responder a amenazas, protegiendo las operaciones del negocio antes de que se vean afectadas (Microsoft, 2025).

A diferencia de servicios como MDR, el SIEM no incorpora un componente humano en su operación. Ofrece a las organizaciones una visión completa de la actividad en su red, lo que les permite reaccionar rápidamente ante posibles ciberataques.

SIEM funciona recopilando, consolidando y analizando en tiempo real grandes volúmenes de datos provenientes de aplicaciones, dispositivos, servidores y usuarios de una organización, lo que permite a los equipos de seguridad identificar y bloquear posibles ataques. Sus capacidades y casos de uso son:

- Gestión de registros: centraliza cantidades grandes de datos, los organiza y evalúa en busca de indicios de amenazas, ataques o vulneraciones.
- Correlación de eventos: clasifica y relaciona los datos para identificar patrones y conexiones que puedan indicar amenazas potenciales, facilitando la respuesta oportuna.
- Monitoreo y respuesta a incidentes: supervisa la red en busca de incidentes de seguridad y proporciona alertas y auditorías detalladas de toda la actividad asociada a cada evento.

Ventajas:

- Visión unificada de las posibles amenazas.
- Detección y respuesta en tiempo real.
- Acceso a inteligencia avanzada sobre amenazas.
- Generación de informes y auditorías para garantizar el cumplimiento normativo.

Para implementarlo es necesario definir los requisitos del SIEM, realizar pruebas piloto, recopilar datos suficientes, establecer un plan de respuesta ante incidentes y optimizar continuamente la solución.

3.8 Herramientas de prevención y contención, acceso mediante roles

Las herramientas de gestión de acceso basadas en roles permiten controlar quién accede a qué recursos dentro de una organización, lo que fortalece la seguridad y reduce los riesgos. En conjunto, estas herramientas previenen movimientos laterales, reducen la superficie de ataque y refuerzan la contención ante incidentes de ciberseguridad.

3.8.1 IAM

Administración de identidad y acceso (IAM). Es un método para gestionar y restringir el acceso de los usuarios, asegurando que solo las personas y dispositivos autorizados puedan acceder a las funciones y los datos confidenciales necesarios para su trabajo (Microsoft, 2025).

IAM garantiza que solo las entidades verificadas pueden acceder de forma segura a los recursos de la empresa, como correos electrónicos, bases de datos, información y aplicaciones, minimizando las interrupciones. Su propósito es administrar el acceso de modo que los usuarios autorizados puedan realizar su trabajo mientras se bloquea a actores malintencionados, como los hackers.

La administración de identidades comprueba un intento de acceso a una base de datos, que es un registro continuo de todos los que deberían tener acceso. Este proceso asegura que solo las personas y servicios autorizados interactúen con los recursos de la organización, mediante la autenticación y la autorización, como lo mencionan en el marco (National Institute of Standards and Technology - NIST, 2024).

Autenticación: proceso mediante el cual las organizaciones verifican que solo las personas, servicios o aplicaciones autorizadas, con los permisos adecuados, puedan acceder a los recursos de la empresa. La administración de acceso supervisa y controla a qué recursos tiene permitido acceder un usuario o dispositivo.

Autorización: consiste en otorgar el nivel de acceso correspondiente una vez confirmada la identidad del usuario.

Ventajas:

- Acceso necesario para las personas adecuadas: control de acceso basado en roles (RBAC).
- Productividad sin límites: inicio de sesión único (SSO)
- Protección de vulnerabilidades de datos: confirmar la identidad del usuario y añadir una capa adicional de protección durante el proceso de inicio de sesión.
- Cifrado de datos: acceso condicional
- Menos trabajo manual de TI: automatizaciones- confianza cero (verificación explícita, privilegios al mínimo y suposición de vulneración)
- Colaboración y eficacia mejoradas
- Tecnologías y herramientas:
- OpenID Connect (OIDC) agrega un componente de identidad y un marco de autorización basado en tokens.
- System for Cross-Domain Identity Management (SCIM)

3.8.2 PAM

Privileged Access Management (PAM) supervisa, detecta y evita el acceso con privilegios no autorizado a recursos críticos (Microsoft, 2025). PAM combina personas, procesos y tecnologías para ofrecer visibilidad sobre quiénes utilizan cuentas con privilegios y cómo interactúan con los sistemas durante sus sesiones. Sus funciones y beneficios principales son:

- Restringe el número de usuarios con acceso a funciones administrativas, aumentando la seguridad y aplicando capas de protección para prevenir filtraciones de información por parte de actores maliciosos.
- Identifica a las personas, procesos y tecnologías que tienen acceso con cierto nivel de privilegios, y establece las políticas correspondientes.
- Otorga acceso a recursos críticos únicamente cuando es necesario.

- Facilita el acceso remoto seguro mediante puertas de enlace cifradas eliminando el acceso mediante contraseñas tradicionales.
- Supervisa las sesiones con privilegios para auditorías e investigaciones detalladas.
- Analiza actividades inusuales con privilegios que puedan representar riesgos para la organización.
- Registra los eventos de las cuentas privilegiadas para cumplir con auditorías de normativa y cumplimiento.
- Genera informes sobre el acceso y la actividad de los usuarios con privilegios.
- Integra seguridad en entornos DevOps mediante la gestión de contraseñas.

Existen diferentes niveles de cuentas, según sus privilegios, tales como: cuentas con privilegios, de servicio, administrador de dominio, de usuario con privilegios de empresa, de administrador local, de emergencia, de administrador de aplicaciones.

3.8.3 EPM

El perímetro de seguridad ampliado (EPM) emplea el modelo *Zero Trust*, un enfoque de ciberseguridad moderno basado en la premisa de "nunca confiar, siempre verificar" y que asume que cualquier sistema puede verse comprometido. La gestión de privilegios de *endpoints* elimina los riesgos en los *endpoints* mediante una combinación de privilegios mínimos (los usuarios obtienen sólo el acceso que necesitan) y control de aplicaciones (las aplicaciones no autorizadas se restringen o bloquean) (One Identity, 2025).

La mayoría de los productos EPM incluyen funciones útiles, como la administración de sesiones, de identidad y de acceso (IAM). Pueden monitorear y registrar las sesiones de los usuarios en los puntos finales, lo que permite auditar las actividades privilegiadas. Los puntos finales son objetivos primordiales: protegerse contra el error humano y mitigar la amenaza de escalada de privilegios.

4 ESTADO DEL ARTE

En la Tabla 4.1 se presenta el resumen de la matriz de referencias, que integra una selección de trabajos previos relacionados con el desarrollo de proyectos de gestión de incidentes de ciberseguridad. Cada referencia incluida describe la metodología empleada por sus autores, así como los enfoques prácticos utilizados para abordar amenazas similares.

Asimismo, se destacan las principales oportunidades de mejora identificadas en dichos estudios, lo que permitió identificar vacíos metodológicos y áreas que este protocolo busca fortalecer. Esta matriz sirve como fundamento comparativo para sustentar la pertinencia y la originalidad del marco propuesto.

De manera general, se pudo ver que los autores Klappholz (2025), Watch (2025), así como las empresas SISA (2025) y la American Hospital Association (2025), coinciden en que Medusa es una de las familias de *ransomware* más activas de los últimos años, caracterizada por el uso de doble extorsión, exfiltración de datos previa al cifrado y modelos de negocio sobre servicio, *Ransomware as a Service* (RaaS). La mayoría de los estudios se destacan por incluir que Medusa aprovecha vulnerabilidades conocidas, y más las que están en aplicaciones expuestas a internet.

Los estudios revisados por Teichmann & Boticiu (2024) muestran énfasis en el impacto organizacional en pérdidas financieras, interrupción operativa, daños reputacionales y afectación a sectores críticos como salud, educación, servicios financieros y pequeñas y medianas empresas. Además, existe un acuerdo sobre la necesidad de marcos de prevención y respuesta mejor estructurados para las tareas de mitigación y emisión de alertas.

Blancaflor (2025) y Ribeiro (2025), apuntan hacia la urgencia de contar con planes de respuesta a incidentes más robustos, mejores prácticas de segmentación de red, reforzamiento de identidad y accesos, e implementación de monitoreo continuo. Sin embargo, también describen con frecuencia la rápida evolución del *ransomware,* lo que genera brechas importantes entre las recomendaciones y la realidad operativa de las organizaciones.

Mientras que el trabajo de Schuster (2023) se centra en una operación gubernamental para neutralizar el *malware* Snake, los artículos de Bravo (2025) y Olyniychuk (2025) analizan específicamente el *ransomware* Medusa desde una perspectiva descriptiva y de inteligencia de amenazas.

En conjunto, los tres trabajos resaltan el papel de las agencias de seguridad y de los análisis técnicos para comprender y enfrentar el cibercrimen, aunque difieren en su enfoque: uno aborda la respuesta operativa contra el *malware*, mientras que los otros dos se centran en el análisis de la amenaza y en estrategias de detección y prevención.

1 *Tabla 4.1 Matriz de referencias para determinar el estado del arte.*

Fuente	**Resumen**	**Metodología**	**Áreas de oportunidad**
El *ransomware* Medusa y la privacidad de datos: un estudio exhaustivo de los ataques de *ransomware* en diversas organizaciones y recomendaciones estratégicas para su prevención en el futuro (Blancaflor, Bauson, Cruz, & Escandor, 2025)	Este estudio analiza sus orígenes, métodos de propagación y características, destacando su cifrado y alcance global. El documento estudia la dinámica operativa del Grupo Medusa	Se presentan casos reales de ataques, como los sufridos por el Distrito Escolar Estatal de Minneapolis, PhilHealth y Toyota Financial Services Análisis de orígenes, métodos de propagación, tácticas de LOTL, vulnerabilidades como ProxyShell, y estudio de casos reales de afectación.	Desarrollar modelos predictivos para la detección temprana de Medusa. Investigación sobre políticas de privacidad ante ataques. Propuestas para fortalecer la ciberseguridad en sectores vulnerables.
Los ataques de *ransomware* más impactantes en 2023 y sus implicaciones comerciales (Teichmann & Boticiu, 2024)	El artículo examina el impacto financiero, operativo y reputacional de un ataque de *ransomware,* y ofrece medidas proactivas para mitigar daños.	Análisis de ciberataques notables, evaluación de costos directos e indirectos de *ransomware,* y revisión de medidas de seguridad preventivas.	Desarrollo de estrategias preventivas enfocadas en sectores específicos. Propuestas de modelos de recuperación rápida y costo-efectiva. Mejora de la gestión de la reputación tras un ataque.
Estados Unidos expone la amenaza del *ransomware* Medusa tras más de 300 ataques en el sector de infraestructura crítica (Ribeiro, 2025)	El artículo describe tácticas y estrategias de *ransomware* Medusa, enfocándose en la propagación, exfiltración de datos, y medidas de mitigación recomendadas.	Análisis de TTP, IOC, y estrategias de detección a través de alertas de agencias gubernamentales (CISA, FBI, MS-ISAC) y estudios de ataques. Desarrollo de mejores prácticas de formación de usuarios para prevenir ataques de ingeniería social.	Investigación sobre el modelo RaaS y sus implicaciones en ciberseguridad. Análisis de técnicas de doble y triple extorsión para su inclusión en un marco de respuesta ante incidentes. Estrategias para proteger vulnerabilidades específicas como RDP y software sin parchear.

El *ransomware* Medusa alcanza niveles récord; el FBI y la CISA brindan información clave sobre seguridad (CYBLE, 2025)	En 2025, incidentes relacionados con Medusa aumentaron, con 60 afectados en los primeros 72 días. Se sugiere establecer prácticas de ciberseguridad para reducir estos peligros.	El FBI y CISA publicaron una advertencia describiendo sus métodos, que abarcan el empleo de software legítimo para realizar movimientos laterales y estrategias de elusión	Capacitación no técnica del personal directivo con protocolos administrativos. Planes formales de respuesta a incidentes.
CISA emite una advertencia sobre el *ransomware* Medusa después de que 300 víctimas de sectores críticos se vieran afectadas (Klappholz, 2025)	CISA y el FBI advierten que Medusa ha afectado a más de 300 organizaciones críticas en EE. UU. desde 2021. El grupo opera como *Ransomware-as-a-Service*,	El asesoramiento conjunto de CISA, el FBI y MS-ISAC proporcionó una serie de mitigaciones que las empresas pueden implementar para mejorar su postura de ciberseguridad.	Gestión de vulnerabilidades, monitoreo de la integridad del sistema y capacitación del personal, utilizando vulnerabilidades en aplicaciones expuestas y técnicas como BOYVD para evadir defensas.
El *ransomware* Medusa causó más de 40 víctimas en 2025 y exigió rescates de hasta 15 millones de dólares (SISA, 2025)	Medusa afectó a 400 en 2025 mediante doble extorsión y fallas en Microsoft Exchange. Peligros como el troyano TgToxic, ataques BYOVD, y campañas de *phishing.*	Técnica BYOVD (Bring Your Own Vulnerable Driver) para deshabilitar software de seguridad Uso de herramientas legitimas como Living Off The Land.	Gestión de parches y vulnerabilidades críticas, defensa contra *malware* móvil, protección contra *phishing* avanzado y segmentación de red y monitoreo continuo.
Un aviso advierte sobre la actividad del *ransomware* Medusa (American Hospital Association, 2025)	El *ransomware* Medusa ha usado doble extorsión y vulnerabilidades conocidas. Ha atacado sectores críticos, como la salud y la educación.	Análisis documental, y de aplicación en casos de uso. Informes y estadísticas sobre el robo y cifrado de datos, la explotación de credenciales y el aprovechamiento de vulnerabilidades conocidas en sistemas.	Gestión de parches de manera ágil, fortalecer seguridad de la gestión de accesos, segmentación de redes y mejor integración de inteligencia de amenazas. FBI, CISA y CIIC recomiendan aplicar parches,

			segmentar las redes y fortalecer la gestión de identidades para prevenir y mitigar los daños.
Operación MEDUSA: Los federales cortaron la cabeza de la herramienta de ciber espionaje rusa "Snake", dirigida a empresas y periodistas estadounidenses (Schuster, 2023).	Operación conjunta entre la agencia de seguridad para desmantelar la infraestructura del *malware* “Snake”	Identificación y análisis de infraestructura, ingeniería inversa, desarrollo de herramienta de neutralización,	Mejora en capacidades de monitoreo y análisis continuo, protocolos de respuesta, campañas de concientización en sectores no técnicos,
Ransomware Medusa: cómo opera y por qué genera preocupación. (Bravo, 2025)	Explica por qué este grupo se ha convertido en una amenaza relevante para las organizaciones y resalta la necesidad de fortalecer las medidas de ciberseguridad.	Análisis descriptivo, casos reales de ataques, datos de organismos oficiales y reportes de empresas de ciberseguridad.	Mayor respaldo académico, comparaciones con otros grupos de *ransomware* y un análisis más profundo del impacto y las estrategias de prevención.
Detección de *Ransomware* Medusa: El FBI, CISA y Socios Advierten sobre el Aumento de Ataques por Desarrolladores de *Ransomware* y Afiliados Contra Infraestructuras Críticas. (Olyniychuk, 2025)	Analiza el crecimiento del *ransomware* Medusa y su impacto en organizaciones a nivel mundial. Señala que el costo promedio de recuperación por ataques de *ransomware* alcanzó 2,73 millones de dólares en 2024	Información de organismos oficiales, inteligencia de amenazas, detección y defensa,	Análisis de impacto organizacional, perspectiva estratégica de ciberseguridad, claridad para audiencias no técnicas.

2

De acuerdo con lo presentado, se reconoce una tendencia clara según la cual los estudios coinciden en que la falta de preparación de las organizaciones, la gestión deficiente de parches, la baja madurez en ciberseguridad y la alta susceptibilidad al *phishing* son los principales factores que facilitan la entrada del *ransomware* Medusa. Además, todos resaltan la importancia del usuario como principal vector de compromiso, por lo que la capacitación continua se presenta como una recomendación constante.

A partir del análisis realizado, se identifica que, aunque existen múltiples estudios sobre ransomware Medusa, estos se centran en aspectos técnicos y de detección, dejando una brecha en la integración de modelos administrativos aplicados a pymes. Por ello, esta investigación propone un enfoque integral que abarca la gestión de riesgos y la respuesta organizacional. Esta ausencia de un marco unificado incrementa la dependencia de cada organización respecto de su nivel de madurez, así como la rapidez con la que puede coordinar esfuerzos con especialistas o agencias externas.

Por lo tanto, el análisis evidencia una oportunidad crítica de mejora: la necesidad de diseñar un marco de actuación integral y específico contra Medusa, que consolide buenas prácticas de prevención, detección y respuesta, y resulte aplicable a organizaciones de distintos tamaños y niveles de madurez. Este vacío metodológico justifica la creación de un modelo más claro, ordenado y práctico, como el que se plantea en el presente protocolo.

5 METODOLOGÍA

La presente investigación es de tipo aplicado, con enfoque mixto (cualitativo y cuantitativo) y diseño no experimental, ya que analiza el fenómeno en un periodo determinado, sin manipular variables. El estudio se desarrolla mediante el análisis de casos reales de Medusa y entrevistas a expertos, con el objetivo de diseñar un marco de gestión de riesgos basado en metodologías reconocidas, como NIST e ISO 27001.

El desarrollo metodológico del proyecto se organiza en las siguientes etapas:

Actualización del estado del arte: se realizó una revisión documental para contextualizar el estudio, analizando fuentes académicas, normas y buenas prácticas en la gestión de incidentes de ciberseguridad, lo que permitió establecer una base teórica sólida.

Recolección de datos: se recopilaron datos mediante encuestas a profesionales de tecnologías de la información, entrevistas a expertos en ciberseguridad y análisis de casos de incidentes de *ransomware*.

Verificación de la información: los datos recolectados se evaluaron para determinar su suficiencia y relevancia para el análisis. En caso de ser necesario, se amplió la recolección de información.

Análisis de datos: los datos cuantitativos se analizaron mediante estadística descriptiva, mientras que la información cualitativa se interpretó mediante categorización temática, lo que permitió identificar patrones, tendencias y percepciones relevantes.

Elaboración de la propuesta: con base en los resultados obtenidos, se diseñó un marco de gestión de riesgos que integra procesos, roles y estrategias para responder a incidentes.

Evaluación del modelo: la propuesta fue revisada considerando las fases de respuesta a incidentes: preparación, detección y análisis, contención, erradicación y recuperación.

Ajustes y rediseño: en caso de ser necesario, la propuesta fue ajustada para cumplir con los criterios establecidos.

Conclusiones y recomendaciones: se presentan los hallazgos del estudio junto con recomendaciones para la implementación del marco propuesto.

En la fase cuantitativa, se aplicaron encuestas a 100 profesionales de tecnologías de la información mediante un muestreo no probabilístico por conveniencia (o intencional), debido a la accesibilidad de los participantes y su relación con el área de estudio. Los datos se analizaron mediante estadística descriptiva, lo que permitió identificar tendencias generales.

En la fase cualitativa, se realizaron entrevistas a 4 expertos en ciberseguridad con experiencia directa en el análisis del ransomware Medusa. La muestra de expertos fue de tipo intencional, no probabilístico, con un enfoque cualitativo y un diseño fenomenológico. La información se analizó mediante categorización temática para interpretar las experiencias y los significados de los participantes.

5.1 Requerimientos o especificaciones

Para el desarrollo de este proyecto de investigación, se realiza una revisión de la literatura que permite conocer el estado del arte sobre el *ransomware* Medusa, sus vectores de ataque y las metodologías existentes para la gestión administrativa y de riesgos en ciberseguridad, utilizando marcos teóricos como NIST e ISO 27001.

Además, se realiza un análisis de casos reales de incidentes relacionados con Medusa, para identificar patrones y lecciones aprendidas, lo cual sirve como base para la propuesta de un modelo administrativo que integre las mejores prácticas en la prevención, respuesta y recuperación ante el *ransomware.*

La recolección de datos se realiza mediante encuestas y entrevistas con usuarios y expertos en ciberseguridad, lo que permite evaluar el nivel de conocimiento y las estrategias actuales de las organizaciones frente a estos ataques.

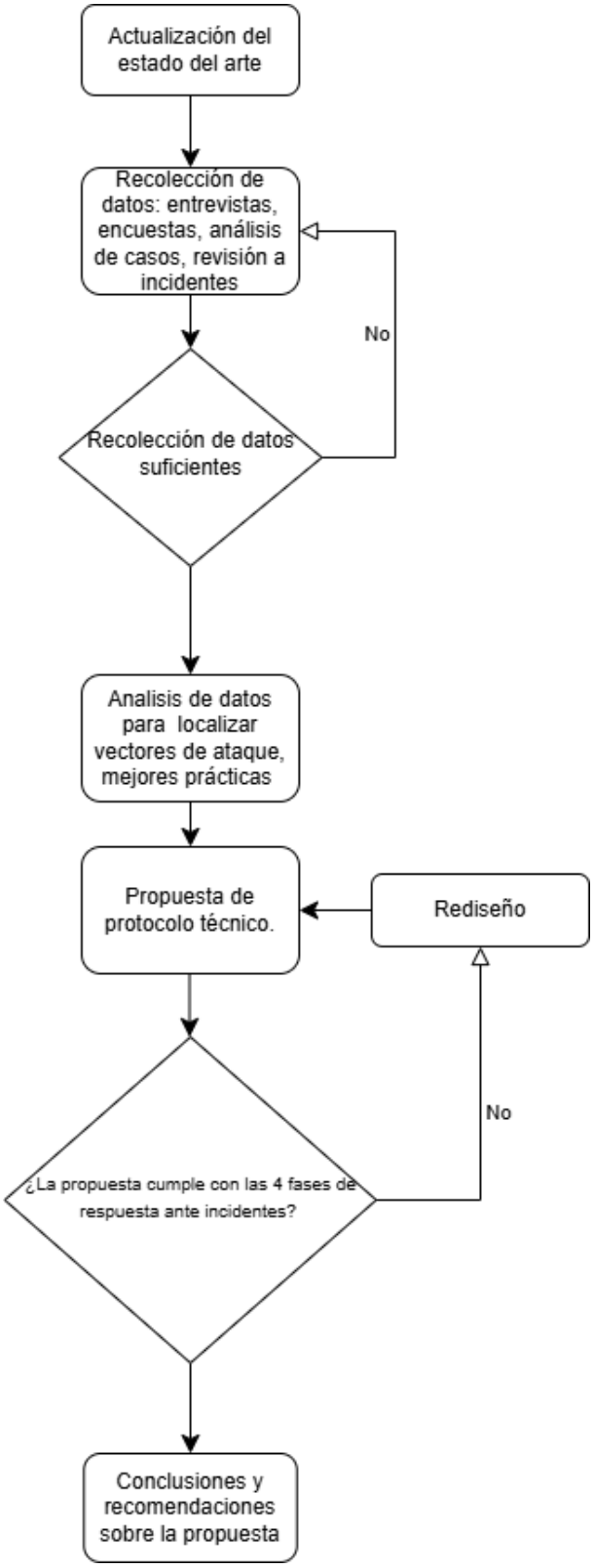

Figura 5.1 Diagrama de flujo para el desarrollo del método (creación propia).

5.2 Diseño e implementación

Para la recolección de datos, se utilizan dos tipos de métodos, por un lado,100 encuestas dirigidas a público de diferentes edades, que laboran en áreas de tecnología, ubicados en Centroamérica y un pequeño porcentaje de Sudamérica, con el objetivo de obtener perspectiva sobre el conocimiento y aplicación real, sobre las fases de la postura de ciberseguridad ante un ataque del *ransomware* Medusa; y por otro lado, también se presentan 4 entrevistas a expertos en el área, con el fin de identificar la postura de un experto de lado de la empresa, ante los ataques del *ransomware* Medusa.

Estas técnicas de recolección de datos están seleccionadas porque pueden ofrecer visibilidad de ambos lados ante un ataque de *ransomware.* Es decir, no sólo tener la perspectiva del personal experto en ciberseguridad sobre cómo actúa ante un ataque, sino también mantener el enfoque en el personal experto en ciberseguridad de las empresas, ya que la mayor parte de las vulnerabilidades se pueden presentar por una mala gestión administrativa y tecnológica por parte de los usuarios directos de las herramientas de la empresa.

5.2.1 Encuestas

La muestra estuvo conformada por 100 profesionales del sector de Tecnologías de la Información (TI), seleccionados mediante un muestreo no probabilístico por conveniencia. El diseño de las encuestas se encuentra de tal forma que lleve una secuencia con información demográfica, cultura de ciberseguridad y, posteriormente, las cuatro fases de ciberseguridad ante un ataque; es decir, políticas y prevención, respuesta y gestión de incidentes, continuidad del negocio y recuperación, auditoría y mejora continua.

Diseño de la encuesta

Con base en la literatura presentada en el marco teórico y en el estado del arte, a continuación, se presentan las secciones y preguntas elaboradas, el objetivo del instrumento y la justificación del planteamiento.

Datos generales:

El objetivo de esta sección es identificar las brechas de género y edad en el área de TI, abordando el área, el tiempo y el tamaño de la empresa donde se labora; esto para evaluar las estadísticas de posicionamiento del área, ya que es un entorno laboral que ha crecido de manera muy rápida en los últimos años, y al tener este panorama, se identifica el estatus actual del área en este entorno. Entre los datos recopilados se encuentran: edad, género, ubicación geográfica, preparación académica, puesto o área de trabajo en TI, antigüedad en la empresa y tamaño de la empresa.

Cultura de ciberseguridad:

Las preguntas de esta sección tienen como objetivo abordar contexto de conocimiento cultural en ciberseguridad, si los encuestados están familiarizados con la seguridad tecnológica, ante un *ransomware* como Medusa, esto para evaluar el grado de conocimiento en ciberseguridad para identificar los sesgos culturales dentro de una organización, ya que la mayoría de los riesgos están identificados en el personal de las empresas.

- ¿Conoces qué es un ataque de *ransomware?*
    - Si/he Escuchado sobre ello, pero no conozco los detalles/No
- Selecciona las opciones que consideres describen cómo este tipo de ataque podría impactar a la empresa
    - Pérdida de información importante o confidencial / Interrupción de operaciones o servicios / Daños a la reputación de la empresa / Pérdidas económicas o multas legales / Robo de datos personales de empleados o clientes / Exigencia de pago para recuperar el acceso/ Despido o sanciones para empleados responsables.
- ¿Has recibido capacitación en ciberseguridad durante el último año?
    - Si/No

Políticas y prevención:

Los cuestionamientos de esta sección tienen como propósito evaluar el grado de conocimiento y aplicación de las políticas internas relacionadas con el uso correcto y

seguro de las herramientas tecnológicas, contraseñas, correos, etc., para identificar el nivel de madurez preventiva ante incidentes de seguridad a fin de tener el cumplimiento de políticas claras de uso tecnológico, siendo esencial en la gestión de ciberseguridad organizacional, con estas respuestas, permite determinar si el personal conoce y aplica las normas básicas de prevención ante un ataque de *ransomware* Medusa.

- ¿La empresa cuenta con políticas claras sobre uso correcto de correo electrónico?
    - Si/ Existen, pero no están bien difundidas/ No lo sé, no existen
- ¿La empresa cuenta con políticas claras sobre la configuración y uso de contraseñas?
    - Si/ existen, pero no están bien definidas / No lo sé, no existen
- ¿La empresa cuenta con políticas claras sobre el uso de dispositivos tecnológicos?
    - Si/ existen, pero no están bien definidas / No lo sé, no existen
- ¿Con qué frecuencia debes cambiar tus contraseñas laborales?
    - Cada mes/ cada 3 meses/ Nunca me lo han solicitado / No lo sé
- ¿Tienes acceso a sistemas críticos según tu rol o cargo?
    - Sí, solo tengo acceso a los sistemas necesarios para mi función / No, tengo acceso a sistemas que no corresponden directamente a mi función/ No sé / No estoy segura(o) de a qué sistemas tengo acceso/ No tengo acceso a sistemas críticos
- ¿Tienes acceso a sistemas generales o de uso común según tu rol?
    - Sí, solo tengo acceso a los sistemas necesarios para mi función / No, tengo acceso a sistemas que no corresponden directamente a mi función/ No sé / No estoy segura(o) de a qué sistemas tengo acceso/ No tengo acceso a sistemas generales
- ¿La empresa realiza campañas específicas para prevenir ataques por phishing, principal medio de entrada del *ransomware* como Medusa?
    - Si constantemente / Ocasionalmente /No se han realizado
- ¿Alguna política o norma de seguridad de TI de la empresa no es muy clara o te causa confusión?
    - Si, hay alguna (s) / No, todo ha sido claro

- ¿Conoces y utilizas un protocolo interno para prevenir *ransomware?*
    - Si, lo conozco y lo aplico / He oído hablar, pero no lo utilizo / No lo conozco, no existe

Respuesta y Gestión de incidentes:

Las preguntas de esta sección tienen la finalidad de analizar el nivel de conocimiento ante la preparación y manejo de incidentes de seguridad informática, para valorar la capacidad de respuesta frente amenazas como *ransomware* Medusa, en beneficio de conocer si los empleados pueden reconocer un incidente y actuar de acuerdo con los protocolos establecidos, identificando el grado de efectividad del plan de respuesta ante incidentes.

- ¿Reconoces alguno de los siguientes tipos de incidentes de seguridad informática?
    - *Phishing* (correo o mensajes engañosos para robar información). / *Ransomware* (secuestro de datos mediante cifrado y demanda de rescate). / Hackeo o acceso no autorizado a sistemas. / *Malware* (programas maliciosos que dañan o roban información). / Ataques de denegación de servicio (DoS/DDoS). / Ingeniería social (manipulación para obtener información confidencial). / Todas las anteriores. / No conozco ninguno de estos.
- ¿Conoces el protocolo que debes seguir y qué acciones tomar ante un incidente de seguridad informática como *phishing*, *ransomware* o hackeo?
    - Si / No
- ¿Sabes a quién reportar un incidente de seguridad informática?
    - Si / No / No estoy seguro
- ¿Sabes cómo y por qué medio debes reportar un incidente de seguridad informática?
    - Sí, sé exactamente cómo y a través de qué canal (correo, sistema de tickets, etc.). / Sé a quién reportarlo, pero no el canal. / No sé cómo se reporta. / No sabía que debía reportarse.

Continuidad del Negocio y Recuperación

Las interrogantes de esta sección tienen como fin evaluar las prácticas implementadas por la organización para la protección y recuperación de la información ante ataques de ransomware, por posibles pérdidas o cifrados de datos, para identificar si las empresas cuentan con políticas efectivas de respaldo, pruebas de restauración y disponibilidad, así como la frecuencia de protección con los mecanismos de recuperación ante el ataque de *ransomware* Medusa.

- ¿La empresa realiza respaldos de información regularmente?
    - Si / No / No estoy seguro
- ¿Los respaldos están protegidos contra cifrado o eliminación por parte de un *ransomware* como Medusa?
    - Si / No / Parcialmente
- ¿Has participado en simulacros o pruebas de restauración?
    - Si / No

Auditoría y Mejora Continua

Las cuestiones de este apartado son con la meta de determinar la existencia de auditorías o revisiones de seguridad, incluyendo el nivel de conocimiento del personal sobre amenazas específicas como el *ransomware* Medusa con la intención de determinar si las organizaciones realizan evaluaciones periódicas para fortalecer las prácticas de protección, obteniendo una visión más clara sobre la capacidad para aprender y mejorar en el panorama de la ciberseguridad.

- ¿La empresa realiza auditorías o revisiones periódicas de seguridad digital?
    - Si / No / No estoy seguro
- ¿Estás familiarizado(a) con el *ransomware* Medusa y su modo de operar?
    - Si, conozco sus métodos / Lo he escuchado, pero no conozco a fondo / No, nunca había oído hablar.

5.2.2 Entrevistas

Se realizaron entrevistas semiestructuradas a cuatro expertos en ciberseguridad, con experiencia en gestión de incidentes y análisis de ransomware, que han tenido contacto directo con Medusa. En esta sección se identifican las preguntas planteadas en las entrevistas a expertos en ciberseguridad. En la primera parte se recopilan datos sobre el entrevistado, como el nombre, cargo, años de experiencia en el sector, nivel organizacional, etc., con el fin de tener presente que las entrevistas fueron realizadas con personal preparado y con experiencia en el tema. El diseño de la entrevista se presenta a continuación.

Entrevista a experto en ciberseguridad: Protocolo ante *ransomware* Medusa

Fecha y hora de entrevista: Medio: Virtual

Nombre:

Cargo o puesto actual:

Empresa:

Años de experiencia en TI / Ciberseguridad:

Área de especialización:

Certificaciones:

Ubicación: Estado/país

Nivel organizacional de participación en decisiones de seguridad

() Alta dirección

() Gestión media

() Técnico operativo

Autorización para uso académico: Si (x) No ()

Objetivo de la entrevista: obtener una perspectiva experta sobre estrategias de gestión y respuesta ante ataques de *ransomware* tipo Medusa, basadas en cuatro fases clave: prevención, detección, respuesta y recuperación.

Sección Estrategia y Políticas de Seguridad

Esta sección tiene la finalidad de identificar las estrategias, metodologías y políticas de seguridad aplicadas por los expertos en TI, ciberseguridad, para la prevención y mitigación de ataques de *ransomware* como Medusa, esto para comprender las políticas y prácticas de seguridad para conocer cómo as organizaciones estructuran sus defensas ante un ataque de *ransomware* como Medusa, indispensable para tener una base sólida en el protocolo propuesto alineándose a las normas internacionales de seguridad de la información.

1. Desde su experiencia, ¿qué tan frecuente considera que son los ataques de *ransomware* actualmente en el entorno empresarial o en las pymes?
2. ¿Conoce o ha tenido contacto con algún caso de *ransomware* específico, como Medusa, LockBit, Conti u otros?
3. ¿Qué metodologías utiliza para gestionar el control de accesos y la administración de privilegios con seguridad en la organización?
4. ¿Cuáles considera que son las principales políticas de seguridad de la información que considera esenciales para la prevención de ataques de *ransomware* Medusa?
5. ¿Podría explicar cómo se estructura el plan de continuidad del negocio frente a un posible ataque de *ransomware* Medusa?

Sección Detección y Monitoreo de Amenazas

Las preguntas aquí planteadas buscan analizar las herramientas y tecnologías de monitoreo utilizadas por las organizaciones para la detección y respuesta ante posibles ataques del *ransomware* Medusa, con el fin de monitorear e identificar como se integran soluciones como SIEM, XDRM o EDR, para reducir tiempos ante incidentes de ataques de *ransomware* Medusa, permitiendo establecer buenas prácticas para fortalecer la resiliencia de las pymes ante estos ataques.

1. ¿Qué herramientas o tecnologías clave usa para detección temprana de *ransomware?*
2. ¿De qué manera se integran soluciones como SIEM (Security Information and Event Management / Gestión de Eventos e Información de Seguridad), XDR (Extended Detection and Response / Detección y Respuesta Extendidas) y EDR (Endpoint Detection and Response / Detección y Respuesta de Puntos Finales) en la estrategia de ciberseguridad para prevenir ataques de *ransomware* Medusa?
3. Desde su perspectiva, ¿cómo definiría la inteligencia de amenazas en ciberseguridad (una herramienta técnica, una estrategia organizacional o una combinación de ambas)?
4. ¿Qué rol cumple la inteligencia de amenazas en la identificación y mitigación de ataques de *ransomware* Medusa?
5. ¿Cuáles son los indicadores clave que permiten detectar la presencia de *ransomware* en la infraestructura de TI?
6. ¿Cuál es la primera acción recomendada en respuesta a estos eventos?

Sección Respuesta y Recuperación ante un Ataque

El propósito de esta sección es examinar y evaluar los protocolos, acciones y estrategias que siguen las organizaciones para responder a y recuperarse de un ataque de *ransomware* Medusa. Y así conocer los mecanismos de defensa y respuesta en una organización frente a incidentes críticos, como un ataque de *ransomware* Medusa, esta información es esencial para diseñar un plan de continuidad y recuperación que minimice el impacto en las pymes.

1. ¿Puede describir el protocolo de respuesta a incidentes que se implementa cuando se detecta un ataque de *ransomware* Medusa en la organización?
2. ¿Cómo gestionan la comunicación interna y externa durante y después de un ataque de *ransomware* para mitigar el impacto reputacional y operativo?
3. ¿Qué medidas se han implementado para garantizar que los respaldos de datos sean seguros y no puedan ser comprometidos por un atacante?
4. ¿Qué acciones se aplican si hay exfiltración y extorsión por parte del atacante para minimizar daños?

Sección Cumplimiento, Normativas y Capacitación

Esta parte del instrumento está diseñada para evaluar el nivel de cumplimiento normativo, la aplicación de estándares de seguridad y la efectividad de los programas de capacitación en las organizaciones frente al riesgo de *ransomware* Medusa y determinar la formación continua y el cumplimiento de normas y estándares internacionales que, son pilares en la ciberseguridad, al analizar estos puntos, lo que permite proponer mejoras en la gestión administrativa que integren el cumplimiento y la concientización en el factor humano, en el marco de la seguridad de la información

1. ¿Qué normativas y estándares de seguridad sigue su organización para asegurar el cumplimiento en la gestión del riesgo de Medusa?
2. ¿Cómo se capacita al personal general de la empresa para evitar que sean víctimas de ataques de *phishing*, ingeniería social o tácticas utilizadas por grupos de *ransomware?*
3. ¿Cómo se capacita al personal de áreas de TI de la empresa para evitar que sean víctimas de ataques de *phishing*, ingeniería social o tácticas utilizadas por grupos de *ransomware?*
4. ¿Qué métricas o indicadores emplean para evaluar la efectividad de las estrategias de gestión administrativa frente a ataques de *ransomware?*
5. Con base en su experiencia, ¿qué consejo daría a las pymes mexicanas para protegerse de Medusa u otros *ransomware* similares?

Sección final: se añade una sección para que el entrevistado pueda agregar algún comentario final que pueda aportar algún elemento extra no mencionado antes, o puntos de mejora para esta entrevista/trabajo. Asimismo, se anexa una nota en la que el entrevistado declara que autoriza el uso de la información para fines académicos.

Observaciones finales:

Nota: Declaro que la información compartida es para fines académicos y autorizo su uso en la tesina de la estudiante **Andrea Piña Contreras.**

5.3 Criterios del desarrollo del protocolo

Con base en la información obtenida mediante entrevistas con expertos y encuestas aplicadas al personal del sector tecnológico, se establecen los criterios fundamentales para el desarrollo del protocolo. Estos criterios están divididos en las 4 secciones, identificadas al inicio del proyecto, y un anexo de mejora continua, cada una con un listado que representa los elementos mínimos indispensables que guiaron su diseño y estructuración, y se describen a continuación:

1. **Prevención**

    a. Políticas de seguridad de la información: Incluir las políticas más sobresalientes sobre prevención.

    b. Gestión de activos críticos, anexando un inventario con la clasificación de criticidad y sensibilidad.

    c. Concientización y capacitación de personal

    d. Gestión de parches, copias de seguridad y actualizaciones.

    e. Controles de accesos, contraseñas y gestión de identidades.

    f. Arquitectura Zero Trust Security

    g. Simulacros y pruebas de seguridad

    h. Segmentación de red (DMZ) y arquitectura segura.

    i. Monitoreo continuo y correlación de eventos.

2. **Detección**

    a) Plan de respuesta a incidentes (roles y responsabilidades).

    b) Monitoreo continuo

    c) Definir umbrales y criterios de alerta

d) Alertas y herramientas de detección-EDR/XDR

e) Detección basada en comportamiento

f) Pruebas y validaciones periódicas

g) Notificaciones internas

h) Incidentes y respuestas

3. Respuesta

a) Procedimientos de aislamiento inmediato (plan de respuesta a incidentes)

b) Roles y responsabilidades del equipo de respuesta

c) Comunicación interna y externa.

d) Coordinación con autoridades y proveedores

e) Preservación de evidencias forenses

f) Procedimientos legales y regulatorios

g) Evaluación del alcance del impacto

4. Recuperación

a) Restablecimiento seguro de operaciones (sistemas y datos)

b) Retorno a operaciones normales

c) Informe de lecciones aprendidas.

d) Actualización del marco para futuros incidentes.

e) Seguimiento y monitoreo post recuperación

5. Plan de mejora continua

a) Actualización de políticas y procedimientos según nuevas amenazas y versiones de estándares.

b) Auditorias periódicas

c) Integración de nuevos controles y tecnologías

d) Entrenamiento y concientización de colaboradores

e) Auditoria de ciber postura de terceras partes

6 RESULTADOS Y DISCUSIÓN

En este apartado se presentan y analizan los resultados obtenidos mediante la aplicación de encuestas a personas del sector de TI y la realización de entrevistas a expertos en ciberseguridad. El objetivo es identificar percepciones, prácticas y niveles de madurez en la gestión de la seguridad de la información en las organizaciones.

Los resultados de las encuestas se estructuran en seis secciones: datos generales de los encuestados; cultura de ciberseguridad; políticas y prevención; respuesta y gestión de incidentes; continuidad de negocio y recuperación; y auditoría y mejora continua.

Por su parte, las entrevistas se organizan en cuatro apartados que permiten profundizar en la perspectiva de los especialistas: estrategia y políticas de seguridad, detección y monitoreo de amenazas, respuesta y recuperación ante un ataque, y cumplimiento normativo y capacitación.

Este análisis ofrece una visión integral de las prácticas actuales, los desafíos identificados y las oportunidades de mejora en el ámbito de la ciberseguridad organizacional.

6.1 Resultados de la aplicación de encuestas

Se presenta la interpretación de los resultados de las 100 encuestas aplicadas a personas que laboran en el sector TI, con base en Centroamérica y en algunos países de Sudamérica.

Los resultados se centran en identificar patrones culturales de ciberseguridad, abarcando las cuatro fases de ciberseguridad, detectando la fase clave a reforzar en el área empresarial y aplicando posteriormente el protocolo de acciones para abordar un ataque de *ransomware* Medusa.

Datos generales:

1.-Edad. En la Figura 6.1. se presenta la distribución etaria de la población, en la cual el grupo de 20 a 29 años concentra la mayor frecuencia (67), seguido por el de 30 a 39 años (15).

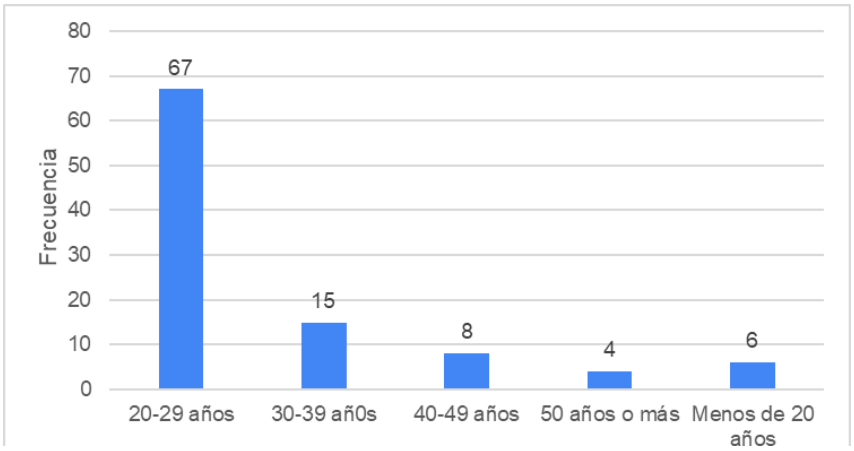

Figura 6.1. Estadística de la pregunta sobre edad, aplicación propia en población de Centroamérica y de algunos países de Sudamérica.

2.- Género

En la Figura 6.2 se observa un gráfico circular que muestra, con base en el sector mayoritario que respondió las encuestas, una participación de 49% de mujeres y 51% de hombres, lo que concluye que el sesgo de género tecnológico se visualiza balanceado; es decir, la introducción de la mujer en este sector ha ido mejorando.

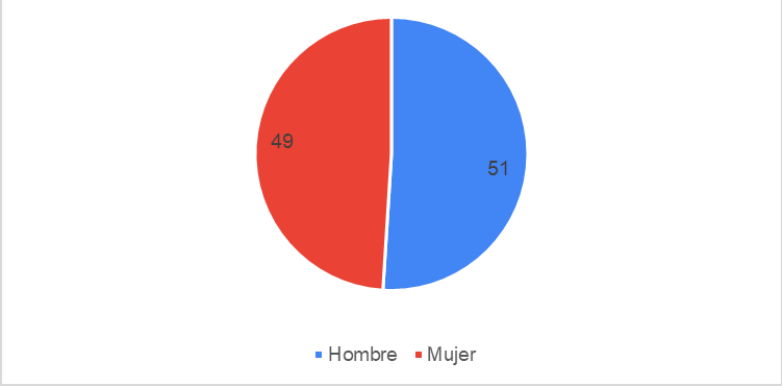

Figura 6.2. Estadística de la pregunta sobre género en una aplicación propia en población de Centroamérica y de algunos países de Sudamérica.

3.- Ubicación geográfica

En la Figura 6.3 se interpreta que el 76% del personal encuestado reside en México, 20% en Sudamérica (Argentina, Ecuador, Colombia, Chile, Guatemala, Paraguay, Brasil,

Nicaragua, Costa Rica, Perú, República Dominicana), un pequeño porcentaje del 3% de Norteamérica en Canadá y Estados Unidos, y una minoría de Europa, con 1% de España.

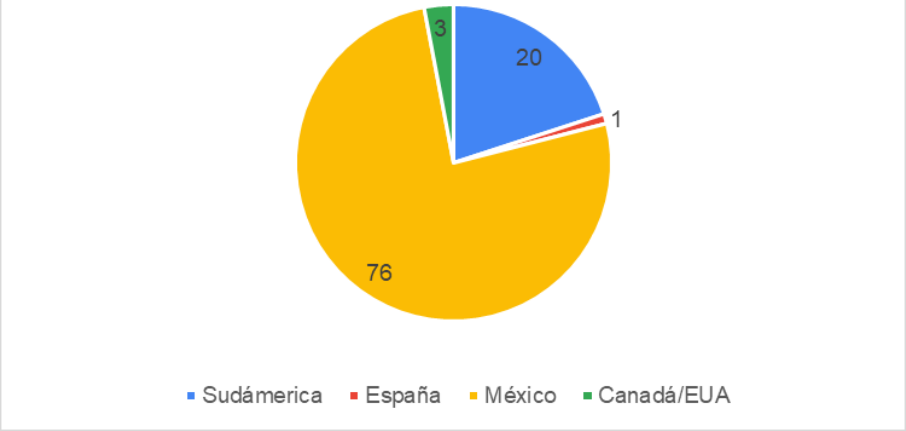

Figura 6.3. Estadística de la pregunta sobre ubicación geográfica, aplicada a población de Centroamérica y de algunos países de Sudamérica.

4.- Preparación académica

En el gráfico de barras de la Figura 6.4 se observa que el nivel académico más frecuente es la licenciatura terminada, con un 58%, continuando la licenciatura trunca o en curso, con un 22%; carrera técnica y posgrado, ambos con un 7%; y, en menor proporción, preparatoria con un 5% y secundaria con un 1%.

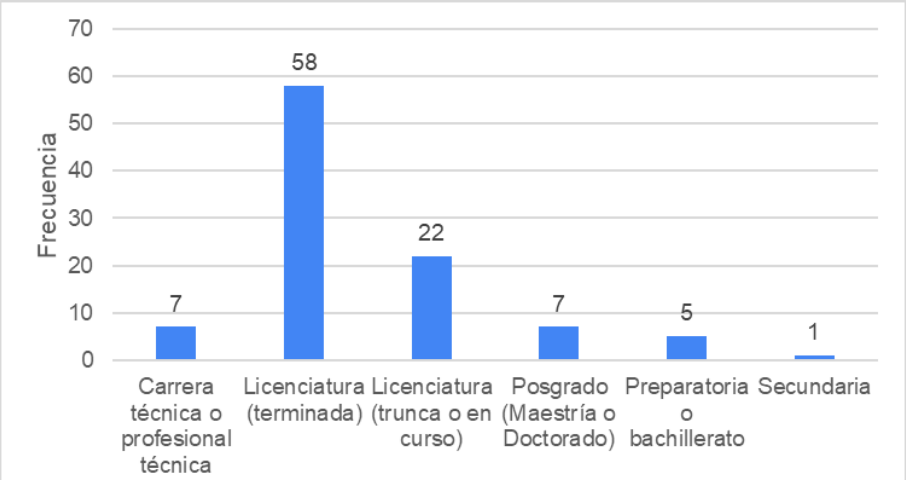

Figura 6.4 Estadística de la pregunta sobre preparación académica, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

5.- Puesto o área de trabajo de TI

Se observa el gráfico de la Figura 6.5 en un 24% de desarrollo de software y aplicaciones, seguida del 12% y 11% en Soporte técnico y seguridad informática respectivamente, en la minoría quedando 9 y 7% con Administración de sistemas, de redes y gestión de TI, teniendo el mayor porcentaje del 31% en áreas diversas, no especificadas dentro de las opciones planteadas.

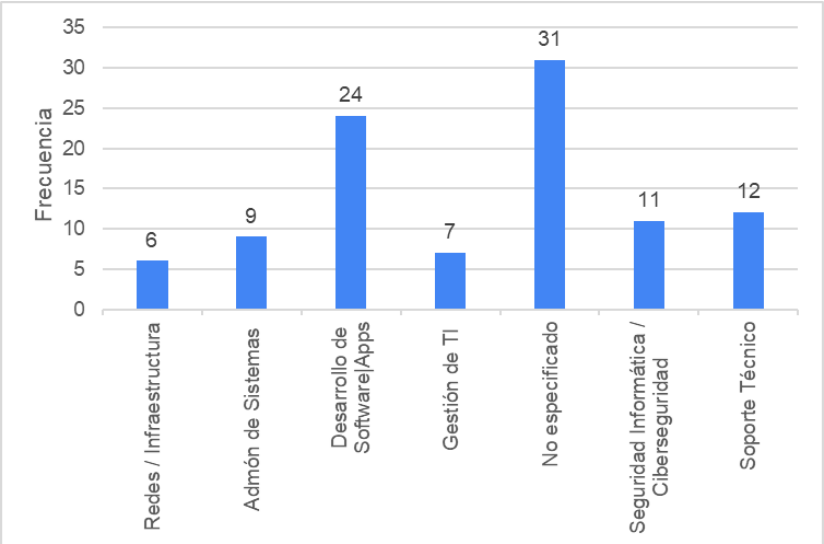

Figura 6.5 Estadística de la pregunta sobre el área de trabajo de TI, aplicación propia en población de Centroamérica y algunos países de Sudamérica

6.- Tiempo laborando en la empresa.

Dando como respuestas en la Figura 6.6 el 35% tienen menos de 6 meses en la empresa, 25% de 6 meses a 1 año, 22% de 1 a 3 años, y teniendo el mayor tiempo, pero minoría de porcentaje con 18% más de 3 años laborando en la empresa actual.

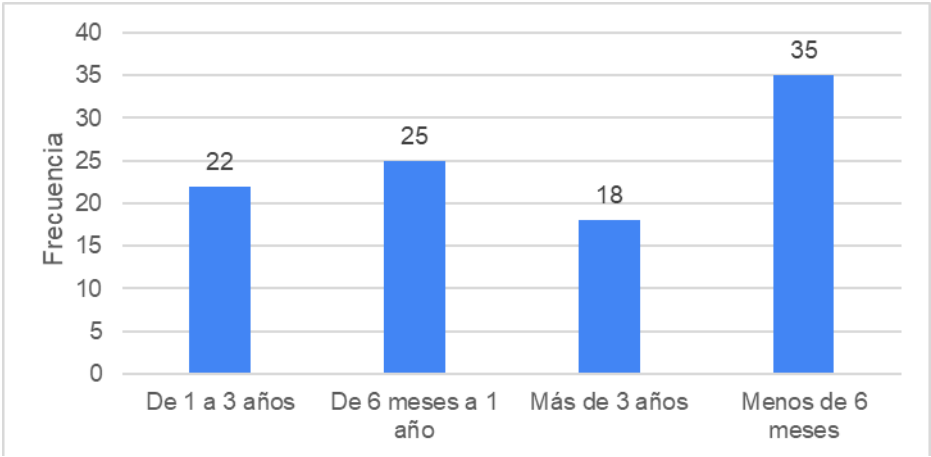

Figura 6.6 Estadística de la pregunta sobre tiempo que llevan laborando en la empresa actual, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

7.- Tamaño de la empresa donde laboras

En la Figura 6.7 e muestra la distribución de los tamaños de empresa: un 31% son grandes empresas, un 28% medianas, un 16% pequeñas y un 16% microempresas.

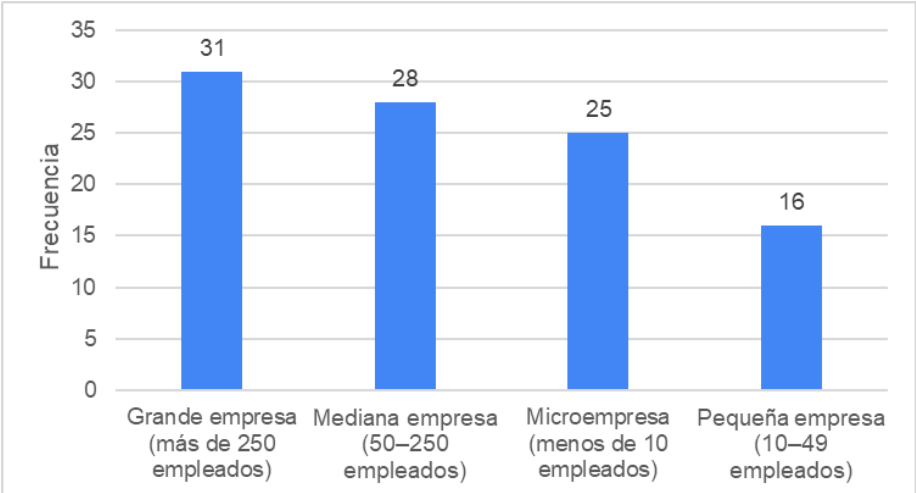

Figura 6.7 Estadística de la pregunta sobre el tamaño de la empresa donde laboran los encuestados, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

Como conclusión general de esta primera sección, se determinó que el sector mayoritario se encuentra con personas de la edad entre 20 y 29 años, en casi iguales proporciones de

géneros entre hombre y mujer, con licenciatura terminada o en curso, y en varias áreas de TI, con 6 meses de antigüedad laboral en la empresa actual.

Sección cultura de ciberseguridad

1. - ¿Conoces qué es un ataque de *ransomware?*

En la Figura 6.8 se observa que el 53% de la población encuestada respondió asertivamente que si conocen qué es un *ransomware,* en minoría un 37% que ha escuchado sobre ello, pero no conoce detalles y 10% que no están familiarizados.

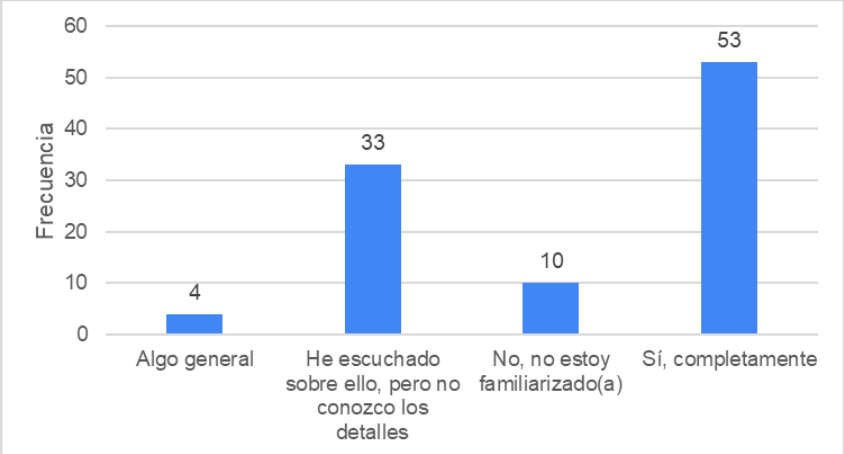

Figura 6.8. Estadística de la pregunta de conocimiento sobre ransomware, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

2.- Selecciona las opciones que consideres describen cómo este tipo de ataque podría impactar a la empresa

Se desglosa en la Figura 6.9 muestra el desglose porcentual de los impactos percibidos del *ransomware,* cabe destacar que los encuestados podían seleccionar más de una opción. El 57% de los encuestados indicó que afecta la pérdida de información crítica, el 53% señaló el robo de datos personales y el 41% reportó la interrupción de las operaciones. Los impactos menos mencionados fueron la exigencia de pago para recuperar los datos, las pérdidas económicas y los daños a la reputación. Un 2% de los participantes manifestó desconocer el impacto del *ransomware.*

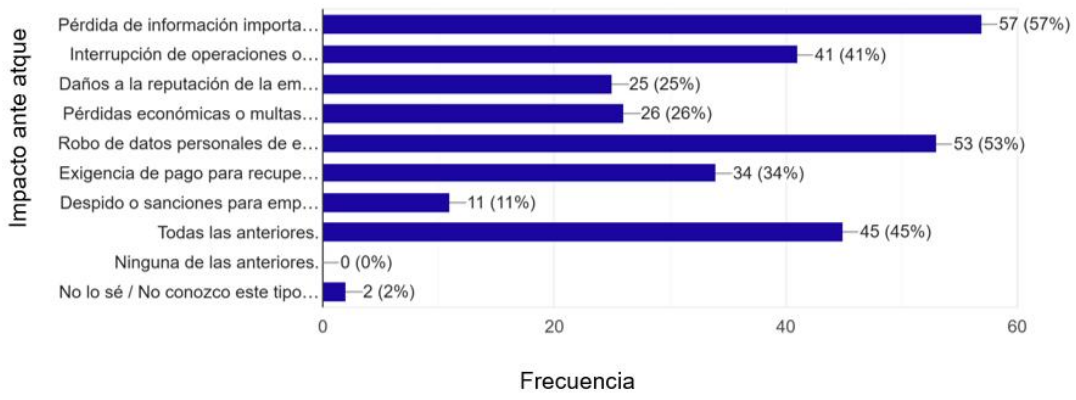

Figura 6.9 Estadística de la pregunta sobre el conocimiento de acciones que describen el impacto de la empresa ante un ataque de ransomware, aplicación propia en población de Centroamérica y de algunos países de Sudamérica.

3.- ¿Has recibido capacitación en ciberseguridad durante el último año?

Se plantea un gráfico circular en la Figura 6.10 donde el 51% de los encuestados indicó que sí han recibido capacitación, mientras que el 49% señaló que no. Esto evidencia que, aunque aproximadamente la mitad de la población ha recibido formación, aún existe un porcentaje significativo que no la ha recibido.

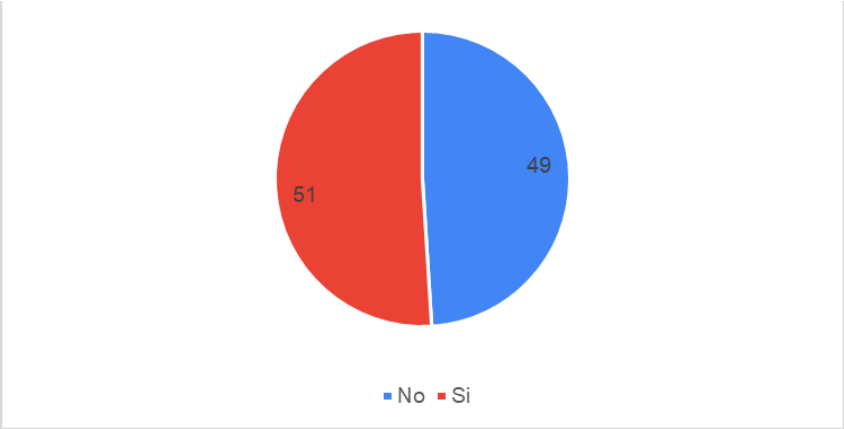

Figura 6.10 Estadística de la pregunta sobre capacitación de ciberseguridad durante el último año, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

Concluyendo esta sección, es importante tener en cuenta que el 47% de los encuestados no conoce sobre el *ransomware,* o solo ha escuchado, pero no sabe los detalles, las acciones de impacto sobre la empresa y que en el último año no ha recibido capacitaciones de ciberseguridad, para identificar las acciones ante un incidente de esta magnitud, como lo es el *ransomware* Medusa.

Sección Políticas y prevención

4.- ¿La empresa cuenta con políticas claras sobre el uso correcto de correo electrónico?

La Figura 6.11 demuestra que el 63% menciona que, si están bien definidas y comunicadas, sin embargo, existe un 28% que, existen, pero no están bien difundidas; y un porcentaje de 9% donde desconocen o no existen en la empresa.

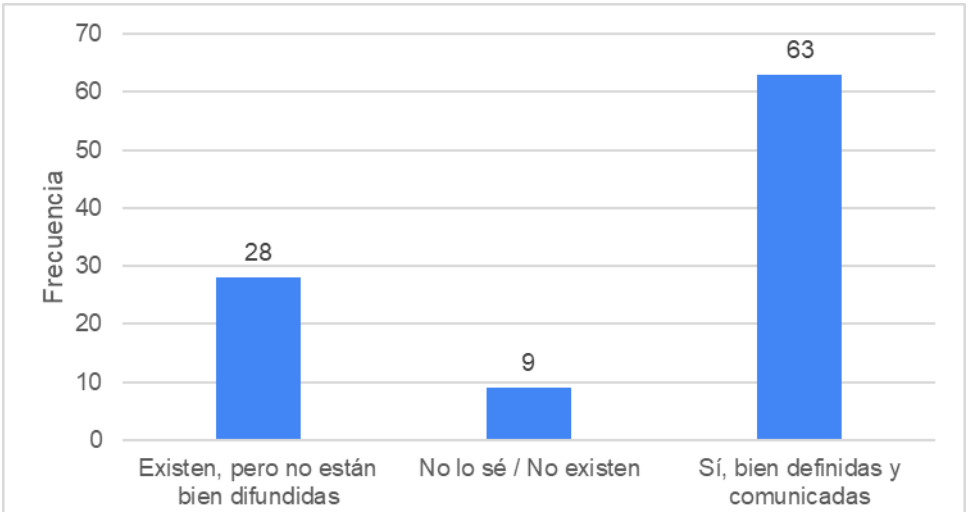

Figura 6.11 Estadística de la pregunta sobre uso correcto de correo electrónico, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

5.- ¿La empresa cuenta con políticas claras sobre la configuración y uso de contraseñas?

El gráfico de la Figura 6.12 demuestra que una proporción importante de encuestados (64%) considera que las políticas están bien definidas y comunicadas; sin embargo, aún hay un grupo que percibe que no se difunden adecuadamente o desconoce su existencia. Esto evidencia la necesidad de fortalecer la comunicación y la concientización sobre las políticas de ciberseguridad en la organización.

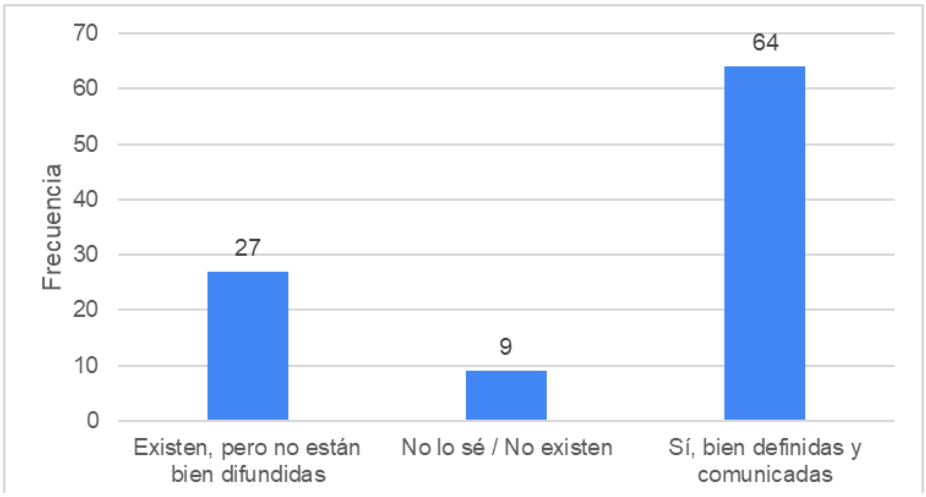

Figura 6.12 Estadística de la pregunta sobre configuración de contraseñas seguras, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

6.- ¿La empresa cuenta con políticas claras sobre el uso de dispositivos tecnológicos?

La Figura 6.13 demuestra que el 64% menciona que, si están bien definidas y comunicadas, sin embargo, existe un 27% que, existen, pero no están bien difundidas; y un porcentaje de 9% donde desconocen o no existen en la empresa.

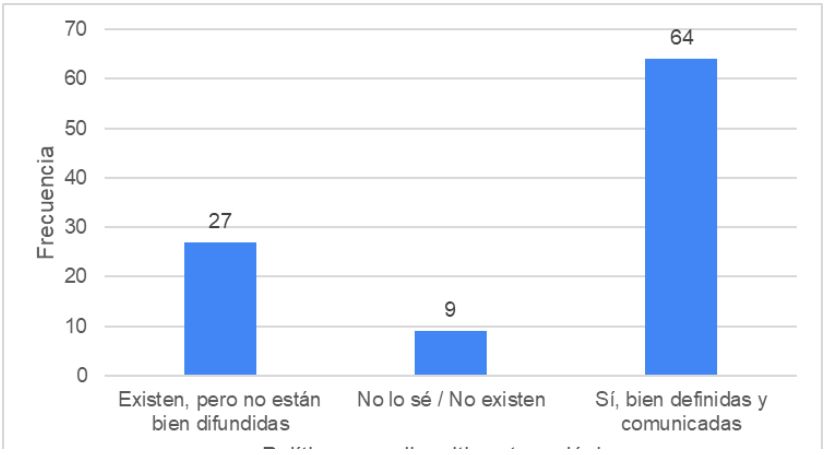

Figura 6.13 Estadística de la pregunta sobre uso correcto de dispositivos tecnológicos, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

7.- ¿Con qué frecuencia debes cambiar tus contraseñas laborales?

En esta pregunta se puede destacar un gráfico de barras, en la Figura 6.14 muestra que el 44% de los encuestados identifica que el cambio de contraseña se realiza cada tres meses, mientras que el 35% indica que no se les ha solicitado. Esto genera una situación negativa en la seguridad de contraseñas.

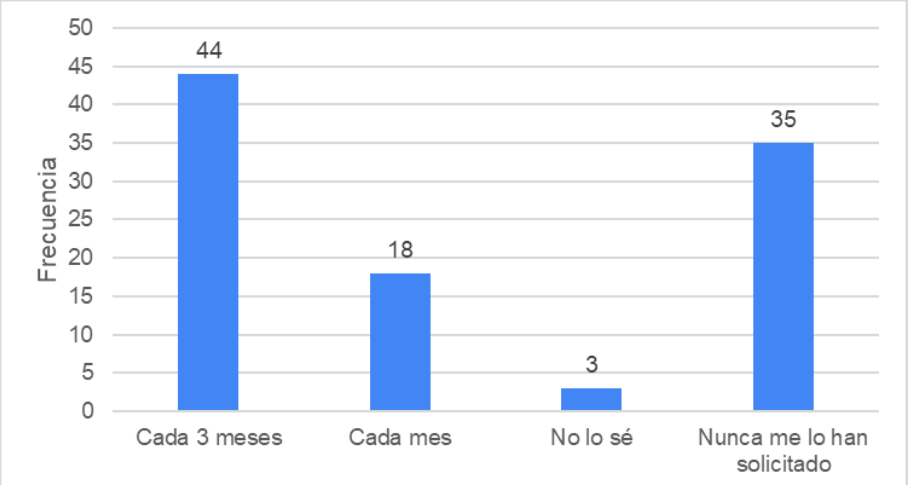

Figura 6.14 Estadística de la pregunta sobre contraseñas seguras, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

8.- ¿Tienes acceso a sistemas críticos según tu rol o cargo?

La estadística de la Figura 6.15 que muestra que el 64% del personal encuestado sí tiene acceso solo a los sistemas necesarios de acuerdo con su función, el 19% que tiene acceso a sistemas que no corresponden directamente a su función, y el 17% que no tiene acceso, quedando sólo con 1% que está seguro de que sí tiene acceso a sistemas críticos.

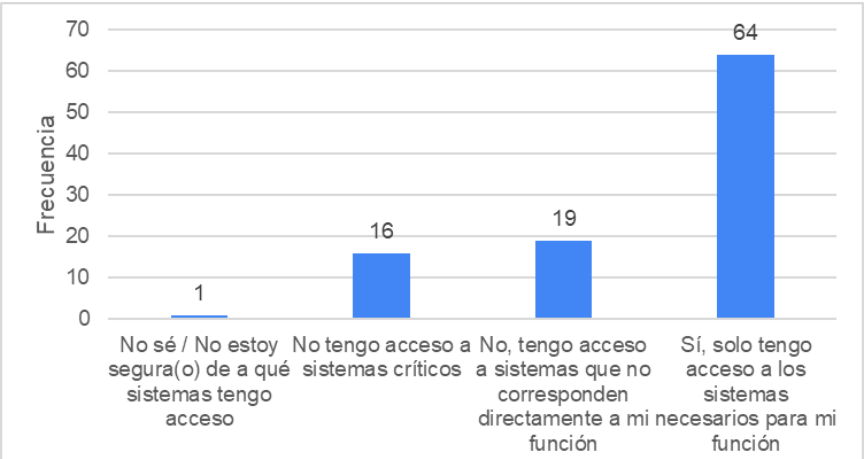

Figura 6.15Estadística de la pregunta sobre accesos a sistemas críticos, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

9.- ¿Tienes acceso a sistemas generales según tu rol o cargo?

Estadística de la Figura 6.16 que muestra que el 79% del personal encuestado sí tiene acceso solo a los sistemas necesarios de acuerdo con su función, el 14% que tiene acceso a sistemas que no corresponden directamente a su función, y sólo el 7% que no está seguro de si tiene acceso a sistemas generales.

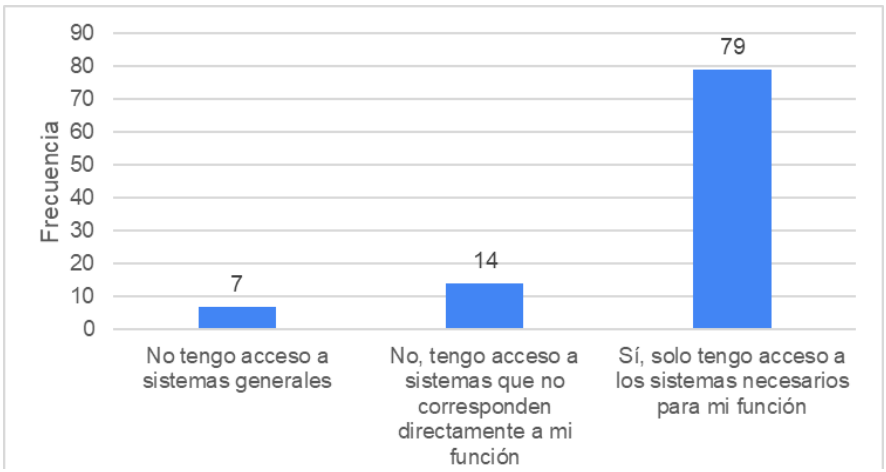

Figura 6.16. Estadística de la pregunta sobre accesos a sistemas generales, aplicación propia en población de Centroamérica y algunos países de Sudamérica

10.- ¿La empresa realiza campañas específicas para prevenir ataques por *phishing*, principal medio de entrada del *ransomware* como Medusa?

En esta pregunta se observa la Figura 6.17 que la mayor parte se reparte en que si se han realizado campañas constante u ocasionalmente, con un porcentaje de 46% y 25% respectivamente, lo que deja en minoría el que no se han realizado con un 29%, a pesar de estos porcentajes, se debe tomar en cuenta que es preocupante que no se hagan de manera constante y que aún exista gran porcentaje que no se han realizado.

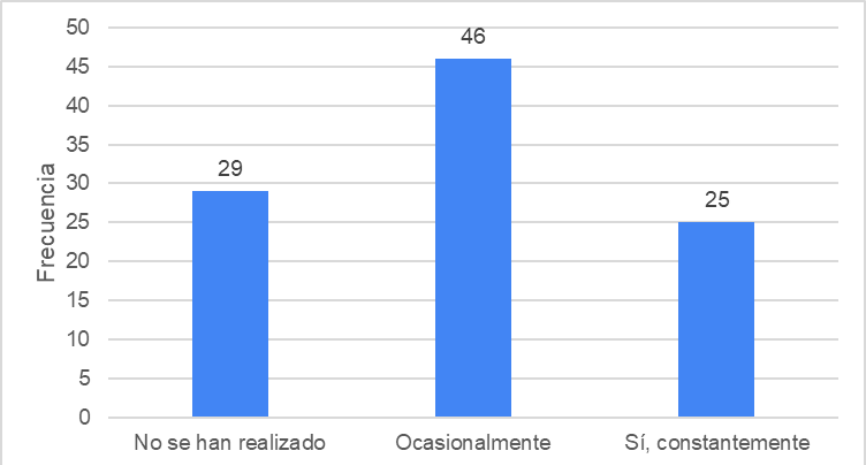

Figura 6.17 Estadística de la pregunta sobre campañas de concientización, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

11 y 12.- ¿Alguna política o norma de seguridad de TI de la empresa no es muy clara o te causa confusión? ¿Cuales?

Este gráfico circular, de la Figura 6.18, muestra que el 92% menciona que todo ha sido claro y el 8% restante menciona que no ha sido todo claro, enfocándose en la estabilidad y orden de datos digitales.

Figura 6.18 Estadística de la pregunta sobre claridad en las políticas de la empresa, aplicación propia en población de Centroamérica y algunos países de Sudamérica

13.- ¿Conoces y utilizas un protocolo interno para prevenir el *ransomware?*

La estadística de la Figura 6.19 sobre esta pregunta deja observar que el mayor peso ha caído sobre que han oído hablar del protocolo, pero no lo utilizan, con tan solo 45%, dejando con un 36% a los que si aplican y un 19% que no conocen o no existe, por lo que es una sugerencia para implementar evaluaciones sobre estas aplicaciones, no sólo que existan y se conozcan, sino que también se apliquen de manera correcta.

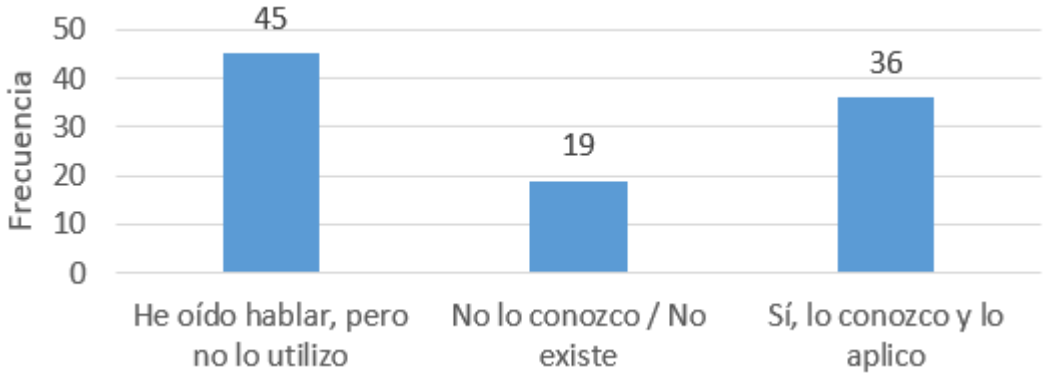

Figura 6.19 Estadística de la pregunta sobre el protocolo para prevenir ransomware, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

Los resultados de esta sección indican que las organizaciones cuentan con bases sólidas en materia de políticas de seguridad y control de accesos, reflejadas en la existencia de

lineamientos definidos, cambios periódicos de contraseñas y la aplicación del principio de mínimo privilegio.

Sin embargo, persisten áreas de mejora relacionadas con la concientización del personal y la preparación frente a amenazas específicas, particularmente ante ataques de *phishing* y *ransomware,* que son los principales vectores de ataque de Medusa, y aún se observa la ausencia de campañas especializadas y de protocolos internos de prevención.

Sección respuesta y gestión de incidentes

14.- ¿Reconoces alguno de los siguientes tipos de incidentes de seguridad informática?

Esta pregunta de la Figura 6.20 es clave para identificar el conocimiento sobre los tipos de incidentes que pueden identificarse, en consecuencia, de un ataque de *ransomware* Medusa, los porcentajes no son muy favorables, se acercan a la mitad de la población encuestada, dando como resultado una media de 46.3 % en conocimiento sobre todos los incidentes, dejando la lista de la siguiente manera:

1. *Phishing*
2. *Malware*
3. Hackeo
4. *Ransomware*
5. Ingeniería social
6. Ataque de denegación de servicio

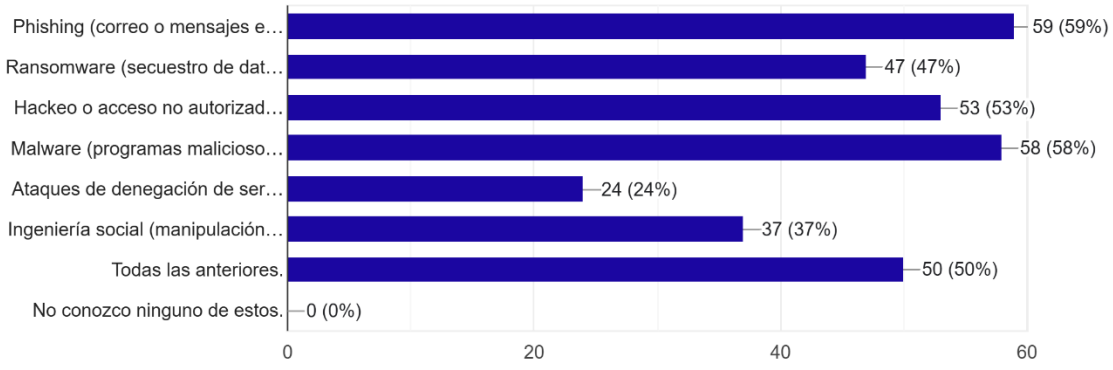

Figura 6.20 Estadística de la pregunta sobre conocimiento de los tipos de incidentes de seguridad informática, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

15.- ¿Conoces el protocolo que debes seguir y que acciones tomar ante un incidente de seguridad informática como *ransomware* o hackeo?

Esta pregunta genera un gráfico satisfactorio visualizado en la Figura 6.21 dado que más de la mitad de la población sabe qué protocolo seguir, sin embargo, aún existe un 34% que no lo sabe, motivo de preocupación y gran vulnerabilidad de seguridad, ya que a pesar de que se tenga en la empresa un protocolo, no lo conocen y podría afectar gravemente, de acuerdo con las acciones posteriores a un incidente.

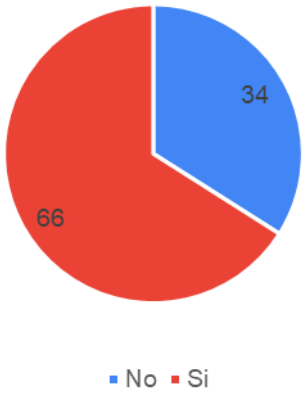

Figura 6.21Estadística de la pregunta sobre protocolo ante incidente de seguridad informática, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

16.- ¿Sabes a quien reportar un incidente de seguridad informática?

En este gráfico de barras de la Figura 6.22 muestra que el 81% si sabe a quién reportar y el 11% y 8% restante no está seguro o no sabe, respectivamente, esto refleja una buena atención sobre identificar a quién reportar algún incidente, sin embargo, aún está casi el 20% que no lo conocen, es una brecha que debería cerrarse, para poder tener un mejor manejo de acciones ante un incidente.

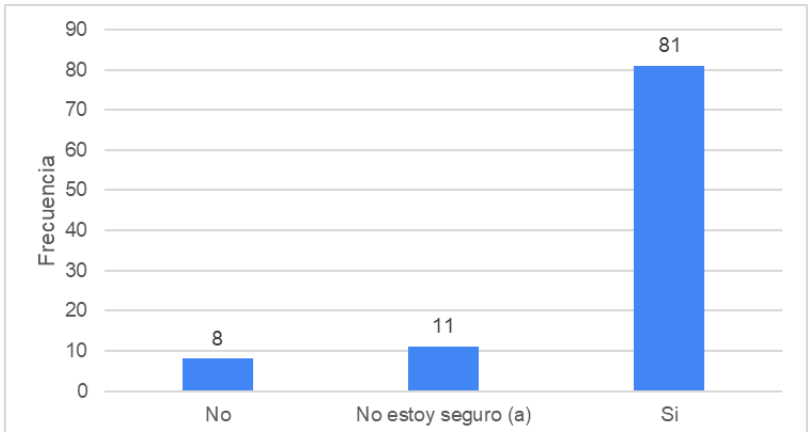

Figura 6.22 Estadística de la pregunta sobre si saben quiénes son los responsables de administrar incidentes y poder reportarles, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

17.- ¿Sabes cómo y por qué medio debes reportar un incidente de seguridad informática?

En la Figura 6.23 se visualiza que el 56% sabe de qué manera y por qué medio hacerlo; sin embargo, el 30% sabe a quién, pero no por qué canal, seguido del 14% que no sabe cómo o incluso no sabe que debía reportarse alguna acción así.

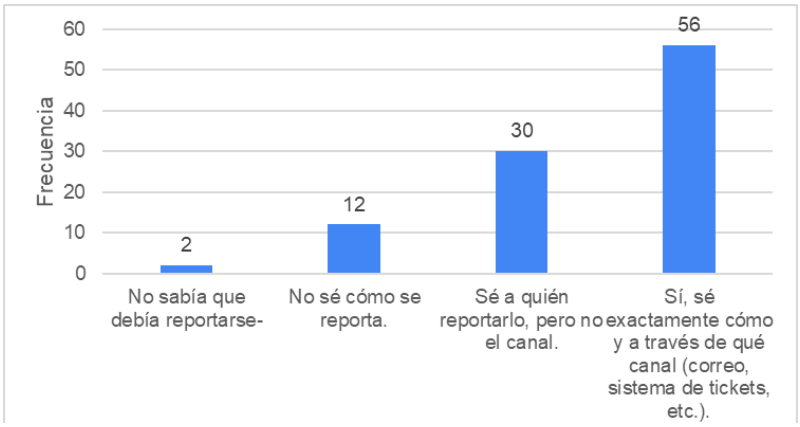

Figura 6.23 Estadística sobre cómo y qué medio se debe reportar un incidente de seguridad, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

Los resultados de la sección de respuesta y gestión de incidentes muestran que la mayoría de los encuestados posee conocimiento general sobre los principales incidentes de

ciberseguridad, como ataques de *phishing*, intrusiones no autorizadas o infecciones por *malware*.

No obstante, aún se identifican deficiencias en la claridad y la definición de roles y responsabilidades dentro de la organización al responder a un incidente, lo que podría afectar la coordinación y la eficacia de la respuesta ante un ataque.

Sección de continuidad del negocio y recuperación

18.- ¿La empresa realiza respaldos de información regularmente?

Esta pregunta de la Figura 6.24 deja ver que el 59% de la población encuestada menciona que sí hace respaldos de información; sin embargo, el 41% no está seguro o no lo hace, lo que causa una alerta sobre esta estrategia de continuidad de negocio, a pesar de tener un gran porcentaje que sabe cómo reaccionar ante un incidente como empleado, pero no qué hacer postincidente.

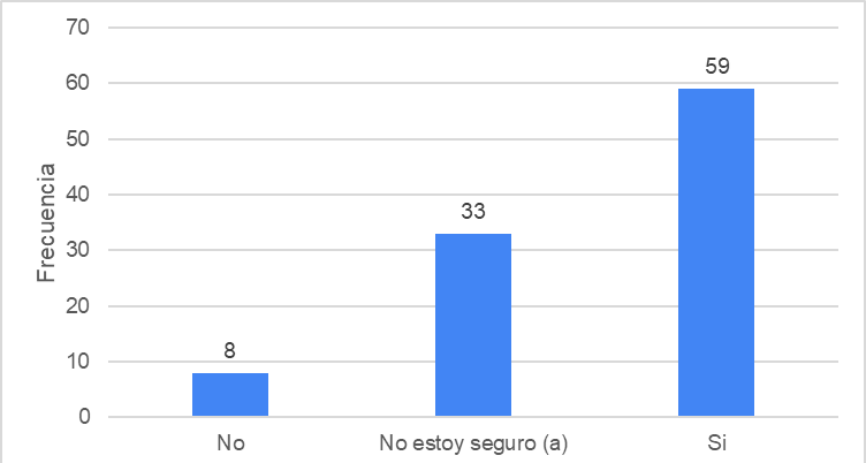

Figura 6.24 Estadística de la pregunta sobre respaldos regulares en la empresa, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

19.- ¿Los respaldos están protegidos contra cifrado o eliminación por parte de un *ransomware* como Medusa?

Esta pregunta es clave en la recuperación. Después del ataque de *ransomware,* se tiene preocupación por qué pasaría si se tienen respaldos, pero no están asegurados, lo que se

ve en la Figura 6.25: solo el 38% sí está protegido, el 17% parcialmente y el 45% no tiene respaldo ni lo tiene protegido.

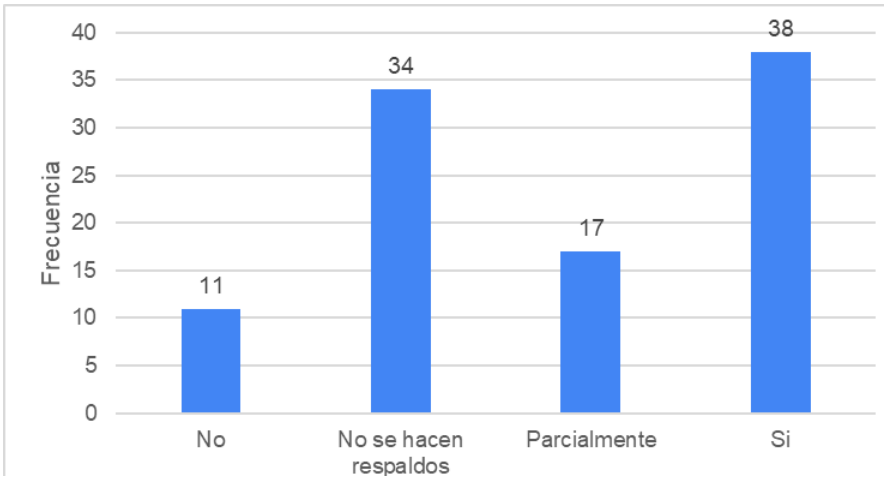

Figura 6.25 Estadística de la pregunta sobre los respaldos protegidos ante un secuestro de datos, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

20.- ¿Has participado en simulacros o pruebas de restauración?

Este gráfico circular de la Figura 6.26 demuestra que el 72% de la población ha declarado que no ha participado en simulacros o pruebas de restauración, lo que significa que tan solo el 28% sí ha participado, lo que significa que la mayoría está totalmente ajena a un evento de recuperación.

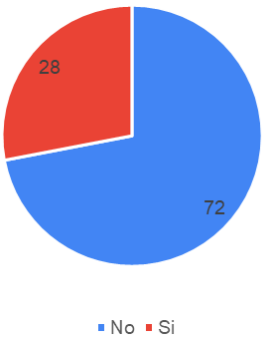

Figura 6.26 Estadística de la pregunta sobre simulacros, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

En la sección de continuidad del negocio y recuperación, los resultados indican que aproximadamente la mitad de los encuestados señala que en sus organizaciones se realizan respaldos de información. No obstante, solo el 38 % menciona que dichos respaldos cuentan con medidas de protección o cifrado, mientras que el resto no aplica dichos controles.

Por otra parte, el 72 % de los participantes indica haber participado en simulacros relacionados con incidentes o contingencias, lo que refleja avances en la preparación organizacional, aunque aún existen áreas de mejora en la protección de los mecanismos de respaldo.

Sección de auditoría y mejora continua

21.- ¿La empresa realiza auditorías o revisiones periódicas de seguridad digital?

El 52 % de la población encuestada refiere que la empresa en la que laboran, si hace auditorias o revisiones periódicas, sin embargo, aún está el 48 % que no lo hace o no está seguro, por lo que significa un gran porcentaje que a pesar de que existan reglas, y se conozcan, no se realizan revisiones periódicas que alerten sobre las brechas de seguridad, las vulnerabilidades que existen tanto en los sistemas, como en los empleados, visualizado en la Figura 6.27.

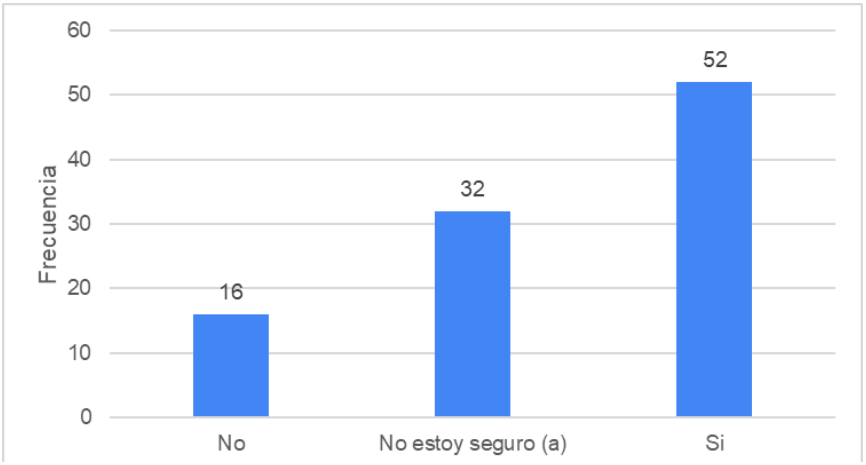

Figura 6.27. Estadística de la pregunta sobre auditorías periódicas, aplicación propia en población de Centroamérica y algunos países de Sudamérica

22.- ¿Estás familiarizado con el *ransomware* Medusa y su forma de operar?

Esta última pregunta, de la Figura 6.28 , refiere a que sólo el 13% conoce de este *ransomware,* por lo que se necesita más información sobre dicho atacante, ya que es de los principales activos que dan un ataque bruto, ya que se observa un 87% que, si ha escuchado, pero no conocen, o incluso no han oído hablar de él.

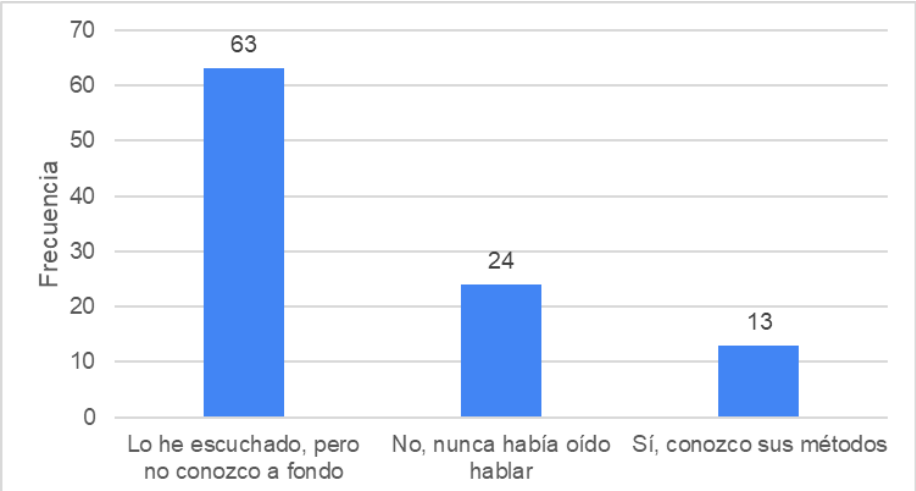

Figura 6.28 Estadística de la pregunta sobre el conocimiento de ransomware Medusa, aplicación propia en población de Centroamérica y algunos países de Sudamérica.

El instrumento de encuesta incluyó una pregunta de control de atención para verificar la consistencia y la calidad de las respuestas. Los resultados muestran que el 85% de los encuestados contestó correctamente, mientras que el 13% entendió la pregunta, pero no identificó la instrucción de control. A pesar de ello, los comentarios finales reflejan percepciones importantes sobre la ciberseguridad:

Entre los comentarios finales de los encuestados, se toman en cuenta que:

- ✓ Las empresas deberían invertir constantemente más en seguridad de la información, ya que es un área que cambia y evoluciona diariamente.
- ✓ La ciberseguridad hoy en día es un tema que debe abordarse mediante buenas prácticas para prevenir delitos informáticos.
- ✓ En muchas empresas y en la comunidad en general, hace falta concientizar sobre la importancia de la seguridad informática.

- ✓ Ciberataques que pueden ser riesgosos debido a su modo de operar, lo cual puede perjudicar a dicha empresa.
- ✓ El *Ransomware* Medusa puede llegar a ser realmente crítico si no se sabe con qué estás tratando.
- ✓ Deberían hacer partícipes a todos, en general, para que tengan conocimiento sobre ciberseguridad.

En la sección de auditoría y mejora continua, solo el 52 % de los encuestados indica que su organización realiza revisiones periódicas, mientras que el 48 % no lo hace o desconoce si se ejecutan, lo que limita la detección de brechas y vulnerabilidades. Además, aunque el 63 % conoce Medusa, solo el 13 % está familiarizado con sus métodos, lo que evidencia un conocimiento superficial de esta amenaza.

Conclusión de las respuestas a las encuestas.

En términos generales, en todas las secciones, los resultados muestran el 76% de los encuestados afirman estar familiarizados con la seguridad tecnológica frente a un *ransomware* como Medusa; sin embargo, solo el 10% de ellos, únicamente ha escuchado del tema sin conocer sus detalles. Esto evidencia un alto nivel de desinformación: aunque la mayoría reconoce distintos tipos de ataques, solo la mitad ha recibido capacitación, y no de forma continua, lo que confirma que el usuario sigue siendo el principal vector de riesgo dentro de las organizaciones.

En relación con las políticas internas, más de la mitad señala que su empresa cuenta con lineamientos claros; no obstante, una parte significativa menciona desconocer si existen o no, o bien no sabe de qué tratan. Este sesgo de desinformación también se refleja en la ausencia de roles y accesos bien definidos, ya que varios colaboradores indicaron tener acceso a plataformas o datos que no corresponden a su área, lo que incrementa las superficies de ataque.

Respecto a la preparación ante incidentes, un porcentaje considerable indica que no conoce ningún protocolo para actuar ante un evento de seguridad, lo que evidencia una clara falta de preparación institucional en materia de respuesta, contención y mitigación de amenazas actuales como Medusa.

Finalmente, los resultados sobre respaldos muestran que, aunque algunas organizaciones cuentan con copias de seguridad, un número similar de encuestados señala que no se realizan o no están protegidas adecuadamente. Esto revela la ausencia de estandarización en las prácticas de respaldo, cifrado y restauración, lo que genera un riesgo crítico para la continuidad del negocio ante un posible ataque de *ransomware.*

6.2 Resultados de la aplicación de entrevistas

A continuación, se presentan, mediante una tabla comparativa, las respuestas de los entrevistados, divididas por pregunta, y se señalan similitudes y diferencias entre ellas, así como un apartado sobre el plus de cada una.

Sección Estrategia y Políticas de Seguridad

En la Tabla 6.1 se presenta una comparativa de las diferentes respuestas de los entrevistados expertos en ciberseguridad sobre la temática de estrategia y políticas de seguridad.

Tabla 6.1 Sección Estrategia y Políticas de Seguridad

Pregunta	Similitud	Diferencias	Rescatable
1.-Frecuencia de ataques *ransomware*	-Los ataques de *ransomware* son muy frecuentes y van en aumento - Reconoces que las Pymes son blanco activo -Mencionan que el *ransomware* actual está muy sofisticado	Frecuencia continua, y gravedad del impacto Se enfoca en estadísticas concretas y menciona tipos de ataque Se enfoca en Latinoamérica y crecimiento del *Ransomware* as a Service	Experiencia, técnico y ejemplos Soporte con datos cuantitativos Perspectiva corporativa

2. Casos específicos	-Mencionan la familiaridad con Medusa, LockBit y Conti -coinciden que son grupos agresivos -mención de análisis o contacto indirecto con incidentes reales	Análisis técnico y simulaciones internas Detalles operativos de los grupos como triple extorsión Experiencia propia con clientes que sufrieron ataques reales	Seguimiento y simulación de ataques Enfoque documentado Experiencia en campo y respuestas de ataques
3.- metodologías de control de accesos y privilegios	-aplicar principio de privilegio mínimo y Zero Trust -MFA y PAM	Explicación Zero Trust en concepto y práctica Enfoque completo, segmentación y auditorías Implementación corporativa y PAM	Verificación continua Modelo más completo Enfoque tecnológico empresarial (CISCO)
4.- Políticas de seguridad para prevenir *ransomware* Medusa	-políticas de backups, control de accesos, gestión de parches, correo seguro, capacitación, respuesta a incidentes	Menciona 6 políticas clave Menciona 7 políticas clave Resume en políticas concretas como Zero Trust, Automatizaciones	Explicación Metodología Practicidad empresarial-automatización
5.- Plan de continuidad de negocio-Medusa	-fases antes, durante y después del ataque -Respaldo, recuperación, pruebas Análisis de impacto y restauración	Fases cronológicas Estructura más formal, técnica Estructura operativa, nube y pruebas	Narrativa ciclo de plan de continuidad de negocio Marcos profesionales Visión práctica y recuperación rápida

Los resultados de esta sección muestran consenso en la frecuencia creciente y sofisticación de los ataques de *ransomware,* especialmente contra Pymes, y en la familiaridad con grupos como Medusa, LockBit y Conti. Coinciden también en la importancia de los controles de acceso (principio de mínimo privilegio, Zero Trust, MFA y PAM) y en políticas clave de seguridad, como los respaldos, la gestión de parches y la capacitación.

Las diferencias se observan en el nivel de detalle técnico y en la aplicación práctica: algunos enfoques son más analíticos o corporativos, mientras que otros destacan experiencias directas, simulaciones y automatización de procesos.

Sección Detección y Monitoreo de Amenazas

En la Tabla 6.2 se muestra una comparativa de las diferentes respuestas de los entrevistados expertos en ciberseguridad, sobre la temática de detección y monitoreo de amenazas.

Tabla 6.2 Sección Detección y Monitoreo de Amenazas

Pregunta	**Similitud**	**Diferencias**	**Plus**
6.-Herramientas detección	-Uso de EDR, XDR, SIEM, IDS, IPS -Monitoreo continuo -correlación de eventos y alertas automatizadas	Función de cada componente Herramientas especificas Cisco XDR	Arquitectura y flujo operativo Variedad tecnológica Enfoque corporativo, inteligencia global
7.-Integración SIEM XDR EDR	-Integración es esencial -EDR y protección de *endpoints* -XDR cobertura -SIEM centraliza	Flujo práctico EDR, SIEM, XDR Función y flujo completo detección proactiva	Técnicas y jerarquías Explicación completa del proceso de integración Automatizaciones
8.-Inteligencia de amenazas	-Combinación entre herramienta técnica y estrategia organizacional Procesos continuos	Anticipar, identificar y mitigar ataques de Medusa Ejemplos de plataformas, herramienta-estrategia	Explicación conceptual Operación y aplicación, herramientas Seguridad-negocio

		Integración en los procesos de negocio	
9.-Rol de inteligencia de amenazas	-Anticipar, identificar y mitigar ataques. -Reducir tiempos de respuesta	Ventaja anticipada Etapas detalladas Detección anticipada de campañas	Conceptos Técnicas Anticipación práctica
10.-Indicadores clave	-Cifrado de archivos, notas, actividad inusual, conexiones sospechosas -Importancia de eventos SIEM	Renombrado de archivos, escaneo de red *Endpoints*, red, credenciales, logs Encriptación, acceso no autorizado, movimiento lateral.	Ejemplos Análisis y clasificación Priorizar rápido
11.-Primera acción recomendada	-Aislar el sistema afectado -Activación de protocolos de respuesta -Rapidez de acción	Aislar el sistema Procedimiento en estructura, Respuesta en los primeros 30 minutos, Activación de plan de respuesta	Técnicas Metodología forense Operación y velocidad de contención

Los resultados reflejan el acuerdo en la importancia del monitoreo continuo y del uso de herramientas como EDR, XDR, SIEM, IDS e IPS, así como en la integración de estos sistemas para correlacionar eventos y centralizar alertas. Se reconoce la relevancia de la inteligencia de amenazas para anticipar, identificar y mitigar ataques, reducir los tiempos de respuesta y priorizar indicadores clave, como el cifrado de archivos, la actividad inusual o el movimiento lateral.

Sección Respuesta y Recuperación ante un Ataque

En la Tabla 6.3 se visualiza un comparativo de las diferentes respuestas de los entrevistados expertos en ciberseguridad, sobre la temática de respuesta y recuperación ante un ataque.

Tabla 6.3 Sección Respuesta y Recuperación ante un Ataque

Pregunta	**Similitud**	**Diferencias**	**Plus**
12.- Protocolo de respuesta	-Flujo estructurado de respuesta -Importancia de aislamiento -presión operativa	7 fases operativas (detectar, contener, notificar, evaluar, erradicar, recuperar, comunicar y aprender) Protocolo formal con 7etapas Modelo corporativo, contención, erradicación, comunicación, recuperación	Operación para pymes Protocolo alineado a estándares internacionales Estrategias en resiliencia corporativa
13.- Comunicación durante un ataque	-Comunicación controlada, transparente y coordinada -Confianza y consistencias de mensaje -Informes a empleados, clientes y socios	Transparencia, calma y confianza Interno, externo y estrategias clave Comunicación y áreas legales	Cultura de aprendizaje post incidente gestión detallada de crisis de comunicación Reputación corporativa
14.-Medidas de seguridad de respaldos de datos	-cifrados -Pruebas periódicas, restauración, Accesos restringidos	Automatización, cifrado, almacenamiento aislado, pruebas Estrategia integral 3,2,1 Principios de inmutabilidad, cifrado, pruebas	Practicas Técnicas Políticas globales

15.-Acciones ante exfiltración y extorsión	-no negociar directamente con los atacantes . Colaborar con autoridades Minimizar daños legales	Investigar, notificar, proteger, colaborar, comunicar Contención, comunicación, alcance, recuperación No negociar, notificar, controlar	Ética y confianza Buenas prácticas internacionales Respuesta rápida y cumplimiento

Los resultados de esta sección destacan la necesidad de protocolos de respuesta claros, el aislamiento rápido de los sistemas y la comunicación coordinada con empleados, clientes y socios. También se valora contar con respaldos cifrados y controlados, y procedimientos ante exfiltración y extorsión. Las diferencias se observan en el nivel de formalidad: algunos presentan protocolos corporativos completos y alineados a estándares, mientras que otros se enfocan en experiencias prácticas para pymes.

Sección Cumplimiento, Normativas y Capacitación

En la Tabla 6.4 se observa una comparación de las diferentes respuestas de los entrevistados expertos en ciberseguridad, sobre la temática de cumplimiento, normativas y capacitación.

Tabla 6.4 Sección Cumplimiento, Normativas y Capacitación

Pregunta	**Similitud**	**Diferencias**	**Plus**
16.-Normas y estándares	Se menciona la norma ISO 27001 como marco para la alineación y el cumplimiento legal.	Cumplimiento práctico y leyes mexicanas ISO, NIST, CIS, COBIT	Cumplimiento en México Técnicas Visión de gobierno en ciberseguridad

17.-Capacitación al personal general	Capacitación constante, concientización como primera línea de defensa	Cultura organizacional Proceso, educación, simulaciones, métricas cultura Capa 8 y evaluación de respuesta en tiempo real	Valor humano como sensor Ciclo de capacitación Dinámica y técnica, respuesta ante *phishing*
18.- Capacitación al personal TI	Formación avanzada y continua	Simulaciones, ejercicios, Simulaciones, métricas Laboratorios, escenarios controlados, team red, blue	Practica constante Metodología y evaluación Entrenamiento
19.Métricas o indicadores	Usar KPIS técnicos y humanos	Técnicas, humanos y procesos Prevención, detección, recuperación, impacto Cumplimiento de parches	Integración de métricas Metodología Indicadores críticos en la industria
20.-. -Consejos para Pymes	Prevención, respaldos, MFA, c	Medidas básicas y realistas SIEM, EDR, segmentación, MFA, respaldo,	Entorno Mexicano Guía completa, seguridad Pymes Prácticas y estrategias

Los resultados de esta última sección muestran similitud en la importancia de cumplir normas como ISO 27001 y de mantener la capacitación continua del personal, tanto general como de TI, como primera línea de defensa frente a ciberataques. También se valora el uso de métricas e indicadores para monitorear la prevención, la detección y la recuperación. Las diferencias se observan en el nivel de detalle y en el alcance.

En términos generales, las respuestas de los cuatro expertos entrevistados en ciberseguridad, quienes han trabajado directamente con el *ransomware* Medusa, evidencian que, aunque existe conciencia sobre la frecuencia y gravedad del *ransomware* y se aplican prácticas como respaldos, MFA y monitoreo, aún persisten brechas importantes en políticas, control de accesos, capacitación continua y estandarización de procesos.

La integración de herramientas de detección es desigual, la respuesta a incidentes no siempre está formalizada y la capacitación varía entre niveles. En conjunto, los hallazgos muestran que las organizaciones cuentan con bases, pero requieren mayor madurez, protocolos más claros y una estrategia integral para enfrentar eficazmente amenazas como Medusa.

Finalmente, existe una tendencia de acuerdo en que la capacitación tanto del personal general como del área de TI es el pilar más crítico y, al mismo tiempo, el más descuidado. La falta de entrenamiento continuo, sumada a una cultura organizacional débil en materia de seguridad, incrementa la probabilidad de éxito de ataques basados en ingeniería social, que siguen siendo el punto de entrada más común.

7 Protocolo de gestión de riesgos y estrategias de mitigación frente a ataques de *ransomware* Medusa.

Introducción

En los últimos cinco años, el *ransomware* Medusa se ha consolidado como una de las principales amenazas para la ciberseguridad empresarial, debido a su capacidad para afectar la información, las operaciones y la continuidad del negocio. Entre sus variantes, Medusa ha ganado notoriedad por su alta capacidad de cifrado, su velocidad de propagación y sus estrategias de doble extorsión, en las que no solo se bloquea el acceso a los datos, sino que también se amenaza con filtrar públicamente los datos si no se cumple con el pago exigido.

Esta amenaza resulta particularmente peligrosa para las pequeñas y medianas empresas (pymes), debido a recursos limitados y a una menor madurez en materia de ciberseguridad. Por ello, suelen carecer de planes sólidos de prevención, detección y respuesta ante incidentes de este tipo.

El impacto de un ataque de *ransomware* Medusa puede ir más allá de la pérdida temporal de información: interrumpe operaciones críticas, deteriora la confianza de los clientes, genera pérdidas económicas significativas y acarrea consecuencias legales. Ante este panorama, es imprescindible que las pymes adopten un enfoque estructurado y proactivo para prevenir, mitigar y responder de manera eficiente a este tipo de amenazas.

El propósito de este marco es diseñar una guía integral de gestión administrativa que combine estándares y mejores prácticas internacionales (ISO 27001, NIST e ITIL) para fortalecer la postura de seguridad de las pymes frente al *ransomware* Medusa.

Referencias normativas:

- ISO 27001. **Base organizacional** para definir políticas, procedimientos, controles, estructura de gestión
- ITIL. Marco de mejores prácticas para la **gestión de servicios de TI (Respuesta y recuperación ante un ataque- continuidad de negocio y operación)**
- NIST. **Identificar, Proteger, Detectar, Responder y Recuperar**

Objetivo del protocolo

Diseñar un protocolo de gestión administrativa basado en estándares internacionales (ISO 27001, NIST e ITIL) que permita a las pymes prevenir, mitigar y responder eficazmente ante ataques de *ransomware* Medusa, garantizando la continuidad del negocio y reduciendo el impacto operativo y reputacional.

7.1 Componentes del marco

7.1.1 Prevención

La prevención en la seguridad de la información consiste en anticipar riesgos y aplicar medidas para proteger los sistemas y los datos. Incluye políticas de seguridad, la clasificación de activos según criticidad y sensibilidad, y la capacitación del personal. Para ello, las organizaciones implementan políticas de seguridad de la información, que establecen normas, responsabilidades y buenas prácticas para proteger los datos y los sistemas, esto permite asignar controles adecuados.

También abarca la gestión de parches, copias de seguridad, controles de acceso, identidades y contraseñas. Se complementa con enfoques como Zero Trust, segmentación de red, y la realización de pruebas de seguridad.

Finalmente, el plan de continuidad del negocio garantiza que las operaciones puedan mantenerse o recuperarse rápidamente ante situaciones adversas, asegurando la resiliencia organizacional.

7.1.2 Políticas de seguridad de la información

La ISO/IEC 27001 es un estándar internacional que forma parte de la familia de normas ISO y está estructurado conforme al Anexo SL, que proporciona la base común para todos los sistemas de gestión ISO, independientemente del sector o del giro de la organización.

En el caso específico de la ISO/IEC 27001, su objetivo principal es gestionar la seguridad de la información, definiendo los requisitos necesarios para implementar, mantener y optimizar un Sistema de Gestión de Seguridad de la Información (SGSI).

Este estándar se apoya en un conjunto de 93 controles de seguridad definidos en el Anexo A, los cuales se organizan en cuatro categorías principales:

- Controles organizacionales
- Controles de personas
- Controles físicos
- Controles tecnológicos

De acuerdo con este marco normativo, se enumeran las políticas de seguridad de la información más relevantes, en particular, aquellas vinculadas a la primera etapa de la ciberseguridad: la prevención.

1. Política de seguridad de la información
    - ✓ Documento rector que define objetivos, compromisos de la alta dirección, roles y responsabilidades en materia de seguridad.
2. Política de control de accesos (A.5 y A.8)
    - ✓ Reglas para gestionar identidades, contraseñas, accesos mínimos necesarios principio de privilegio mínimo, autenticación multifactor, etc.
3. Política de uso aceptable de activos (A.5.10 y A.5.11)
    - ✓ Define cómo se deben usar los recursos tecnológicos, correo electrónico, internet, dispositivos móviles y medios de almacenamiento.
4. Política de clasificación y manejo de la información (A.5.12 y A.5.13)
    - ✓ Establece niveles de confidencialidad (pública, interna, confidencial, restringida) y cómo se debe proteger y compartir cada tipo.
5. Política de seguridad física y ambiental (A.7)
    - ✓ Control de accesos a instalaciones, protección de equipos, vigilancia, y medidas contra incidentes ambientales.
6. Política de gestión de recursos humanos en seguridad (A.6)
    - ✓ Incluye verificaciones previas a la contratación, cláusulas de confidencialidad, capacitación en seguridad y responsabilidades del personal.
7. Política de gestión de copias de seguridad (A.8.12)

- ✓ Reglas para realizar respaldos periódicos, su almacenamiento seguro y pruebas de restauración.

8. Política de protección contra *malware* y amenazas técnicas (A.8.7 y A.8.8)
   - ✓ Uso de antivirus, actualizaciones, parches, controles de *endpoints* y navegación segura.
9. Política de seguridad en las comunicaciones (A.8.19 – A.8.23)
   - ✓ Cifrado, protección en redes, uso de VPN, seguridad en correo electrónico y transferencia de datos.
10. Política de continuidad y resiliencia (A.5.29 y A.5.30)
    - ✓ Orientada a mantener operaciones críticas ante incidentes, pero también preventiva al establecer redundancia y planes de respaldo.

a. Gestión de activos críticos, inventario clasificado-criticidad y sensibilidad.

Es el proceso en el cual, una organización identifica, documenta, valora y protege los recursos más importantes en el funcionamiento de las operaciones y continuidad de negocio.

Entre estos activos se mencionan información, sistemas, infraestructura tecnológica, software, hardware, personal y procesos, y su pérdida representa un impacto significativo para la organización.

Sirve para priorizar la protección y asignación de recursos, facilitar la toma de decisiones, garantizar la continuidad del negocio, así como del cumplimiento normativo.

La clasificación de los activos según su criticidad y sensibilidad se presenta en la Tabla 7.1 Clasificación de activos según la criticidad: y la Tabla 7.2 Clasificación de activos según la sensibilidad.

Tabla 7.1 Clasificación de activos según la criticidad

Nivel de criticidad	Descripción	Ejemplo
Critico	Su pérdida o falla detiene procesos clave del negocio y afecta directamente la operación o reputación.	Servidor, bases de datos, ERP, sistema financiero
Alto	Su interrupción causa afectaciones importantes, pero existen mecanismos temporales de contingencia.	Correo electrónico, CRM, servidor de archivos.
Medio	Su pérdida genera molestias operativas moderadas o retrasos controlables.	Sistema de registro interno, portal de empleados.
Bajo	No impacta significativamente las operaciones; su función es de apoyo o administrativa.	Equipos de prueba, impresoras, software auxiliar.

Tabla 7.2 Clasificación de activos según la sensibilidad

Nivel de criticidad	Descripción	Ejemplo
Critico	Información confidencial cuya divulgación o alteración puede causar daños severos legales, financieros o reputacionales.	Datos personales, financieros, credenciales de acceso, reportes de seguridad.
Medio	Información interna que no es pública, pero cuya exposición no implica daño severo inmediato.	Procedimientos internos, manuales técnicos, reportes de desempeño.
Bajo	Información pública o sin riesgo relevante en caso de divulgación.	Material de marketing, boletines o comunicados institucionales.

En el caso específico del *ransomware* Medusa, la clasificación de la información adquiere un valor estratégico adicional, ya que este tipo de *ransomware* utiliza técnicas de doble extorsión, en las que el atacante no solo cifra la información, sino que previamente exfiltra datos sensibles para amenazar con su publicación si la organización no paga el rescate.

Por ello, la clasificación de la información no solo debe considerar su nivel de confidencialidad interna, sino también el riesgo de exposición pública y el impacto reputacional que podría generar una filtración de datos.

b. Concientización y capacitación de personal:

Es el proceso en el cual se forma y sensibiliza a los colaboradores de una organización respecto a los riesgos de ciberseguridad, buenas prácticas digitales y protocolos de seguridad ante incidentes.

El objetivo de este apartado es convertir al personal en la primera línea de defensa ante amenazas como Medusa. Todo el personal de la organización debe participar, desde niveles operativos, hasta directivos.

En cuanto al personal en general, mantener entrenamientos constantes sobre campañas de concientización y simulacros, para medir la capacidad de respuesta del personal, en tiempo real; cada empleado, puede verse como un "sensor humano", el cual es capaz de detectar intentos de *phishing* por mencionar un ejemplo.

Esto se desglosa en:

- Implementar programas de concientización con contenido práctico y políticas claras.
- Realizar simulacros sobre: *phishing* simulado, en envío de correos falsos controlados; ingeniería social práctica, en prueba de respuesta a llamadas o solicitudes fraudulentas; retroalimentación inmediata, con informes de errores y recomendaciones para corregir.
- Entrenamiento en procedimientos internos, identificar actividades clave como solicitudes de acceso y datos sensibles, uso seguro de herramientas corporativas como VPN, correo corporativo, almacenamiento en la nube, antivirus, firewall, etc.
- Evaluación y métricas en constante monitoreo, con encuestas para asegurar la comprensión de las políticas, campañas y ajustarlas según sea necesario.
- Cultura de ciberseguridad, en este punto, incentivar que el personal reporte incidentes, integrar la ciberseguridad como parte de todos, no sólo de un área.

Por el lado de la capacitación al personal de áreas de TI, es similar a la de general, solo que, en este ámbito, destaca, el nivel más profundo en entrenamientos de detección avanzada, respuesta a incidentes y escenarios de ataque controlados, sobre todo, la actualización constante en herramientas, de EDR/XDR, MDR, SOAR. Como: Microsoft Defender for Endpoint para-Windows, Sophos Home Free, ESET Protect, por mencionar algunos.

Del mismo modo, contenido práctico sobre cómo identificar correos sospechosos, enlaces maliciosos, adjuntos peligrosos y solicitudes inusuales, que son los principales vectores de ingreso del *ransomware* Medusa.

Entre los componentes base de una capacitación se deben incluir: diagnóstico de necesidades, objetivos de aprendizaje, contenido temático, método, perfil del instructor, materiales y recursos, cronograma y evaluación del aprendizaje y de la capacitación.

c. Gestión de parches, copias de seguridad y actualizaciones.

Una opción eficaz y comprobada es la estrategia 3-2-1: consta de 3 copias de los datos: mantener una original y 2 copias; 2 medios diferentes, como discos locales, almacenamiento de red, cinta o la nube; y 1 copia fuera de línea, que impide que el *ransomware* cifre todas las copias simultáneamente.

Respaldos inmutables, es decir, que no se pueden modificar ni eliminar una vez generados y por cierto tiempo. Esto dirige a respaldos automáticos, cifrados y guardados con el método 3-2-1, con cuentas privilegiadas mediante PAM, es decir, accesos muy limitados y probar regularmente su recuperación.

Aunque las copias de seguridad representan una de las principales medidas de recuperación frente a ataques de *ransomware,* en el caso de Medusa no son suficientes por sí solas, ya que el atacante puede conservar copias de la información exfiltrada y utilizarla como mecanismo de presión adicional mediante su publicación.

d. Controles de accesos, contraseñas y gestión de identidades.

Se aplican principalmente 3 métodos para esta sección, el primero es el principio de privilegio mínimo como pilar del control y la gestión de accesos, es decir, cada usuario

recibe solo los permisos necesarios para la ejecución de sus tareas, siguiendo el segundo método con el control basado en roles, en este sentido, asignar permisos según el rol, así como las reglas más granulares, que consideren atributos como ubicación, dispositivo, nivel de riesgo, etc.

El tercer método, autenticación multifactor, MFA, esto trata del uso de tokens, aplicaciones de autenticación, biometría que consta del factor de conocimiento, es decir, información que solo el usuario debe saber, como ejemplos, una contraseña, pin; factor de posesión, objeto que el usuario debe tener físicamente, como un celular donde pueda consultar algún token o aplicación de autenticación; factor biométrico, algo que es parte de la persona, como una huella dactilar o reconocimiento facial.

Otra metodología funcional es el modelo Zero trust, que a continuación en la siguiente sección se desglosa sobre qué contiene, y de qué forma se puede aplicar.

e. Arquitectura Zero Trust Security como control prioritario contra Medusa.

- Confianza cero, no confiar en nada ni en nadie, incluso dentro de la red corporativa.
- Verificación absoluta, comprobar todo de manera explícita, aunque todo sea muy obvio.
- Asumir riesgo, hay que admitir que todo puede ser vulnerado.
- Acceso de privilegios al mínimo, mediante Just InTime (JIT) / Just Enough Administration (JEA), quiere decir que debe conceder permisos solo por el tiempo necesario, o limitar los permisos a lo necesario para la ejecución de la tarea, en el entendido de que JIT controla cuándo se otorga el acceso y JEA controla cuándo se concede el acceso.

f. Simulacros y pruebas de seguridad

Son aquellos ejercicios planificados donde se simulan ciberataques, incidentes o fallos de seguridad ante un ataque de Medusa *Ransomware,* permiten ver si la organización detecta a tiempo, aísla el daño y recupera la operación sin pagar rescate.

Estos simulacros y pruebas de seguridad sirven para verificar la efectividad de los planes de respuesta a incidentes, la reacción del personal ante una crisis y detectar fallas de comunicación, así como la capacidad de detección, contención y recuperación.

Debe contener un objetivo claro, el escenario simulado pero realista, como un intento de ataque de Medusa, el alcance, roles y responsabilidades, la serie de eventos, registro y monitoreo, evaluación de desempeño y la retroalimentación; este tipo de ejercicios se deben realizar por lo menos una vez al año y las pruebas de copias de seguridad al menos cada tres meses.

En escenarios realistas, se deben contemplar correos con supuestos documentos legales, facturas falsas y archivos comprimidos con los cargadores iniciales de malware. En cuanto a un ejemplo sobre una simulación ante un ataque de Medusa, se visualiza como:

1. Un empleado abre un archivo adjunto sospechoso desde el correo corporativo
2. Se simula el cifrado de archivos en un servidor, se puede cifrar archivos en una carpeta de red, mostrando un mensaje falso de rescate y ante esto, se desactiva el acceso a servicios simulados como el propio correo.
3. El equipo de seguridad detecta alertas mediante el firewall, en este caso, el coordinador del simulacro debe dirigir el ejercicio y supervisarlo, el equipo técnico de TI detecta, aísla, mitiga y restaura servicios, en cuanto al equipo de comunicación controla la comunicación interna y externa para que esto no se propague con más personal, en cuanto al analista de ciberseguridad, registra los logs del evento, y el origen del ataque, todo se documenta para tener un plan de mejora actualizado.
4. La evaluación por realizar se centra en el aislamiento del equipo, comunicación al responsable, inicio del protocolo de respuesta y restauración de datos desde el *backup*.

g. Segmentación de red, zona desmilitarizada (DMZ) y arquitectura segura

La segmentación de red trata de dividir una gran red en varias subredes más pequeñas y controladas, esto con el fin de limitar el movimiento lateral de amenazas como lo hace el *ransomware* Medusa.

Para que sea una arquitectura segura, debe cumplir con cuatro capas, la primera es la externa, el firewall perimetral que filtre todo el tráfico entrante y saliente, la capa intermedia que aísla de la red interna aquellos servidores expuestos como web, correo y DNS, el tercero es la capa interna y red corporativa, este contiene sistemas críticos y bases

de datos, se protege con firewall interno y controles de acceso, por último se mantiene la capa de respaldo, con servidores de backup y monitoreo mediante SIEM.

h. Plan de continuidad de negocio

Se contemplan la redundancia de la infraestructura, la recuperación ante desastres en la nube, los respaldos segmentados y las pruebas periódicas para asegurar una recuperación rápida. El plan se considera antes, durante y después de un ataque.

Antes del ataque, en la preparación, se realiza el análisis del impacto del negocio, esto consta de la identificación de los procesos y sistemas críticos, y así, determinar el tiempo máximo de recuperación y el punto máximo de recuperación, es decir, cuánto tiempo como máximo puede estar caído un servicio, y cuánta pérdida de datos es tolerable, sin dejar de lado la definición de las estrategias de continuidad, con los respaldos.

Durante el ataque, iniciar con los protocolos de respuesta inmediata, como lo es el aislamiento de los sistemas afectados y notificación al equipo de respuesta, la comunicación interna y externa para evitar que el atacante robe información, Aquí se deben establecer roles claros, identificar quién lidera la respuesta técnica y quien lidera la comunicación, así mismo, en esta etapa se ejecutan soluciones temporales o manuales para continuar operando de forma mínima, al menos hasta la restauración.

Después del ataque, se realizan los procedimientos de recuperación, en el que se hace la restauración desde backups verificados, asegurando que la amenaza fue eliminada, esta recuperación se hace de forma escalonada, es decir, se priorizan las funciones criticas para el negocio.

Por último, post recuperación se toma un plan de comunicación de crisis, donde se definen los canales para informar con mensajes predefinidos a toda la comunidad, esto con la finalidad de minimizar el pánico y daño reputacional, se ejecutan capacitaciones y simulacros para medir tiempos de respuesta y claro, con esto la actualización del plan de acuerdo a las lecciones aprendidas en las pruebas y los incidentes reales, con el acompañamiento de auditorías post incidentes y actualización de políticas y parches de seguridad.

En los puntos clave para el ransomware Medusa, se deben incluir procedimientos para gestionar filtraciones y cumplir con las normativas de protección de datos, con apoyo de la GDPR y de la Ley Federal de Protección de Datos Personales.

GDPR (Reglamento General de Protección de Datos – Europa)

- Notificación obligatoria de incidentes en un plazo máximo de 72 horas.
- Registro de medidas de mitigación y acciones correctivas.
- Aplicación del principio de responsabilidad proactiva (accountability).

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México)

- Obligación de informar al titular de los datos cuando se produzca una vulneración que afecte sus derechos.
- Implementar medidas de seguridad administrativas, técnicas y físicas.
- Mantener un programa integral de protección de datos y evidencias del cumplimiento.

7.1.3 Detección

La implementación de umbrales de tráfico saliente permite identificar no solo anomalías técnicas en la red, sino también posibles intentos de exfiltración de información previos al proceso de cifrado característico de los ataques de *ransomware.*

En este contexto, la detección basada en el comportamiento se convierte en un mecanismo clave para identificar actividades sospechosas, como la compresión masiva de archivos o el establecimiento de conexiones persistentes con servidores de comando y control (C2) antes de que el ataque sea visible.

Detectar estas señales tempranas resulta especialmente relevante ante amenazas como Medusa, ya que identificar el ataque antes de la fase de cifrado puede evitar escenarios de doble extorsión, lo que representa una diferencia crítica respecto a los modelos tradicionales de *ransomware.*

a. Definir umbrales y criterios de alerta, información detallada en la Tabla 7.3 Definición de umbrales y criterios de alerta, la tabla es un ejemplo de implementación práctica

que muchos equipos de ciberseguridad crean basándose en documentación técnica de NIST y (The MITRE Corporation, 2025)

Tabla 7.3 Definición de umbrales y criterios de alerta

Tipo de Evento	Evento detectado	Umbral	Criterio de alerta	Nivel de riesgo
Autenticaciones	Intentos fallidos de inicios de sesión	Más de 5 intentos en 10 minutos por usuario	Posible ataque de fuerza bruta o intento de acceso no autorizado	Medio
Consumo de CPU	Picos anormales en servidores	Más del 80% de consumo durante 10 minutos o más	Posible cifrado por *ransomware* Medusa	Medio
Accesos privilegiados	Uso de cuentas de administrador fuera del horario laboral	Inicios de sesión anómalos en horarios no laborales	Posible compromiso interno, desplazamiento lateral por *ransomware* Medusa	Alto
Tráfico de red	Aumento inusual en transferencia de datos salientes	Más del 200% del promedio por día	Posible exfiltración por *ransomware* Medusa	Alto
Modificación de archivos	Cambios o cifrados masivos	Más de 100 archivos modificados en 5 minutos	Actividad por *ransomware* Medusa	Critico
Alertas SIEM/EDR	Detección masiva de ejecución de procesos	Correlación de eventos registrados	Sospecha de *ransomware* Medusa	Critico

b. Alertas y herramientas de detección

La clave está en la integración de las herramientas: el EDR protege el *endpoint*, el XDR correlaciona datos en la red, en la nube y en los usuarios, y el SIEM consolida la visibilidad organizacional.

En cuanto al EDR, proporciona visibilidad en tiempo real del comportamiento de cada dispositivo final y es capaz de identificar patrones sospechosos, bloquear la ejecución de procesos de cifrado masivo, aislar el equipo infectado para cortar la propagación y permitir un análisis forense del incidente. Algunos ejemplos de herramientas son: CrowdStrike Falcon, SentinelOne y Microsoft Defender for Endpoint.

XDR, mantiene la visibilidad y respuesta extendida, detecta movimientos laterales y conexiones a servidores de Command y Control, correlaciona los eventos y orquesta acciones automáticas, en la integración, XDR recibe eventos del EDR y los correlaciona para ejecutar respuestas automáticas.

Con el SIEM, se apoya para correlacionar eventos que en conjunto indican actividad del *ransomware,* y envía alertas al equipo de seguridad, este centraliza, normaliza los eventos, es decir, identifica los patrones que, de manera individual, parecen normales, pero en conjunto, son señales de ataque, como ejemplos, los intentos masivos e inicio de sesión, subida de datos y actividad anómala en la red. Ejemplos de estas herramientas son: Splunk, IBM QRadar, Elastic Security.

A nivel de red, se utilizan los sensores IDS/IPS, estos monitorean el tráfico en búsqueda de patrones maliciosos, herramientas como Suricata, Snort, Palo Alto Threat Prevention, detectan patrones de tráfico malicioso, conexiones con C2 (Command & Control) y explotación de vulnerabilidades.

c. Detección basada en comportamiento.

La detección basada en el comportamiento monitorea continuamente la actividad del sistema, de la red y de los usuarios. Utiliza algoritmos, reglas de correlación o incluso inteligencia artificial para detectar desviaciones del comportamiento normal.

Entre las etapas del funcionamiento se encuentran:

- Establecimiento de la línea base: registro del comportamiento normal de los usuarios, procesos y sistemas, como los horarios de acceso, el volumen de tráfico y los comandos ejecutados.

- Monitoreo continuo: observando las actividades en tiempo real, como los movimientos de res, procesos del sistema o modificaciones de archivos.
- Análisis y correlación: comparando las acciones actuales con el patrón normal, el sistema genera una alerta o bloqueo automático al detectar una desviación significativa de estas acciones.
- Respuesta automatizada: herramientas como EDR o SIEM, aíslan el equipo, detiene los procesos sospechosos y notifican el equipo de seguridad,

d. Pruebas y validaciones periódicas.

Las pruebas y validaciones periódicas son esenciales para comprobar la efectividad de los controles de seguridad, la detección temprana de amenazas y la capacidad de respuesta del personal ante incidentes reales como un ataque de *ransomware,* en la Tabla 7.4 se observan algunos tipos de prueba y ejemplos.

Tabla 7.4 Pruebas y validaciones periódicas

Tipo de prueba	Descripción	Ejemplo
Pruebas técnicas controladas	Simulación de ataques reales en entornos seguros para verificar detección	Ejecutar un archivo señuelo (simulador de *ransomware)* y comprobar si el SIEM genera alerta.
Validaciones de procesos	Evaluación de la correcta ejecución de protocolos y roles de respuesta	Revisar si el personal notifica incidentes conforme al procedimiento establecido.
Revisiones de configuración	Análisis de políticas, reglas y firmas de detección.	Validar que los filtros del firewall y antivirus estén actualizados y activos

e. Notificaciones internas

Son los avisos formales que se generan y distribuyen dentro de la organización cuando se detecta una actividad sospechosa, como un ataque de *ransomware* Medusa, su objetivo es

garantizar la comunicación rápida, clara y escalonada entre las áreas para activar los protocolos de respuesta sin generar pánico o desinformación.

A continuación, se muestra la Tabla 7.5, sobre los principales medios de notificación y su uso principal, y en la Tabla 7.6 el rol con la responsabilidad principal

Tabla 7.5 Principales medios de notificación interna

Medio	Uso principal
Correo corporativo seguro, con cifrado	Comunicación formal y trazable entre equipos técnicos y directivos.
Sistema de gestión de incidentes como Jira, Service Now, Asana	Registro oficial del incidente y su evolución.
Teléfono para llamada directa o mensaje	En casos críticos que requieren acción inmediata.
Panel SIEM o consola de monitoreo	Genera alertas automáticas visibles a los analistas en tiempo real.
Mensajería instantánea como Teams	Avisos inmediatos y coordinación rápida.

Tabla 7.6 Roles y responsabilidades en notificación interna

Nivel o rol	Responsabilidad
Analista SOC o de ciberseguridad	Emite la alerta inicial con evidencias técnicas.
Líder de TI o Responsable de seguridad de la Información (CISO)	Evalúa la gravedad y autoriza la notificación a niveles superiores.
Equipo de respuesta a incidentes	Coordina la comunicación con las áreas afectadas y da seguimiento técnico.
Alta Dirección / Comité de seguridad	Toma decisiones estratégicas y aprueba medidas de contención.
Usuarios internos	Reciben notificaciones preventivas o instrucciones específicas (por ejemplo, desconectar equipos).

f. Incidentes y respuestas

SABSA (Sherwood Applied Business Security Architecture) es un marco de arquitectura de seguridad empresarial que asegura que cada control y respuesta estén alineados con los objetivos del negocio.

En el contexto de la ciberseguridad y el ransomware, se aplica para estructurar la gestión estratégica de incidentes, asegurando la coherencia entre lo técnico y lo administrativo.

La aplicación que sigue se basa en 5 líneas:

1. Contextual: Alinea la gestión de incidentes con los objetivos del negocio, es decir, define qué sistemas y datos son críticos para priorizar su protección.
2. Conceptual: Diseña la estrategia general de respuesta a y recuperación, creando plan de respuesta ante *ransomware.*
3. Lógica: Traduce políticas en procesos técnicos, estableciendo procedimientos de detección, contención y restauración.
4. Física: Implementa controles y herramientas específicas, como EDR, SIEM, backups, etc.
5. Componente: supervisa los controles para su correcto funcionamiento, mediante pruebas, auditorías y métricas.

7.1.4 Respuesta

Es importante considerar que amenazas como Medusa no ejercen únicamente presión técnica sobre las organizaciones, sino también presión psicológica y mediática asociada a la exposición pública de la información comprometida.

En este contexto, el rol de la comunicación institucional adquiere un carácter crítico en la gestión del incidente, dejando de ser un elemento opcional o secundario.

Asimismo, la coordinación con el área legal debe activarse desde las primeras etapas del incidente, incluso antes de confirmar una posible filtración de datos, con el fin de preparar la respuesta organizacional y el cumplimiento de obligaciones regulatorias.

De igual manera, la decisión de no pagar un rescate debe sustentarse en criterios objetivos, como la evidencia forense disponible, la evaluación del impacto reputacional y la capacidad real de recuperación de los sistemas afectados. Estos elementos permiten diferenciar claramente la respuesta organizacional ante amenazas como Medusa de otros tipos de ransomware que no incorporan componentes de filtración ni de extorsión pública.

a. Procedimientos de aislamiento inmediato (plan de respuesta a incidentes): evitar movimiento lateral.

Pasos iniciales clave:

1. Aislar los *endpoints* y servidores comprometidos
2. Desconectar de la red local y VPN.
3. Evitar que se conecten a unidades compartidas, nube o correos corporativos.
4. No apagar los equipos
5. Mantenerlos encendidos permite conservar evidencia para análisis forense y recuperación.
6. Activar el protocolo de respuesta a incidentes.
7. Notificar al equipo de seguridad y documentar los eventos.
8. Revisar alertas del EDR/XDR y del SIEM para confirmar la extensión del compromiso.
9. Bloquear cuentas comprometidas, especialmente usuarios con privilegios elevados, para cortar el acceso del atacante.
10. Preservar evidencia
11. Capturar logs, imágenes de memoria y registros de red antes de cualquier limpieza.

b. Roles y responsabilidades del equipo de respuesta

A continuación, se presenta la Tabla 7.7, con los niveles o roles y las responsabilidades principales que intervienen en un equipo de respuesta ante incidentes.

Tabla 7.7 Roles y responsabilidades del equipo de respuesta

Rol	Responsabilidad	Acciones
Coordinador del equipo de respuesta (CISO o Líder de seguridad)	Dirige y supervisa todas las fases del manejo del incidente.	Autoriza acciones de contención y recuperación. Coordina la comunicación interna y externa. Informa a la alta dirección.
Analista de ciberseguridad	Monitorea, detecta y confirma alertas de seguridad.	Analiza logs y correlaciones en SIEM. Identifica patrones sospechosos. Documenta evidencias técnicas.
Administrador de TI	Contención técnica y restauración de sistemas.	Aísla servidores o *endpoints* comprometidos. Aplica parches y restablece respaldos. Valida la integridad del sistema posterior al ataque.
Especialista forense digital	Preserva y analiza evidencias electrónicas.	Realiza análisis forense de archivos, memoria y red. Identifica vector de ataque y posibles exfiltraciones. Elabora informe técnico detallado.
Responsable de comunicación	Gestiona mensajes internos y externos durante el incidente.	Emite comunicados controlados al personal. Coordina mensajes con dirección y área legal. Previene la difusión de información no oficial.
Alta dirección	Toma decisiones estratégicas durante el incidente	Define nivel de impacto y continuidad operativa. Autoriza comunicación externa (proveedores, clientes). Evalúa acciones posts incidentes.

c. Coordinación con autoridades y proveedores.

El objetivo es garantizar que la organización cumpla con sus obligaciones legales, reglamentarias y contractuales, minimice los riesgos de exposición y facilite la recuperación rápida de los sistemas y datos tras un incidente de *ransomware.*

El procedimiento recomendado es el siguiente:

i. Una vez detectado el incidente, el equipo de respuesta notifica al coordinador de seguridad, se documenta el evento en la bitácora de incidentes, incluyendo alcance, sistemas afectados y evidencia que se encuentre disponible.
ii. Se determinan si los datos comprometidos incluyen información sensible, y se revisan los marcos normativos aplicables.
iii. Se realiza una notificación formal a las autoridades competentes, incluyendo tipo de datos comprometidos, fecha y hora del incidente, medidas de contención aplicadas y plan de recuperación.
iv. Se ejecuta la coordinación de contacto con proveedores críticos de tecnología, servicios en la nube o backups para confirmar el estado de los respaldos y coordinar la recuperación de datos o servicios.
v. Por último, se mantiene el seguimiento mediante documentación, sobre las interacciones y medidas aplicadas, integrando lecciones aprendidas y comunicación constante con las autoridades y proveedores.

d. Preservación de evidencias forenses.

i. Aislar el equipo, desconectar/red, no apagar si necesitas memoria.
ii. Registrar detección (quién, cuándo, sistema). fecha/hora local, quién detectó, sistemas afectados, IP, usuarios implicados.
iii. Capturar memoria RAM y procesos activos: usar herramienta de captura de memoria.
iv. Capturar tráfico de red, si es posible.
v. Fotografiar evidencias físicas y pantalla.
vi. Imágenes forenses del disco, podría ayudar la herramienta write- blocker.
vii. Exportar logs EDR
viii. Verificar backups/snapshots.

ix. Generar hashes y registrar en cadena de custodia
x. Transferir a almacenamiento cifrado y seguro.
xi. Analizar en Workstation forense (sobre copia).
xii. Documentar todo (bitácora) y coordinar con legal/autoridades.

e. Procedimientos legales y regulatorios

La exfiltración de datos personales, incluso en escenarios en los que el cifrado de la información no se materializa con éxito, constituye un incidente relevante desde la perspectiva normativa y de protección de datos.

Este tipo de eventos puede implicar la obligación de notificar a las autoridades competentes, comunicar la situación a los titulares de los datos afectados y generar evidencia documental que permita acreditar la gestión del incidente.

En este sentido, el cumplimiento de las disposiciones normativas no debe considerarse únicamente como un requisito legal, sino también como un componente estratégico dentro de la mitigación del impacto reputacional y la gestión de la confianza de los usuarios y partes interesadas.

Identificar el tipo de información afectada y la ubicación de la organización, esto basándose en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en México, por ejemplo, o el Reglamento General de Protección de Datos en Europa.

En la organización que se ubique, deberá hacer notificaciones a los titulares de los datos si es que se comprometen sus derechos, notificar a la autoridad de control en un máximo de 72 horas desde el incidente, implementar medidas de seguridad técnicas, físicas y administrativas, y documentar las acciones correctivas y preventivas.

En ataques de *ransomware* con doble extorsión como Medusa, las obligaciones legales pueden activarse incluso cuando la organización logra restaurar sus sistemas desde respaldos, ya que la posible exfiltración de datos personales puede generar responsabilidades regulatorias y obligaciones de notificación

Esto se definiría de la siguiente manera:

a. Activar al área legal y cumplimiento.
   Revisar contratos, políticas de seguridad de la información, acuerdos de confidencialidad (NDA) y cláusulas de ciberseguridad.
b. Determinar la obligación de notificar.
   Si hubo filtración de datos personales o sensibles, y a quiénes reportar.
c. Emitir notificación oficial.
   Dirigida a autoridades competentes, las organizaciones correspondientes a la ubicación geográfica del suceso.
   Incluir tipo de datos afectados, número estimado de registros, impacto potencial y medidas correctivas y preventivas.
d. Comunicación a afectados.
   Mensaje formal y claro indicando riesgos y recomendaciones, como cambio de contraseñas, monitoreo de cuentas, aislamiento de *endpoints*.
e. Conservación de evidencia.
   Mantener intactas las pruebas digitales y documentales para posibles auditorías o procesos legales, desde las copias.

f. Evaluación del alcance del impacto

En esta sección se tiene por objetivo medir la magnitud del daño operativo y técnico que provocó el ataque; esto, con el fin de definir prioridades de recuperación y acciones de mejora continua.

De acuerdo con:

- Revisión de los logs y los registros del SIEM o EDR
- Análisis forense de los sistemas cifrados
- Consultas con áreas de negocio y TI
- Informe final del impacto, clasificado por niveles:
    - Bajo: Afectación mínima, recuperación en menos de 24 horas
    - Medio: Afectación parcial, recuperación moderada en 1- 3 días

- Alto: Afectación significativa, pérdida de datos o servicios, recuperación en más de 3 días
- Critico: Compromiso total, datos exfiltrados, daño legal grave.

7.1.5 Recuperación

A diferencia del *ransomware* genérico, la recuperación frente a Medusa no concluye con la restauración de los sistemas comprometidos, ya que los datos robados pueden publicarse semanas o incluso meses después del incidente. Esta situación implica que la organización permanezca expuesta a posibles escenarios de extorsión secundaria o daño reputacional prolongado.

a. Restablecimiento seguro de operaciones (sistemas y datos).
    - Verificación completa de erradicación del *ransomware* y sus puertas traseras.
    - Restauración de datos a partir de respaldos verificados aplicando la regla 3-2-1, que consiste en 3 copias de los datos, 2 medios distintos y 1 fuera de línea, o en la nube con cifrado.
    - Validación de integridad y consistencia de la información restaurada.
    - Reinstalación limpia del sistema operativo y software crítico.
    - Aplicación de parches, actualizaciones y refuerzo de configuraciones, priorizando vulnerabilidades criticas conocidas
    - Escaneo de seguridad antes de reconectar a la red corporativa, integración SIEM o sistemas de monitoreo para detectar anomalías activas.
    - Validación de acceso seguro y controlado a los sistemas restaurados.
b. Retorno a operaciones normales.
    - Pruebas funcionales para confirmar operatividad total
    - Reincorporación gradual de sistemas, con prioridad en servicios críticos.
    - Comunicación interna en cuanto a la reanudación de los servicios
    - Seguimiento a incidencias después del reinicio de operaciones
    - Mejora continua y monitoreo constante sobre los datos y servicios
c. Informe de lecciones aprendidas

Debe incluir:

- Orden cronológico de los hechos, desde la detección, respuesta y recuperación
- Identificación de los puntos vulnerables explotados por Medusa
- Evaluación de la efectividad de los controles técnicos y organizativos aplicados
- Análisis de las decisiones durante la respuesta
- Recomendaciones técnicas y administrativas
- Feedback del personal que estuvo involucrado en el incidente

Incluir este documento en un espacio designado a incidencias, para tener en cuenta en futuros casos

d. Actualización del marco para futuros incidentes.
    - Revisar y mejorar el plan de respuesta a incidentes, al menos de manera anual.
    - Actualizar las políticas de seguridad de la información, respaldos, cifrados y control de accesos, con periodicidad anual.
    - Incluir nuevos escenarios de *ransomware* Medusa en simulaciones, de manera semestral o anual, como parte del protocolo de concientización.
    - Reforzar protocolos de comunicación interna y externa.
    - Capacitaciones constantes y de aprendizaje para futuras incidencias.
e. Seguimiento y monitoreo post recuperación.
    - Monitoreo de logs, y tráfico de red posterior al restablecimiento de operaciones
    - Auditorías internas de seguridad a los sistemas involucrados
    - Supervisión de cumplimiento de medidas correctivas y preventiva

En ataques asociados a *ransomware* Medusa, la fase de recuperación no concluye con la restauración de los sistemas, ya que los datos previamente exfiltrados pueden ser publicados semanas o meses después del incidente.

Para poder llevar un seguimiento, se recomienda la aplicación de 3 controles esenciales, los cuales son: el monitoreo de foros de filtración, revisión de credenciales y el monitoreo de la Dark web, especialmente el blog de Medusa

f. Seguimiento

Esta fase de recuperación debe complementarse con un conjunto de acciones de seguimiento orientadas a reducir el riesgo residual y anticipar posibles filtraciones de información.

En este contexto, resulta recomendable implementar un monitoreo prolongado de foros y sitios de filtración utilizados por grupos de *ransomware,* con el objetivo de detectar oportunamente la posible publicación de datos exfiltrados. Este monitoreo puede incluir la vigilancia de portales asociados a grupos de *ransomware,* espacios de la Dark web y repositorios donde comúnmente se divulga información obtenida en ataques de doble extorsión.

Asimismo, es necesario realizar una revisión exhaustiva de las credenciales potencialmente comprometidas durante el incidente, considerando que los atacantes pueden haber obtenido acceso válido a sistemas internos, correos electrónicos o plataformas corporativas.

Esta revisión debe contemplar la rotación de contraseñas, la revocación de accesos sospechosos y la implementación o fortalecimiento de mecanismos de autenticación multifactor.

Finalmente, el proceso de recuperación debe incluir el reforzamiento de controles de seguridad posteriores al incidente, orientados a reducir la probabilidad de recurrencia del ataque.

Entre estas medidas se encuentran la actualización de políticas de seguridad, la mejora de los mecanismos de detección y monitoreo, la segmentación de redes y la capacitación del personal en prácticas de ciberseguridad. Estas acciones permiten fortalecer la resiliencia organizacional frente a amenazas de *ransomware* avanzado como Medusa, caracterizadas por combinar cifrado de información con estrategias de filtración y presión pública.

7.1.6 Plan de mejora continua

a. Actualización de políticas y procedimientos según nuevas amenazas y versiones de estándares.

La organización debe revisar y actualizar de forma constante sus políticas, lineamientos y procedimientos de seguridad, asegurando que se mantengan alineados con las nuevas versiones de los marcos normativos (ISO 27001:2022, NIST, ITIL) y con las amenazas emergentes, como las nuevas variantes de *ransomware.*

Periodicidad: Revisión semestral o tras incidentes relevantes.

Responsable: Seguridad de la información o comité de ciberseguridad.

b. Auditorias periódicas

Las auditorías permiten verificar el cumplimiento, efectividad y mejora de los controles implementados. Pueden ser internas o externas, según el alcance del SGSI (Sistema de Gestión de Seguridad de la Información).

Periodicidad: Anual o semestral

Responsable: Auditor interno o externo especializado

c. Integración de nuevos controles y tecnologías

Consiste en la adopción de nuevas herramientas, sistemas o medidas de protección que refuercen la detección, prevención y respuesta ante ciberataques.

Periodicidad: Anual según herramientas o amenazas emergentes.

Responsable: Equipo de ciberseguridad y dirección de tecnología

d. Entrenamiento y concientización de colaboradores

La concientización es crucial para reducir el riesgo humano como vector de ataque. El entrenamiento debe enfocarse en la detección temprana de amenazas, el manejo de correos electrónicos sospechosos, el uso seguro de contraseñas y la respuesta ante incidentes.

Periodicidad: trimestral

Responsable: Recursos Humanos y Ciberseguridad.

e. Auditoria de Ciber postura de terceras partes

Evalúa el nivel de seguridad de los proveedores, aliados o contratistas que gestionan o acceden a los sistemas y datos de la organización. Se revisa su cumplimiento de políticas, certificaciones y prácticas seguras.

Periodicidad: Anual

Responsable:

CISO | Comité de Seguridad: se encarga de definir los criterios y los proveedores a evaluar.

Área de Compras | Contratos: incluir cláusulas de seguridad en los convenios.

Auditor externo o interno: ejecutar revisiones técnicas y documentales.

Proveedor evaluado: entregar evidencias, certificados y controles aplicados.

7.1.7 Anexos del marco de gestión de ciberseguridad

La Tabla 7.8 es una matriz de indicadores de gestión de la ciberseguridad que muestra el cumplimiento de los requisitos mínimos y sus métricas correspondientes.

Tabla 7.8 Matriz de indicadores de gestión de ciberseguridad en pymes contra ransomware Medusa

Lineamiento	Evidencia	Métricas
	Prevención:	
Políticas de seguridad de la información	Documento rector Gestión de accesos MFA Uso aceptable de activos Clasificación y manejos de información Seguridad física RRHH Copias de seguridad	Nivel de cumplimiento de políticas de seguridad: Accesos, privilegios, MFA, segmentación de red.

	Protección contra *Malware* Seguridad en las comunicaciones Continuidad y resiliencia	
Gestión de activos críticos	Inventario clasificado en criticidad y sensibilidad	Número de vulnerabilidades críticas identificadas y mitigadas en un período definido.
Concientización y capacitación del personal	Capacitación actualizada y continua	Porcentaje de personal capacitado: Participación y éxito en simulaciones de *phishing* y formación de ciberseguridad.
Gestión de parches y copias de seguridad	Actualizaciones y copias de seguridad	Porcentaje de sistemas con parches al día: Evalúa la reducción de vulnerabilidades explotables.
Controles de accesos	Gestor de contraseñas, gestión de identidades, MFA	Porcentaje de cuentas administradas y con MFA
Segmentación de red	Segmentar con apoyo de firewall	Porcentaje de *endpoints* cubiertos por firewall
Monitoreo continuo	Establecer métricas de monitoreo	
	Detección	
Plan de respuesta a incidentes	Monitoreo continuo, actualización de responsables y actividades, establecer fechas	Nivel de conocimiento entre empleados, sobre plan de respuesta a incidentes
Alertas y herramientas de detección	Definición de umbrales EDR/XDR Detección basada en comportamiento	Número de alertas reales vs. falsas: Evalúa la eficiencia de SIEM, EDR y XDR.
Pruebas y validaciones periódicas	Notificaciones internas Campañas de concientización práctica y teórica	Tiempo medio de detección (MTTD): Desde que ocurre un incidente hasta que se identifica.

		Cobertura de monitoreo: Porcentaje de *endpoints*, servidores y servicios críticos bajo supervisión activa.
	Respuesta	
Procedimientos de aislamiento	Plan de respuesta a incidentes Roles y responsabilidades del equipo de respuesta	Tiempo medio de respuesta (MTTR): Desde la detección hasta la contención efectiva del ataque.
Comunicación interna y externa	Coordinación con autoridades y proveedores	Número de incidentes contenidos sin propagación: Indicador de efectividad de protocolos de aislamiento y contención.
Preservación de evidencias	Registro de eventos, recopilación de evidencias forense	Porcentaje de incidentes manejados según playbooks: Evalúa cumplimiento de protocolos establecidos.
Procedimientos legales y regulatorios	Identificar las políticas actuales, actualizar contratos, NDA, documentación legal.	Porcentaje de actualización sobre los procedimientos legales y regulatorios
	Recuperación	
Restablecimiento seguro de operaciones	Sistemas y datos identificados Documentación de PBC	Tiempo de recuperación de sistemas críticos: Comparado con el RTO definido en el BCP.
		Porcentaje de datos restaurados correctamente: Comparado con el RPO definido.
Seguimiento y monitoreo post recuperación	Informe de lecciones aprendidas Actualización de marco para futuros incidentes	Frecuencia de pruebas exitosas de backups: Evalúa confiabilidad de la infraestructura de recuperación.

Plan de mejora continua		
Actualización	Actualización constante de políticas, procedimientos	Lecciones aprendidas implementadas: Número de ajustes a políticas, procedimientos o configuraciones tras incidentes o simulacros.
Auditorias	Auditorías internas y externas periódicas	Número de incidentes de *ransomware* por periodo: Tendencia a la baja indica eficacia de controles preventivos.
Entrenamiento	Campañas de concientización periódicas generales y especificas al sector de seguridad.	Costos asociados a incidentes: Incluye tiempo, recursos, posibles sanciones y daños reputacionales.

7.1.8 Directorio de contactos clave

En la Tabla 7.9 y la Tabla 7.10, se encuentra el directorio de contactos clave para el proceso antes, durante y después de un ataque de *ransomware* Medusa.

Tabla 7.9 Directorio contactos clave y función, de manera interna

Contacto clave	Función
Responsable de seguridad de la información	Coordinación general del incidente
Administrador de red	Aislar y restaurar sistemas
Encargado de servidores backups	Verificar y recuperar respaldos
Analista de ciberseguridad	Monitoreo, detección y análisis técnico
Soporte técnico	Atención a usuarios afectados, comunicación interna y externa.
Responsable de continuidad de negocio	Garantizar continuidad operativa Revisión normativa

Dirección general	Toma de decisiones, autorización final
Proveedor de nube	Soporte técnico, revisión de logs, restauración
Proveedor de antivirus	Soporte para limpieza y recuperación
Consultoría forense	Preservación de análisis forense

Tabla 7.10 Directorio contactos clave y función, de manera externa

Entidad	Rol/Cuándo contactar	Contacto
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) México	Protección de datos personales (LFPDPPP) Si hay fuga o exposición de datos personales	home.inai.org.mx
Policía Cibernética (Guardia Nacional) México	Investigación y reporte de incidentes delictivos En caso de ataque confirmado o chantaje	088: Al llamar al 088, se brindará asesoría para presentar una denuncia ante el Ministerio Público.
Centros de respuesta ante incidentes informáticos México	Asesoría técnica y coordinación Apoyo en análisis forense Durante y post incidente	https://csirt.com.mx/
Trusted Introducer, TI Directory, ofrece un listado acreditado de equipos de respuesta con detalles actualizados	Directorio completo y actualizado al que se puede acceder para obtener contactos de equipos de respuesta ante incidentes informáticos (CSIRT/CERT).	https://tf-csirt.org/trusted-introducer/directory/teams/

7.1.9 ¿Cómo trabaja Medusa?

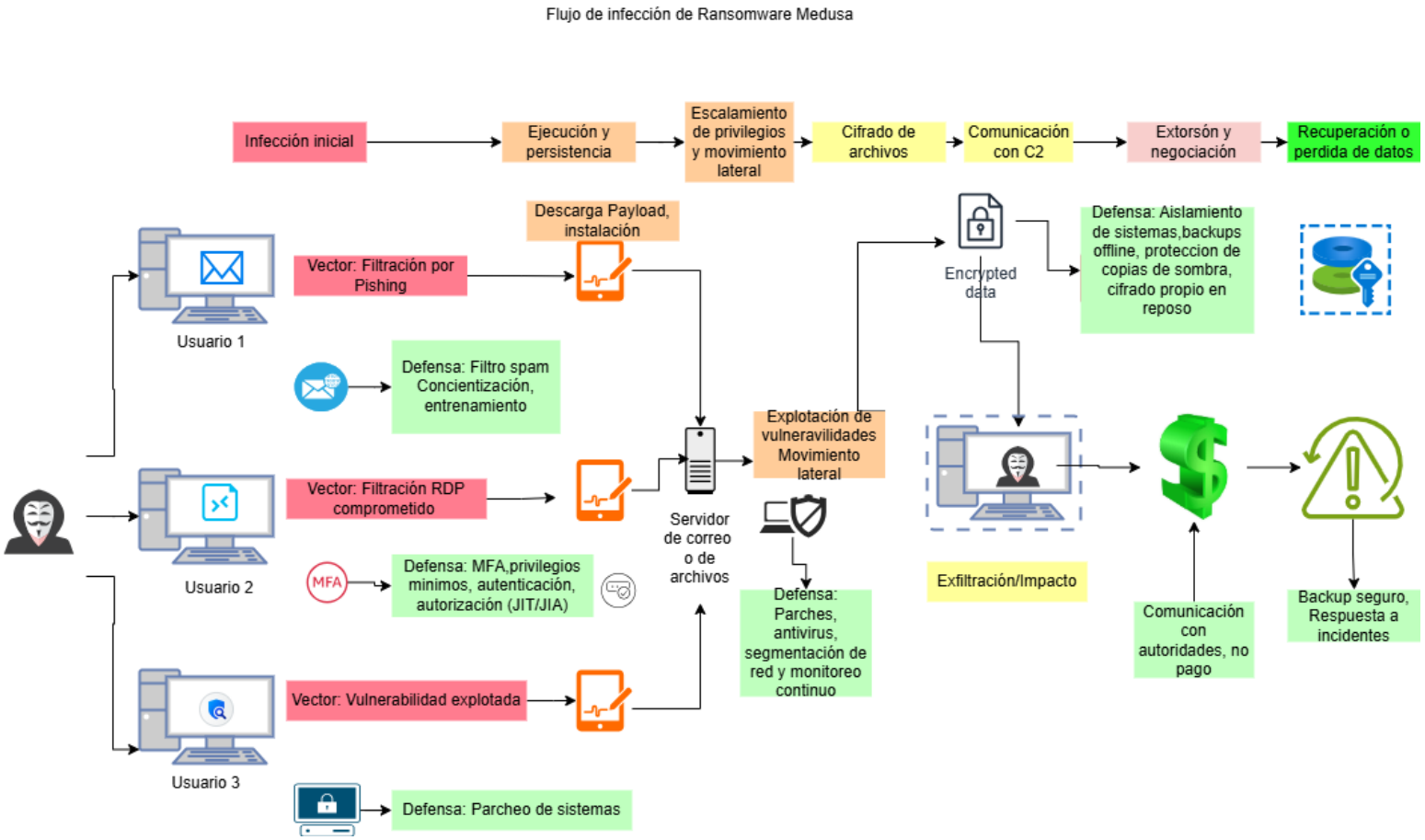

Figura 7.1 Infografía ¿Cómo trabaja Medusa*? Elaboración propia*

7.1.10 Flujograma de procedimientos ¿Qué hacer en caso de un ataque de *Ransomware* Medusa?

Figura 7.2 Infografía ¿Qué hacer ante un ataque de Medusa*? Elaboración propia*

7.2 Caso de estudio

Con el propósito de contextualizar la aplicación práctica del marco administrativo propuesto, a continuación, se presenta un caso de uso que describe la actuación real de una organización ante un ataque de *ransomware* Medusa.

En la Tabla 7.11 se contrastan las acciones que la empresa implementó durante el incidente con las medidas que, de acuerdo con el análisis realizado, podrían haberse implementado para reducir los tiempos de respuesta, minimizar los costos operativos y fortalecer la seguridad en futuros eventos. Esta comparación permite identificar brechas, oportunidades de mejora y la eficacia del protocolo desarrollado.

Tabla 7.11 Caso de estudio

Fase	Empresa afectada	Acción según protocolo propuesto
Infección inicial: Pishing	No había filtro spam, ni concientización con el personal que estuvo en contacto directo en el momento del ataque.	Desarrollar una campaña de entrenamiento a los encargados de TI y empleados generales. Agregar filtro spam, definición de roles, campañas de concientización en ciberseguridad.
Ejecución y persistencia	Ingreso de datos, sin una autenticación previa.	MFA, autorización, autenticación.
Escalamiento de privilegios	Privilegios al máximo, ya que el mismo personal que fue vulnerado, tenía varios roles y permisos, por lo que tenía accesos a los que no le correspondían.	Parcheo de sistemas, privilegios mínimos y solo los necesarios por el tiempo necesario.
Cifrado de archivos	Antivirus sin monitoreo continuo, basado solo en las alertas del mismo software, cifrado de archivos parcial.	Antivirus actualizado, segmentación de red.

Extorsión y negociación	Sin Backups offline, por lo que tardaron en recuperar.	Comunicación con autoridades, respaldos 321
Plan de mejora continua	Se tiene un documento forense, pero no se ha dado seguimiento a concientización y mejora continua.	Respuesta a incidentes, documentación al día, capacitación constante sobre nuevos ataques y formas de prevención.

Para complementar el análisis del caso presentado y establecer una visión estructurada del comportamiento organizacional ante un ataque de ransomware Medusa, se elaboró un diagrama de secuencia que describe las acciones correspondientes a cada rol involucrado.

El diagrama de la Figura 7.31 permite visualizar con precisión las responsabilidades, interacciones y flujos de actuación de acuerdo con el protocolo presentado, facilitando la identificación de áreas de mejora y la definición de procesos más eficientes para la gestión del incidente.

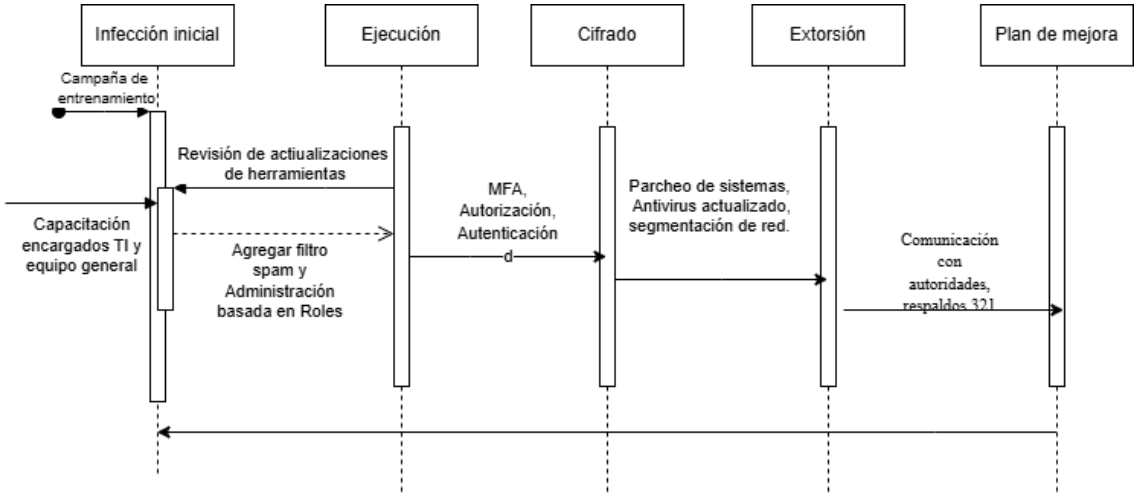

Figura 7.31. Estudio de caso. Elaboración Propia

CONCLUSIONES

El *ransomware* Medusa se ha convertido en un peligro creciente para la operatividad de las pequeñas y medianas empresas. Sin embargo, tras el análisis de la literatura y de los documentos disponibles, así como de los resultados de encuestas dirigidas al sector de tecnología de la información y de entrevistas con expertos en ciberseguridad, se determinó que no existe un protocolo administrativo concreto que ayude a estas empresas a gestionar el riesgo frente a un ataque de Medusa. Esta falta de directrices aumenta las posibilidades de una respuesta lenta, de la pérdida de información y de afectaciones a los procesos esenciales del negocio.

Ante esta realidad, este proyecto propone una arquitectura de gestión de riesgos enfocada en disminuir el impacto operativo del *ransomware* Medusa, proporcionando una solución práctica y en línea con normas internacionales como NIST, ISO/IEC 27001 e ITIL. Esta tiene cuatro fases clave: prevención, detección, respuesta y recuperación con mejora continua, lo que facilita una gestión integral antes, durante y después del incidente.

Se han desarrollado productos prácticos que se presentan en el capítulo 7: un protocolo formal, una matriz de indicadores de gestión de ciberseguridad, un diagrama de flujo para actuar ante un ataque y un mapa del funcionamiento del ransomware Medusa, los cuales ayudan a entender, adoptar y aplicar el marco en organizaciones con diferentes grados de madurez en ciberseguridad.

Los datos recopilados mediante las herramientas de diagnóstico muestran que la mayoría de las pymes no tienen procesos administrativos sólidos para abordar incidentes relacionados con *ransomware;* sin embargo, también indican una alta disposición para establecer directrices claras y procedimientos estandarizados como los aquí presentados.

Además, el desarrollo de este proyecto ha alcanzado sus objetivos, de la siguiente forma:

Cumpliendo con el objetivo número uno, se identificaron los principales vectores de ataque utilizados por el *ransomware* Medusa, confirmando al menos tres métodos críticos de propagación que requieren atención prioritaria: phishing dirigido, archivos adjuntos

maliciosos y robo de credenciales. Esto se realizó mediante la revisión de la literatura, estudios de caso y revisión de incidentes pasados.

En lo referente al segundo objetivo, sobre la propuesta de estrategias clave para prevenir, detectar y mitigar estos incidentes, se realizó mediante un análisis comparativo de las mejores prácticas, entrevistas con expertos y los resultados de encuestas realizadas en el sector de TI, se seleccionaron y justificaron las cinco estrategias clave de gestión de riesgos para la prevención, detección y mitigación de este tipo de amenaza, los cuales se destacan las políticas de copias de seguridad, segmentación de red con herramientas de detección, definición de roles y responsabilidades, integración del modelo Zero Trust, planes de concientización con una clara comunicación interna y externa.

Finalmente, con base en los resultados y el análisis de marcos reconocidos como NIST, ISO 27001 e ITIL, se cumple con el objetivo tres, sobre definir un modelo de respuesta administrativa a incidentes de Medusa, incluyendo las cuatro fases de la ciberseguridad ante un ataque de ransomware, y definiendo un modelo de respuesta a los ataques de *ransomware* Medusa, que abarca las fases de preparación, detección, respuesta y recuperación. Este modelo tiene como propósito mejorar la resiliencia de las pymes frente a Medusa, lo cual se evidenció mediante un caso de uso, aunque la evaluación en un escenario real queda como trabajo para el futuro.

Por lo tanto, se concluye que la arquitectura de gestión creada es relevante, factible y práctica, enfocada en mejorar la resiliencia organizativa y la toma de decisiones en el ámbito de la seguridad de la información ante Medusa, lo que cumple con la meta de ingeniería establecida.

Como limitación del estudio, se reconoce que la muestra utilizada no representa la totalidad del sector empresarial de las pymes, por lo que futuras investigaciones podrían ampliar el alcance para validar el marco en un contexto más amplio.

REFERENCIAS

Amazon Web Services, Inc. (noviembre de 2025). *¿Cuál es la diferencia entre SSL y TLS?* Obtenido de Amazon Web Services, Comparación de soluciones en la nube: https://aws.amazon.com/es/compare/the-difference-between-ssl-and-tls/

American Hospital Association. (14 de marzo de 2025). *Advisory warns of Medusa ransomware activity*. Recuperado el 28 de Abril de 2025, de American Hospital Association Headline: https://www.aha.org/news/headline/2025-03-14-advisory-warns-medusa-ransomware-activity

Baker, K. (20 de febrero de 2025). *5 Types of Ransomware.* Recuperado el 5 de marzo de 2025, de Crowdstrike: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/types-of-ransomware/

Blancaflor, E., Bauson, V. L., Cruz, A. L., & Escandor, M. (31 de enero de 2025). Medusa Ransomware against Data Privacy: A Comprehensive Study of Ransomware Attacks Across Various Organizations and Strategic Recommendations for Future Prevention. *ACM DL*, 28-34. doi:https://doi.org/10.1145/3700706.3700711

Bravo, C. A. (15 de abril de 2025). *Ransomware Medusa: cómo opera y por qué genera preocupación*. Obtenido de welivesecurity: https://www.welivesecurity.com/es/ransomware/medusa-como-opera-america-latina/

Cibersecurity & Infraestructure Security Agency . (12 de marzo de 2025). *StopRansomware: Medusa Ransomware.* Recuperado el 22 de abril de 2025, de Cybersecurity Advisory: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a

Cloudflare. (noviembre de 2025). *¿Qué es la defensa en profundidad? | Seguridad en capas*. Obtenido de Cloudflare Learning: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-defense-in-depth/

Cordova, B. (17 de marzo de 2025). Alertan sobre ataques “ransomware” Medusa en Estados Unidos: Recomendaciones de autoridades para prevenirlos. *2001online.com*. Recuperado el 20 de Marzo de 2025, de https://bit.ly/4svkpgN

CYBLE. (2025). *Medusa Ransomware Hits Record Levels, FBI and CISA Provide Key Security Insights*. Recuperado el 2 de mayo de 2025, de Cyble Trending: https://cyble.com/blog/medusa-ransomware-surges-as-fbi-share-insight

Dubec, M. M. (4 de abril de 2025). Por qué Medusa Ransomware es una amenaza creciente para la infraestructura crítica. *Illumio Cybersecurity*, 3. Recuperado el 8 de abril de 2025, de https://www.illumio.com/es-mx/blog/why-medusa-ransomware-is-a-growing-threat-to-critical-infrastructure

Gitlan, D. (12 de marzo de 2025). *Cifrado Simétrico vs Asimétrico: Explicación de las principales diferencias.* Recuperado el 20 de marzo de 2025, de SSL Dragon: https://www.ssldragon.com/es/blog/cifrado-simetrico-asimetrico/#What-is-Symmetric-Encryption

Gobierno de México. (2025). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* México: Cámara De Diputados Del H. Congreso De La Unión. Obtenido de https://bit.ly/4cK1M3P

Jimenez Huaman, L. Y. (2024). Implementación de un modelo de ciberseguridad basado en las metodologías ISO/IEC 27032 y NIST para la gestión de incidentes cibernéticos en una universidad pública [Tesis de maestría, Universidad Privada del Norte]. *Repositorio de la Universidad Privada del Norte*, 21-23. doi:https://hdl.handle.net/11537/41697

Klappholz, S. (13 de marzo de 2025). *CISA issues warning over Medusa ransomware after 300 victims from critical sectors impacted*. Recuperado el 13 de abril de

2025, de IT PRO: https://www.itpro.com/security/ransomware/medusa-ransomware-cisa-advisory

Lakshmanan, R. (12 de enero de 2024). *Medusa Ransomware on the Rise: From Data Leaks to Multi-Extortion.* Recuperado el 20 de enero de 2025, de thehackernews: https://thehackernews.com/2024/01/medusa-ransomware-on-rise-from-data.html

Microsoft. (2025). *¿Cuál es la diferencia entre IAM y PAM?* Obtenido de Seguridad de Microsoft: https://www.microsoft.com/es-mx/security/business/security-101/what-is-privileged-access-management-pam

Microsoft. (2025). *¿Para qué se usa la detección y respuesta administradas (MDR)?* Obtenido de Seguridad de Microsoft: https://www.microsoft.com/es-mx/security/business/security-101/what-is-mdr-managed-detection-response#:~:text=La%20detecci%C3%B3n%20y%20respuesta%20administradas%20(MDR)%20es%20un%20servicio%20de,la%20respuesta%20r%C3%A1pida%20a%20incidentes

Microsoft. (2025). *¿Qué es una plataforma XDR?* Obtenido de Seguridad de Microsoft: https://www.microsoft.com/es-mx/security/business/security-101/what-is-xdr#:~:text=Mejora%20la%20productividad%20y%20la,para%20actividades%20de%20mayor%20valor.

Microsoft. (2025). *¿Qué es una solución SIEM?* Obtenido de Seguridad de Microsoft: https://www.microsoft.com/es-mx/security/business/security-101/what-is-siem

National Institute of Standards and Technology - NIST. (2024). *Marco de Seguridad Cibernética (CSF) 2.0 / Cybersecurity Framework 2.0.* Gaithersburg, MD, EE. UU: U.S. Department of Commerce. doi:https://doi.org/10.6028/NIST.CSWP.29.spa

NIST Special Publication. (2025). NIST Cybersecurity Framework 2.0. *National Institute of Standards and Technology*, 11. doi:https://doi.org/10.6028/NIST.SP.1308.2pd

Olyniychuk, D. (13 de marzo de 2025). *Detección de Ransomware Medusa: El FBI, CISA y Socios Advierten sobre el Aumento de Ataques por Desarrolladores de Ransomware y Afiliados Contra Infraestructuras Críticas*. Obtenido de SocPrime: https://socprime.com/es/blog/medusa-ransomware-attacks-covered-in-aa25-071a-detection/

One Identity. (2025). *The definition of Endpoint Privilege Management (EPM).* Obtenido de One Identity LLC website: https://www.oneidentity.com/what-is-endpoint-privilege-management/

Paloalto Networks. (10 de enero de 2025). *What is Multi-Extortion Ransomware?* Recuperado el 15 de febrero de 2025, de Palo Alto: https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware

Parvini, S. (15 de marzo de 2025). Cybersecurity officials warn against potentially costly Medusa ransomware attacks. *The Associated Press*, 1. Recuperado el 20 de Marzo de 2025, de https://apnews.com/article/fbi-cisa-gmail-outlook-cyber-security-email-6ed749556967654ff41a629a230973e6

Pérez Castro, J. C. (20 de junio de 2020). Estudio Monográfico Sobre La Amenaza Ransomware, Su Impacto En Las Organizaciones y Buenas Prácticas Para Su Prevención y Manejo. 40-50. Recuperado el 25 de marzo de 2025, de https://repository.unad.edu.co/handle/10596/42143

Ribeiro, A. (13 de marzo de 2025). *Estados Unidos expone la amenaza del ransomware Medusa, con más de 300 organizaciones atacadas en el sector de infraestructura crítica.* Obtenido de industrialcyber: https://industrialcyber.co/cisa/us-exposes-medusa-ransomware-threat-as-over-300-organizations-targeted-across-critical-infrastructure-sector/

Schuster, S. (10 de mayo de 2023). Operación MEDUSA: Los federales cortaron la cabeza de la herramienta de ciberespionaje rusa "Snake", dirigida a empresas y

periodistas estadounidenses. *ProQuest*. Obtenido de https://www.proquest.com/docview/2813774695?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals

ServiceNow. (noviembre de 2025). *¿Qué es la tecnología de la información (TI)?* Obtenido de ServiceNow website: https://www.servicenow.com/es/products/itsm/what-is-information-technology.html

SISA. (10 de marzo de 2025). *Medusa Ransomware Claims 40+ Victims in 2025, Demands Ransoms Up to $15Mn*. Recuperado el 20 de abril de 2025, de Watch, SISA Weekly Threat: https://www.sisainfosec.com/weekly-threat-watch/medusa-ransomware-claims-40-victims-in-2025-demands-ransoms-up-to-15mn

Teichmann, F., & Boticiu, S. (2024). The most impactful ransomware attacks in 2023 and their business implications. *Int. Cybersecur.*, 301-311. doi:https://doi.org/10.1365/s43439-024-00115-3

The MITRE Corporation. (2025). *ATT&CK Matrix for Enterprise*. Obtenido de MITRE ATT&CK: https://attack.mitre.org/

Treviño, A., Cutler, A., & Guccione, D. (2 de abril de 2025). *¿En qué consiste la extorsión cibernética?* Recuperado el 5 de abril de 2025, de Keeper: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/types-of-ransomware/

8 ANEXOS

8.1 Anexo: Encuestas a público general que labora en sector TI

A continuación, se presenta el formato establecido para las encuestas al público del sector de TI, que consta de 22 preguntas, desglosadas en secciones según las fases de la ciberseguridad.

También se incluyen imágenes representativas de las entrevistas realizadas a los expertos en ciberseguridad. No se presentan de manera íntegra los datos personales ni la totalidad de las respuestas, debido a que, conforme a la legislación vigente en materia de protección de datos personales, es obligatorio resguardar la información que pueda identificar a los participantes.

8.2 Anexo: Entrevista Experto 1

Entrevista a experto en ciberseguridad: Protocolo ante ransomware Medusa

Fecha y hora de entrevista: 6 de agosto 2025 5:00 pm **Medio:** Virtual

Cargo o puesto actual: IT Security Analyst

Años de experiencia en TI / Ciberseguridad: 3 años

Área de especialización: Análisis de vulnerabilidades

Certificaciones: CCST Cybersecurity, CCST Networking, AWS Cloud Practicioner, ICS2 CC.

8.3 Anexo: Entrevista Experto 2

Entrevista a experto en ciberseguridad: Protocolo ante ransomware Medusa

Fecha y hora de entrevista: 27 Julio 2025 **Medio:** Virtual

Cargo o puesto actual: Global Cybersecurity Delivery Manager

Años de experiencia en TI / Ciberseguridad: 15

Área de especialización: Ciberseguridad

Certificaciones: CEH, CISM, NSE,1,2,3,4,7, PCNSE, ISO27001, Diplomando en Ciberseguridad Estrategica

8.4 Anexo: Entrevista Experto 3

Entrevista a experto en ciberseguridad: Protocolo ante ransomware Medusa

Fecha y hora de entrevista: 15 agosto 2025 9:30am **Medio:** Virtual

Cargo o puesto actual: Cybersecurity Engineering Leader LATAM & The Caribbean

Años de experiencia en TI / Ciberseguridad: 26 años de experiencia

Área de especialización: Seguridad de la información, gestión de riesgos y continuidad

Certificaciones: CCIE, Security OPS, CCNP Security, CISM, ISO 27001 Lead Implementer entre otras.

8.5 Anexo: Entrevista Experto 4

Entrevista a experto en ciberseguridad: Protocolo ante ransomware Medusa

Fecha y hora de entrevista: 20 de agosto 2025 10:00am **Medio:** Virtual

Cargo o puesto actual: Consultor Infraestructura y ciberseguridad

Años de experiencia en TI / Ciberseguridad: 8

Área de especialización: Ciberseguridad Fortinet

Certificaciones:

Fortinet Certified Solution Specialist Network Security

Fortinet Network Security 7.4 Support Engineer

Fortinet Enterprise Firewall 7.4 Administrator

OT Security Sales Training

Fortinet Certified Professional Network Security

Fortinet NSE 6 - FortiSwitch 7.2

Fortinet FortiGate 7.4 Administrator

Trellix Endpoint Security | Technical Specialist

Glosario de acrónimos

AES: Advanced Encryption Standard (Estándar de Cifrado Avanzado)

BYOVD: Bring Your Own Vulnerable Driver (Trae Tu Propio Controlador Vulnerable)

CISA: Cybersecurity and Infrastructure Security Agency (Agencia de Ciberseguridad e Infraestructura de Estados Unidos)

DES: Data Encryption Standard (Estándar de Cifrado de Datos)

DNS: Domain Name System (Sistema de Nombres de Dominio)

EDR: Endpoint Detection and Response (Detección y Respuesta de Puntos Finales.)

EPM: Endpoint Privilege Management (Gestion de privilegios de endpoints.)

FBI: Federal Bureau of Investigation (Oficina Federal de Investigación)

GDPR: General Data Protection Regulation (Reglamento General de Protección de Datos)

IAM: Identity and Access Management (Gestión de Identidades y Accesos)

ICMP: Internet Control Message Protocol (Protocolo de Control de Mensajes de Internet)

ISO: International Organization for Standardization (Organización Internacional de Normalización)

MDR: Managed Detection and Response (Detección y Respuesta Gestionadas)

MS-ISAC: Multi-State Information Sharing and Analysis Center (Centro de Análisis y Compartición de Información Multiestatal)

MSSP: Managed Security Service Provider (Proveedor de Servicios de Seguridad Gestionados)

MXDR: Managed Extended Detection and Response (Detección y Respuesta Extendida Gestionadas)

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)

PAM: Privileged Access Management. (Gestión de Cuentas Privilegiadas)

RaaS: *Ransomware* as a Service (*Ransomware* como Servicio)

RMF: Risk Management Framework (Marco de Gestión de Riesgos)

SIEM: Security Information and Event Management (Gestión de Información y Eventos de Seguridad)

SSL/TLS: Secure Sockets Layer / Transport Layer Security (Protocolos de Seguridad de la Capa de Transporte)

TI: Tecnologías de la Información

XDR: Extended, Detection and Response (Detección y Respuesta Extendidas)