ESTRATEGIAS DE PROTECCIÓN Y BUENAS PRÁCTICAS CONTRA ATAQUES DE RANSOMWARE

JOSÉ MIGUEL SÁNCHEZ DÍAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2023

ESTRATEGIAS DE PROTECCIÓN Y BUENAS PRÁCTICAS CONTRA ATAQUES DE RANSOMWARE

JOSÉ MIGUEL SÁNCHEZ DÍAZ

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

KATERINE MARCELES VILLALBA
Directora

DANIEL FELIPE PALOMO
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 18 de junio de 2023

DEDICATORIA

Primero y ante todo Al que está sentado en el trono de Honor y Gloria durante toda la eternidad, el dueño y dador de la vida que sin su amor y su disciplina no hubiera alcanzado jamás el gusto por la sabiduría y el conocimiento, a mi esposa e hija que sacrificaron muchos buenos momentos en familia, por permitirme alcanzar esta preciada meta, a mi madre que con su consejo y admiración me motivó a continuar por el buen camino y dio los mejores días de su vida para educarme y hacerme útil a la sociedad.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE ILUSTRACIONES

pág.

GLOSARIO

ATAQUE CIBERNÉTICO: Constituye un daño causado a través de las redes de internet, basado en la implantación de *malware* que afecta a personas del común, empresas y a la infraestructura crítica de un país, con el objetivo de robar, secuestrar o destruir información, causando con ello daños graves a sus víctimas.

BITCOIN: Moneda virtual creada para ser utilizada en transacciones relacionadas con el entorno virtual, este es el tipo de pago más utilizado por delincuentes informáticos.

CIBERDELINCUENTES: Personas con conocimientos en informática, en todo nivel, que han logrado dejar al descubierto las vulnerabilidades de las redes y negocios que se realizan en internet, atacan todo tipo de hardware y software con vulnerabilidades, es difícil el control de este tipo de personas debido a herramientas de la red que los hace anónimos ante las autoridades.

MALWARE: Código malicioso ejecutado por el usuario o víctima que no tiene en cuenta protocolos de seguridad en la inspección de archivos, sobre todo aquellos que son poco conocidos o sospechosos. Aprovecha además vulnerabilidades de los sistemas operativos o software desactualizados o ilegales para abrirse una puerta para obtener información

RANSOMWARE: Malware diseñado para impedir el libre acceso a la información de la víctima o a su equipo informático, introducido a través de correos electrónicos fraudulentos utilizando técnicas de ingeniería social, que, al ser ejecutados, descarga el código malicioso que se encarga de encriptar y codificar todo tipo de archivos.

RESUMEN

Con la aparición de la pandemia SARS-CoV-2, la mayoría de las actividades humanas se vieron obligadas a refugiarse en la tecnología, único factor que les permitió llevar a cabo todas las acciones productivas y comunicativas. Desde el comercio hasta situaciones tan elementales como las consultas médicas pasaron a formar parte de plataformas virtuales, con el fin de preservar la vida y la salud de los funcionarios y trabajadores en todo el mundo.

Pero ello trajo una consecuencia consigo, el aumento de ataques cibernéticos y de los delitos informáticos en todo el mundo. Colombia no fue la excepción, con el aumento de manera exponencial de los delitos informáticos, ha causado pérdidas a diferentes sectores de la economía. Por tal motivo, este estudio se enfoca en la marcada tendencia que generó el ransomware, uno de los fraudes típicos y con mayor auge en las empresas colombianas, dado que, por la inobservancia de ciertos factores de riesgo, muchas personas aún caen en la trampa de los correos electrónicos malintencionados, que al ser abiertos descargan un malware, causando un secuestro de la información.

Por consiguiente, esta propuesta estableció parámetros de seguridad que dan una solución efectiva, sin costos elevados, preservando la integridad y la seguridad de la información, en cualquier escenario en el mundo. Este análisis se realizó en una empresa en particular, con el objetivo de ser aplicable en otras empresas en auge y con pocos recursos, que quieran utilizar estos métodos y estrategias para aumentar la seguridad informática y cerrar cada vez más la brecha a los ciberdelincuentes, que aprovechan a usuarios de tecnologías de información con bajos conocimientos en herramientas digitales.

Palabras claves: Malware, Ransomware, Amenaza, Ciberdelincuentes, Vulnerabilidades.

ABSTRACT

With the appearance of the SARS-CoV-2 pandemic, most human activities were forced to take refuge in technology, the only factor that allowed them to carry out all productive and communicative actions. From commerce to situations as elementary as medical consultations, they became part of virtual platforms, in order to preserve the life and health of officials and workers around the world.

But this brought a consequence with it, the increase in cyber-attacks and computer crimes throughout the world. Colombia was not the one, exponentially increasing all computer crimes, except causing losses to different sectors of the economy. For this reason, this study focuses on the marked trend that ransomware generated, one of the typical frauds and with the greatest boom in Colombian companies, since, due to the non-observance of certain risk factors, many people still fall into the trap of Malicious emails, which when opened download malware, causing information hijacking.

Therefore, this proposal established security parameters that provide an effective solution, without high costs, to this problem, preserving the integrity and security of the information, in any scenario in the world. This analysis was carried out in a particular company, with the aim of being applicable to other booming companies with few resources, who want to use these methods and strategies to increase computer security and increasingly close the gap to cybercriminals, who They take advantage of information technology users with little knowledge of digital tools.

Keywords: Malware, Ransomware, Threat, Cybercriminals, Vulnerabilities.

INTRODUCCIÓN

Las diferentes crisis en la humanidad son responsables de grandes cambios. Las guerras son generadoras de inventos que posteriormente sirven de manera excepcional a las comunidades, las crisis entre las que se cuentan las enfermedades también hacen parte de la evolución tecnológica y sanitaria de la humanidad. Actualmente el mundo está viviendo un cambio a raíz de una pandemia inesperada que fue altamente contagiosa, afectando el trabajo en sociedad que realizan muchas personas, en especial para aquellas que requieren el contacto social para el intercambio ya sea de tipo: comercial, adquisición de productos y otro tipo de necesidades inherentes al ser humano.

Esta pandemia conocida por todos abrió un mundo de nuevas expectativas, donde jugó un rol bastante importante el uso de las herramientas digitales, aunque ya estaban en uso, eran poco empleadas, por causa de costumbres como asistir de forma presencial a las organizaciones o sitios de trabajo de las personas; pero actualmente se han convertido en imprescindibles, debido a que las autoridades sanitarias a nivel mundial recomendaron aislamiento físico con el fin de evitar y disminuir contagios y con ello la muerte, trayendo consigo una nueva tendencia de uso de las herramientas tecnológicas, ofimáticas y el comercio virtual.

Por este motivo, muchas personas optaron por trasladar sus oficinas, a sus lugares de residencia, esta situación aumentó las vulnerabilidades en los sistemas informáticos, por el uso de elementos tecnológicos sin ningún tipo mecanismo de protección, como por ejemplo: antivirus, firewall o protocolos de seguridad informática que pudieran disminuir los ataques remotos, dejando al descubierto una gran cantidad de información por ciberdelincuentes, que aprovecharon la oportunidad para aumentar sus ganancias ilícitas explotando las brechas de seguridad de los entornos informáticos.

Esta investigación aborda uno de los problemas con mayor porcentaje de riesgo corporativo y personal de secuestro de información a cambio de dinero o bitcoins, el **ransomware.** Este malware posee la capacidad de ser altamente perjudicial y de fácil instalación, incluso ha mutado en diferentes versiones, muchas de ellas se actualizan diariamente por editores de código asociados a estas prácticas, causando problemas aún para las empresas de software antivirus y para la comunidad en general que aún no ha hallado una solución concreta a este mal, afectando las redes informáticas a nivel global.

Por consiguiente, la educación y la capacitación de buenas prácticas organizacionales en el uso de la información y de los sistemas informáticos se ha convertido en una prioridad para las empresas, las implementación de planes de mejoramiento, del sistema de gestión de seguridad de la información y la realización de auditorías para encontrar vulnerabilidades, técnicas que deben estar en la agenda de los gobiernos empresariales con el fin de evitar cuantiosas pérdidas por el secuestro de la información (ransomware) u otras modalidades de crimen cibernético.

Por esta razón, esta investigación se enfoca en identificar métodos que permitan hacer frente a esta amenaza, puesto que el ransomware es uno de los malware con mayor avance en los ambientes tecnológicos, en su mayoría empresariales, esto a causa del manejo de correos electrónicos infectados, que aparentan contener información importante con algún beneficio para el lector, o técnicas de ingeniería social basados en el engaño con cuentas de cobro falsas, como multas de tránsito u otros aspectos afectando directamente a usuarios, funcionarios de entidades y todo tipo de personas que utilizan el correo electrónico como herramienta para recibir o enviar mensajes de notificación. Como consecuencia, los daños ocasionados, además de generar pérdidas económicas, interrumpe la ejecución de actividades relacionadas con el uso de computador o máquina infectada, esto si se ha guardado una copia de seguridad que sea factible recuperar cuando la requiera

el usuario, por el contrario si no se cuenta con esa solución, es posible perder la información, el funcionamiento normal de las funciones de las máquinas infectadas e incluso ser utilizado como plataforma de lanzamiento de ataques por parte de los ciberdelincuentes dependiendo la clase de ransomware que infecte el dispositivo.

En este último caso, si el ataque es impulsado desde un correo empresarial o institucional, puede causar daños irreversibles al buen nombre de la empresa. Con todo eso, las pérdidas pueden ser millonarias, sin contar con el pago de la liberación del equipo infectado, se convierte entonces en una cifra considerable de pérdidas. De tal manera que, este documento permitirá establecer diferentes estrategias de tipo preventivo, mitigando el alto impacto de esta amenaza, generando con ello una cultura de buenas prácticas digitales, poniendo en práctica cada una de las actuaciones propuestas en el desarrollo de la actividad.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La gran cantidad de usos que tiene un computador y los dispositivos móviles, representan para muchas personas parte de su eficiencia en lo que se refiere al aspecto laboral. Actualmente muchas personas realizan sus trabajos y controlan negocios a través de plataformas digitales por diferentes motivos; pero la causa principal que ha llevado a muchas personas y sociedades a la adopción de este tipo de métodos fue la pandemia registrada a finales del año 2019 (SARS-CoV-2), sumado a ello, las actividades personales como reuniones y transacciones comerciales tuvieron un aumento exponencial debido al aislamiento que se presentó en diferentes partes del mundo, como norma preventiva en contra del contagio.

Sin embargo, esta enorme complejidad con el uso de diferentes aplicaciones y enorme cantidad de datos estableció un nuevo reto en lo que se refiere a la seguridad informática, dado que los sistemas de seguridad que tienen los computadores personales y otros dispositivos son frágiles y en algunos casos inexistentes, en comparación a los sistemas de seguridad que implementaron las empresas en sus instalaciones para hacer frente a las amenazas cibernéticas.

“Los vectores utilizados por los cibercriminales apuntan generalmente al envío de correos electrónicos masivos, con llamativos y alarmantes asuntos que consiguen en un porcentaje muy alto que las víctimas ejecuten los enlaces incluidos en los mensajes que notifican”[1]. Por lo tanto, este texto contiene las formas de ataque más comunes en Colombia por ransomware; a través del cual se ha logrado demostrar las vulnerabilidades de los sistemas informáticos de las empresas sobre todo

[1] POLICIA DE COLOMBIA, [Sitio web]: Colombia. Tendencias cibercrimen Colombia 2020 p. 20. Disponible en: https://caivirtual.policia.gov.co/contenido/tendencias-cibercrimen-colombia-2019-2020

aquellas que están forjadas recientemente y no cuentan con el presupuesto para implementar un sistema de gestión de seguridad de la información en sus áreas.

La organización analizada no ha sido víctima del ransomware desde inicio de sus actividades, en lo que se refiere a seguridad informática, debido a las políticas establecidas desde el departamento de las Tecnologías de la Información quien tiene la responsabilidad de llevar a cabo estrategias que minimicen los impactos de un posible ataque cibernético, relacionado con todo tipo de malware o virus informático, ocupando un lugar importante en los procesos de la entidad y con un seguimiento especial por parte de la alta gerencia. No obstante, debido al constante nombramiento de funcionarios y/o trabajadores a las instalaciones, la seguridad informática se encuentra en constante ataque, puesto que muchos no aplican los conceptos de las capacitaciones realizadas, tomando con ligereza algunos aspectos básicos como, descarga de archivos adjuntos o ejecutando archivos de dudosa procedencia que incluso tienen editores desconocidos, poniendo en riesgo el componente informático de la entidad y a su vez la información de clientes, trabajadores y usuarios de los servicios de la organización.

Lo cierto es que, el malware ocasionaría otro daño de grandes proporciones, como el bloqueo de uno o varios equipos informáticos de trabajo, causando la suspensión de los servicios por falta de herramientas tecnológicas que permitan la prestación normal de las actividades y servicios a sus clientes y usuarios.

Una de las acciones del ransomware es cifrar los archivos, dejando los datos almacenados inservibles, por lo tanto, sin esta información, la empresa sufriría grandes atrasos en sus procesos puesto que, cada área de la entidad maneja procedimientos claros, con ítems y productos que deben ser aplicados en un tiempo establecido por el usuario, causando pérdida de confianza y credibilidad, al no ejecutar sus labores de manera eficiente.

1.2 FORMULACIÓN DEL PROBLEMA

El ransomware es uno de los ataques cibernéticos que ha cobrado mayor fuerza en Colombia, debido a la pandemia del COVID 19, muchos sectores económicos y productivos, incluso entidades del estado y otras organizaciones, han optado por utilizar de manera concurrente las plataformas tecnológicas, con el fin de cumplir los protocolos de bioseguridad establecidos por las autoridades sanitarias.

Esto más allá de convertirse en una solución para las empresas, se convirtió en un problema sobre todo en el aspecto informático, debido a que los funcionarios tuvieron que migrar con su trabajo de oficinas a sus casas, bajo la figura del trabajo en casa; convirtiéndose en la oportunidad perfecta para los ciberdelincuentes que, aprovechando las vulnerabilidades de los equipos informáticos personales de los trabajadores, que en su mayoría no cumplen con la arquitectura básica de seguridad, estas pequeñas empresas, según estadísticas de la Policía Nacional de Colombia [2] fueron las principales afectadas con este tipo de ataques.

En lo que se refiere a la organización objeto de análisis, muchos procesos como el mantenimiento de hardware, software y otros relacionados con los servicios de la entidad, tuvieron una transformación en cuanto a la manipulación de la máquina se refiere, debido a su alta demanda con referencia a soporte y mantenimiento de computadores en su mayoría portátiles, circulaba mucha información de tipo confidencial, como archivos, claves de usuario, videos e información financiera y personal de sus clientes. Esto causó un riesgo importante, que consistía en conectar este tipo de equipos de cómputo a la red privada de la entidad, como estos podrían estar infectados e iniciar un contagio a través de la red o en su defecto utilizar la red como medio para enviar de manera automática, correos infectados con ransomware.

[2] Ibid., p. 15.

Afortunadamente se encontró todo tipo de malware en diferentes equipos, pero no se identificó ataques con ransomware. En contraste con el trabajo realizado, se implementó soluciones antivirus de marcas reconocidas y con altos privilegios, además firewall de última generación basados en software, que protegieron los equipos informáticos de los usuarios después del mantenimiento realizado.

Debido a lo anterior, surge la siguiente pregunta problema:

¿Cómo serían los métodos de protección que debería contemplar la organización objeto de análisis frente a un ataque de Ransomware?

2 JUSTIFICACIÓN

Uno de los principales métodos de mitigación de esta problemática es el uso adecuado del correo electrónico, herramienta indispensable para realizar todo tipo de trámites administrativos, que posee un grado de credibilidad superior a los de otras redes sociales y canales de comunicación, puesto que está vinculado directamente con los componentes gerenciales de la empresa y mantienen un soporte o acuse de recibo al emisor, así como al receptor o destinatario. Pero esta herramienta se ha convertido en una puerta a los ataques de la ciberdelincuencia, los cuales buscan llamar la atención de los usuarios con técnicas de ingeniería social, para vulnerar la información, con la instalación de software malicioso que hurta o secuestra la información, exigiendo a la víctima dinero a cambio de recuperar sus datos. Este tipo de actos han causado pérdidas a nivel mundial onerosas, además muchas empresas prefieren no informar este tipo de situaciones para evitar tener mala reputación con sus clientes, disminuyendo la denuncia y perpetuando el negocio, dado que las autoridades desconocen las fuentes de los ataques cibernéticos.

Por ello es importante realizar acciones tempranas, con el fin de detectar todos los vacíos que existen en la organización y realizar acciones preventivas en contra del ransomware, esto minimizará los riesgos, evitando pérdida de información, de dinero y sobre todo de la reputación que es la base de la credibilidad de los clientes en cuanto al manejo responsable de su información.

De manera que, se ha optado como medio preventivo y a la vez disuasivo, utilizar cuentas de correo electrónico y páginas de servicios web corporativos y contratados, desde plataformas que ofrezcan capas de seguridad la configuración como el bloqueo de remitentes desconocidos o con mala reputación, desarrollando un sistema de seguridad con que optimice los procesos y minimice lo riesgos relacionados con ataques informáticos.

Finalmente, el propósito de esta investigación es encontrar los vectores de infección y ataque del malware, debido a que su forma de propagación es cada vez más rápida y se vale de la ignorancia digital de muchos funcionarios para ejecutar los ataques. Por lo tanto, es importante establecer cada uno de los métodos de contagio, similar a una infección en el cuerpo humano, mientras más rápido se conozcan los factores que propagan la enfermedad, será más ágil su curación. Así actúan también las redes informáticas, encontrando hoy en día la solución de muchos ataques con ransomware de forma ágil en páginas web [3], se publica de manera gratuita y sencilla la solución y se evita continuar con la cadena de propagación de este código malicioso, puesto que ya no cuentan con métodos para realizar la extorsión por el secuestro de la información, por lo tanto, el negocio deja su rentabilidad.

De igual forma se busca generar una cultura de seguridad informática en los funcionarios de la entidad, con alternativas publicitarias como banners, pantallas en los pasillos de la corporación con información que se refieran al uso adecuado de las herramientas digitales y estrategias como publicación de videos que logren concientizar a los funcionarios de los peligros que se encuentran actualmente en red. Con ello y con el empleo constante de estos métodos, se generarán hábitos y posteriormente la preservación de la seguridad de la información de la empresa.

[3] NO-MORE-RANSOMWARE. [Sitio web]. USA: La batalla contra el ransomware. Disponible en: https://www.nomoreransom.org/es/index.html

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar estrategias y buenas prácticas para garantizar la seguridad de la información contra ransomware mediante un entorno controlado.

3.2 OBJETIVOS ESPECÍFICOS

- Examinar los sistemas de protección ante ataques de ransomware que tiene la organización objeto de análisis, mediante la caracterización de cada uno de ellos con el fin de identificar con qué herramientas cuenta para enfrentar este tipo de incidentes.

- Establecer el diseño de un escenario controlado simulando la arquitectura tecnológica de la organización objeto de análisis, con el fin de hacer pruebas de al menos 2 muestras de tipos de ransomware haciendo uso de los vectores de ataques más utilizados para su propagación y de esa manera identificar qué tan robustos son los mecanismos de defensa con que cuenta la empresa.

- Proponer estrategias de protección y buenas prácticas que permitan ofrecer garantías seguridad de la información a la organización objeto de análisis, a partir de los resultados obtenidos al aplicar pruebas sobre el escenario controlado.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Impacto por infección de ransomware en las organizaciones: Los diferentes ataques causados por ransomware, se han convertido en uno de los problemas más comunes a los que se enfrentan las pequeñas y medianas empresas en la actualidad. Las cifras son difíciles de cuantificar, debido a su crecimiento, sobre todo en lo que se refiere al comercio electrónico; no obstante, con base en informes de empresas de años anteriores, es posible deducir el impacto que tiene este malware en la sociedad.

La investigación está centrada en organizaciones pequeñas y medianas, en su mayoría las empresas que están empezando en el mundo comercial, consideran que son inmunes a ataques por ciberdelincuentes. Este concepto ha convertido este tipo de organizaciones en un blanco llamativo para una posible estafa y ha representado un incremento del 78% [4] de ataques, esto demuestra la capacidad y desarrollo en cuanto a ingeniería social se refiere por parte de los atacantes, además el negocio del software ha representado ganancias significativas para delincuentes aprendices, o aquellos que han tomado este delito como emprendimiento, debido que los ataques actuales son simples y se realizan con bajo conocimiento de herramientas digitales.

Respecto al cifrado de datos en las organizaciones, hubo un aumento en ataques a los archivos del 65%, esta cifra es el doble de las reportadas en los años 2020 y 2021, con un leve incremento en 2021, comparado con las cifras de años anteriores.

[4] DEN, EN, et al [Sitio web]. Informe De Amenaza Cibernética De Sonicwall. 2021.p. 31. Disponible en: https://www.sonicwall.com/es-mx/2022-cyber-threat-report/

Esto es una clara señal del aumento de los ataques, siendo proporcional a la adquisición de ganancias [5] ilegales por los atacantes, no obstante, redujo la cifra de extorsión por este delito en 3%, puesto que sus datos no fueron cifrados, pero existió un tipo de solicitud de dinero a cambio de evitar publicar información confidencial.

La afectación de las organizaciones a nivel regional, se evidencia claramente en el aumento de ataques, debido al entorno digital y la baja o nula calidad de sistemas de seguridad de la información en las empresas, en cifras las organizaciones reportaron intento de ataques por ransomware del 57%[6], otras organizaciones identificaron diferentes vectores y más peligrosos que los anteriores en un porcentaje del 59%, además aumentó el ataque de ciertos sectores como el comercial y aquellos que se relacionan con redes sociales (que cuentan con información empresarial como teléfonos, direcciones de correo o cuentas de mensajería instantánea sincrónica) se apreciaron un aumento del 72% de estos ataques.

Con el avance de este malware, también han aumentado las soluciones, incluso se ha forjado una comunidad digital en contra del ransomware, que ha deshabilitado por completo el efecto de algunos daños causados por esta amenaza. Este tipo de comunidades y de expertos se encuentran en sitios web como *no more ransomware*[7]; además, que estas soluciones sencillas son frecuentemente utilizadas por personas que han sufrido ataques, o que después de ser atacadas, sus secuelas se convirtieron en defensa contra diferentes ataques, la mayoría de las empresas que fueron afectadas por el ransomware, prácticamente el 99% lograron revocar sus datos cifrados, gracias a expertos en TI, comunidades, blogs y otro tipo de ayudas que se encuentran en internet.

---

[5] Óp. Cit, p. 33.
[6] GUTIÉRREZ, Dayro, et al. [Sitio web]. Amenazas cibernéticas y su impacto en las organizaciones del sector industrial y servicios de Colombia en la última década.2022. p. 41. Disponible en: https://repository.unad.edu.co/handle/10596/31937
[7] Óp. Cit.

En segundo lugar, un método que restaura todos los datos, de manera segura, sin necesidad de pagar rescates o ciberseguros, son las copias de seguridad, en el 73% [8]de las organizaciones que reportaron ser afectados por ransomware, más de la mitad de las empresas optaron por utilizar sus copias de seguridad, que a pesar de las implicaciones de tiempo y lo que tarda la recuperación del sistema, lograron volver a sus actividades días después del colapso causado por el malware.

Cabe subrayar que, el optar por el pago del rescate, no es sinónimo de recuperar los datos completamente. Muchos afectados que pagaron el rescate solamente recuperaron algo más de la mitad de la información, en un bajo porcentaje se evidencia la recuperación de la totalidad de la información, siendo entonces las copias de seguridad un método eficiente para restaurar la información.

4.1.2 Medios de infección de ransomware: Es conveniente analizar los ataques que representan mayor riesgo para las organizaciones, siendo estos la mayor fuente de financiación para los atacantes, utilizaran todo tipo de métodos para implantar el malware y dar valor a su ataque[9].

4.1.3 Vulnerabilidades en los equipos: A causa de las vulnerabilidades que los atacantes encuentran en los equipos o servidor, es posible llevar a cabo una infección exitosa, para ello utilizan herramientas desarrolladas para escanear los equipos, con el fin de lograr introducir el malware[10].

[8] NARVÁEZ, Folker, et al. [Sitio web]. Revisión del estado del arte en técnicas para prevención y detección temprana de Ransomware. p 28 Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/26932/2/resumen%20analitico%20en%20educacion%20rae%20-%20folker%20narvaez.pdf

[9] SGANDURRA, Daniele, et al. [Sitio Web]. Análisis Dinámico Automatizado de Ransomware. p.12. Disponible en: https://arxiv.org/pdf/1609.03020

[10] CASTRO, Martha Irene, et al. Introducción a la seguridad informática y el análisis de vulnerabilidades. p. 30.

4.1.3.1 Vulnerabilidades por actualizaciones: Es conveniente aplicar métodos a través de expertos en TI, con el fin de evitar este tipo de vulnerabilidades, estas acciones son evitadas o ignoradas por personal que no cuenta con conocimiento respecto a los riesgos del malware. Evidencia de ello es, suponer que un dispositivo o sistema informático no requiere un mantenimiento adecuado, en efecto, esto es aprovechado por los ciberdelincuentes al notar que los equipos carecen de seguridad, instalando diferentes tipos de malware.

4.1.3.2 Redes domóticas: Los dispositivos y redes domóticas se han convertido en una brecha explotada por los criminales, debido a sus escasos y deficientes métodos de seguridad, falta de cifrado de sus dispositivos y claves débiles o genéricas. Para hacer frente a este riesgo, si la organización utiliza elementos domóticos, es conveniente segmentar la red, colocando estos elementos en (DMZ) apartados de la red principal e instalando otros dispositivos o métodos de barrera que alerten, bloqueen y disminuyan los riesgos de estos dispositivos.

4.1.3.3 Políticas de seguridad informática: Es necesario establecer políticas de actualización de contraseñas, uso de contraseñas alfanuméricas y en lo posible con símbolos. Estas contraseñas establecen una barrera sólida para los atacantes, evitando su ingreso con el uso de software que descubren contraseñas inseguras como nombres o cadenas de números predecibles. Otra política relacionada con las contraseñas es no reutilizar o reciclar contraseñas, o compartir usuarios con otros equipos, esto ocasiona que la contraseña sea susceptible a ser descifrada y usada de forma fraudulenta, brindando acceso a privilegios no otorgados a usuarios no autorizados.[11]

[11] MAIMÓ, Lorenzo Fernández. Detección de botnets y ransomware en redes de datos mediante técnicas de aprendizaje automático. p. 4. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=289541

4.1.3.4 Correos fraudulentos o Spam: Al hablar de correos falsos, se refiere a aquellos que se asimilan a personas u organizaciones reconocidas, que cambian una letra o incluso parte de la dirección del correo original, para engañar al receptor, quien al verificar su procedencia abre el archivo adjunto, el cual suele estar infectado con malware y es instalado en la máquina objetivo, a veces sin ser detectado por el usuario. De igual forma se utilizan redes sociales o algunas aplicaciones de mensajería para compartir estos archivos infectados y vulnerar la seguridad del sistema.

4.1.3.5 Direccionamiento a sitios web inseguros. Mensajes que advierten un tipo de sanción de tránsito o requerimientos judiciales a los correos o aplicaciones de mensajería del dispositivo de la víctima, incluyendo los SMS, son utilizados como estrategia para insertar una URL que redirecciona al usuario a sitios web, al ingresar a estos lugares inseguros se descarga diferentes tipos de malware que aprovecha las brechas de seguridad de la máquina objetivo e implanta ransomware. Además, estos sitios web inseguros tienen la capacidad de infectar los dispositivos con adware y código que se instala sin necesidad que el usuario lo autorice.

4.1.4 Estadísticas de infección por ransomware en Colombia. La amenaza y los ataques realizados por ransomware en Colombia crecen día a día. La falta de educación digital unida a la ignorancia de muchos funcionarios de diferentes áreas de múltiples empresas ha llevado al colapso de plataformas de CSIRT a nivel mundial. Los delincuentes no satisfechos con extraer la información privada y confidencial también encriptan los archivos de la víctima, o en algunos casos bloquean el acceso a la máquina que contiene dichos archivos, enviando mensajes de extorsión a los afectados, para obtener ganancias extorsivas.

Sin embargo, si la víctima no accede a los requerimientos extorsivos, el criminal amenaza con publicar parte de la información confidencial en bases de datos públicas o venderla al mejor postor, causando desprestigio en caso de que sea información organizacional, debido a factores como la confidencialidad y reserva de la información o en el peor de los casos al ser información personal, la divulgación de fotos, imágenes privadas, archivos de cuentas bancarias y otra información privada.

Esta es una clara amenaza que muchos ignoran, debido a factores como la desinformación o la falta de interés en lo que se refiere al cuidado de la información organizacional. Es fundamental realizar capacitaciones para dar a conocer estos riesgos que afectan a todo tipo de organizaciones, en diferentes niveles. Colombia ha sido afectado en varias ocasiones por el ransomware, en entidades públicas y privadas causando pérdidas millonarias. Los datos analizados fueron extraídos de los reportes de amenazas por Sonicwall, una de las entidades más importantes en cuanto a seguridad informática se refiere en Estados Unidos, comprometida con el análisis constante de los diferentes vectores del ransomware a nivel mundial, que a su vez realiza investigaciones con agencias a nivel mundial de lucha contra el malware, que se asocian para establecer una lucha frontal contra el malware. En Colombia los ataques por ransomware han aumentado un 18% en lo corrido del año 2022, cifra preocupante si se suma a las de los años anteriores (2021 y 2020) donde se estaba superando las dificultades subyacentes generadas por efectos de la pandemia.[12]De igual forma, fueron detectados 11 millones de amenazas, ataques perpetrados en varias organizaciones, convirtiendo a Colombia en uno de los países con mayores niveles de riesgo en cuanto a ataques informáticos se refiere a nivel global.

[12] POLICIA DE COLOMBIA, [Sitio web]: Colombia. Tendencias cibercrimen Colombia 2020 p. 20. Disponible en: https://caivirtual.policia.gov.co/contenido/tendencias-cibercrimen-colombia-2019-2020

4.1.5 Tipos de ataques causado por ransomware: El secuestro digital de datos es considerado una de las conductas que más ha generado daños a los empresarios en Colombia en los últimos años, pues el ransomware se ha convertido en un negocio altamente lucrativo. Actualmente esta actividad está siendo desarrollada por el crimen organizado o delincuentes independientes convirtiéndola en una empresa delincuencial con muchos actores involucrados que en efecto son anónimos, razón por la cual actúan con libertad. Así como la tecnología basada en internet contribuye al desarrollo de la economía mundial, también se ha convertido en un lienzo en blanco para los ciberdelincuentes cada vez más organizados. Cuando este tipo de ataques se materializan los atacantes usan criptografía que tienden a ser exponencialmente seguras, donde se infiere que, deberán usar técnicas forenses para recuperar la información y aun así no se garantiza que los datos sean reintegrados en su totalidad. El ransomware aprovecha vulnerabilidades del software de cualquier sistema operativo o aplicación, algunos ataques lo realizan a servidores web desactualizados, sistemas conectados a internet, impresoras de red, equipos médicos entre otros que no cuentan con suficientes métodos de protección que disminuyan las amenazas.

Los ciberdelincuentes utilizan técnicas que pretenden obtener cuentas con privilegios de administrador usando *phishing*, ingeniería social, por medio del spam enviando un correo electrónico falso con enlaces web maliciosos o adjuntos con ficheros comprimidos como .rar o .zip que capten la atención del usuario que lo descargue y ejecute un programa maligno sin saberlo. En cuanto al vector de ataque Locky conviene destacar que se dedica a infectar equipos hospitalarios o el ransomware de dispositivos móviles que afectan principalmente a los Android.[13]

[13] INCIBE [Sitio web]. Ransomware: una guía de aproximación para el empresario. p. 7. Disponible en: https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

4.2 MARCO CONCEPTUAL

4.2.1 Confidencialidad: Método que conserva la información que no es de carácter público, a mantener su reserva por los funcionarios que tienen relación a causa de sus labores, quienes deben ocultar dicha información y mantenerla en secreto, siendo la ley quien determina a quién debe ser compartida, por canales seguros y que cumplan ciertas normas de seguridad.

4.2.2 Integridad: Consiste en mantener la información completa lejos de modificaciones o cambios que destruyan su origen. Su principal objetivo es evitar que se modifique arbitrariamente, cambiando su significado o en el peor de los casos, para el fin con la que fue creada. En caso de delitos informáticos, es preciso añadir que se debe preservar todos los datos obtenidos, en vista que pone en duda la credibilidad de aquellos que la trasmiten.

4.2.3 Disponibilidad: Se refiere a tener la información dispuesta para aquellos integrantes de la organización que están autorizados y que requieren acceso a ella, en su mayoría para la toma de decisiones adecuadas en el ámbito administrativo y corporativo.

4.2.4 Políticas de seguridad: Son todas las buenas prácticas y procedimientos de la seguridad de la información que permiten mantener un ambiente seguro con todos los integrantes de la organización, basado en buenos comportamientos y uso adecuado de la información.

4.2.5 Estándares de seguridad: Son modelos a seguir en lo que se refiere a la seguridad de la información. Por ello es conveniente determinar parámetros de seguridad que promuevan y prevengan daños causados por malas prácticas.

4.2.6 Riesgo: Es la probabilidad de ser atacado por una amenaza inminente, basada en una vulnerabilidad que no haya sido detectada, causando daños a la información, pérdida de credibilidad y posibles sanciones de tipo administrativo y penal, debido al manejo de información confidencial. Se debe contar con métodos de prevención basados en políticas de seguridad que disminuyan el riesgo de ataque.

4.2.7 Vulnerabilidad: Falta o carencia de sistemas de seguridad, software antivirus y elementos que proporcionen alertas. Se define también como vacíos o brechas utilizadas por el atacante con el fin de extraer información de manera ilegal con fines ilícitos o con fines extorsivos.

4.2.8 Ataque: Intento organizado e intencionado para buscar y encontrar vulnerabilidades o debilidades en sistema informático o de redes. Cuando se logra el ataque se afectan los pilares de la información, en todas sus etapas debido a que los datos están controlados por los atacantes y pueden ser modificados, añadidos o eliminados de manera aleatoria.

4.2.9 Amenaza: Todo elemento o acción capaz de atentar contra la seguridad de la información. Situación que se puede presentar si los objetivos de los atacantes se llevan a cabo, debido a no contar con buenas prácticas de seguridad informática.

4.2.10 Ransomware*:* Es un malware que impide el acceso, además, secuestra o amenaza con destruir la información e induce a la víctima a pagar para recuperar sus datos.

4.2.11 Clases de Ransomware*:* pueden afectar las acciones del equipo o servidor: En primer lugar y el más utilizado para realizar secuestro de información es el **ransomware de bloqueo,** el cual se encarga de bloquear por completo cualquier función del dispositivo hasta que no se reciba dinero por un rescate. En segundo lugar, el **ransomware de cifrado,** el cual es más destructivo y peligroso, debido a su impacto en archivos individuales o carpetas del sistema, convirtiendo los archivos en otro formato.

4.3 MARCO LEGAL

Aspectos generales en cuanto a la legislación de delitos informáticos en Colombia: En el mundo cibernético al igual que en el mundo real, existen infinidad de delincuentes, estafadores, pedófilos, traficantes de drogas, ladrones y todo tipo de delincuencia incluso organizada. La violación contra los pilares de la seguridad de la información configura los delitos informáticos, por tal razón en Colombia se legisla a favor de quienes son víctimas, teniendo en cuenta que se considera que la información hace parte de la intimidad y preservar su confidencialidad un derecho fundamental establecido en el artículo 15 de la Constitución Política de Colombia debe tener una especial protección.[14]

[14] SECRETARIA SENADO. [Sitio web]. Colombia: Constitución Política de 1991. Disponible en: http://www.secretariasenado.gov.co/constitucion-politica

Este tipo de acciones se relacionan con interceptación de información, utilización ilegítima de un sistema informático, utilización de software malicioso, hurto por plataformas tecnológicas y delitos semejantes, incluso aún no descritos. Los primeros antecedentes normativos se establecen en ley 527 de 1999 que enmarca la regulación y el uso de los datos, comercio electrónico y firmas digitales, posteriormente en la ley 1266 de 2008 se establece la regulación del *habeas data* y uso de la información de datos personales. En el año 2009 se modifica el código penal donde se crea un nuevo bien jurídico o una nueva categoría de delito, con la puesta en vigencia de la ley 1273 de 2009 "de la protección de la información y de los datos" con ocho artículos desde el 296A al 296J. Dicho de otra manera, la ley 1273 de 2009 es una herramienta efectiva para enfrentar de manera contundente los delitos informáticos y los delitos conexos, esta ley además se compensa con acuerdos internacionales que brindan recursos informáticos mediante el convenio de "Cibercriminalidad".

4.3.1 Delitos comunes relacionados con la ley 1273 de 2009[15]: En relación con el delito que se enmarca en el **Artículo 269A Acceso abusivo a un sistema informático,** cualquier persona natural o jurídica puede ser víctima de ese acceso abusivo comprometiendo pilares de la seguridad de la información como la confidencialidad, quienes se dedican a flanquear la seguridad tienen técnicas como el *trashing* cuya acción permite obtener y recolectar información de archivos borrados, además de la ingeniería social donde se manipula un usuario legitimo para obtener información confidencial como claves y datos**.**

En la conducta enmarcada en el **Artículo 269B Obstaculización ilegitima de sistema informático o red de telecomunicación** los delincuentes cibernéticos usan malware que tienen la facultad de reproducirse y trasmitirse de forma automática, generado fallas en el software conocido como virus, otros ataques como

[15]Ibid. Ley 1273 de 2009.

la bomba lógica con código malicioso, son insertados en una red informática para ordenar ciertas acciones como enviar correos no deseados, realizar transacciones, dañar o eliminar archivos comprometiendo la disponibilidad de la información. El web spoofing es un claro ejemplo de un ataque que vulnera pilares de la seguridad de la información como la confidencialidad y eventualmente la disponibilidad tiene como objetivo suplantar una página web real para realizar una acción fraudulenta capturando datos y claves o enviar correos electrónicos falsos de entidades de banco o entidades oficiales solicitando actualizar datos o cambio de contraseñas. Este delito se encuentra tipificado en el **Artículo 269B Interceptación de datos informáticos.**

Otro delito muy común es dañar, modificar o cambiar sin autorización datos de un software o documentos de tipo electrónico**,** en este caso el ciberdelincuente puede verse involucrado en seis conductas descritas en el **Artículo 269D, Daño informático** donde en efecto, vulnera la integridad y disponibilidad de la información. Muchos compran, venden, distribuyen o adquieren software malicioso en las calles, para ahorrar dinero en la compra de software legal, tal vez ignoran que esto también es un delito por superficial que parezca y se refleja **en el Artículo 269E.**

El Artículo 269F Violación de datos personales se complementa con la ley 1581 de 2012, la más frecuente es el hackeo a cuentas de Facebook y correos electrónicos se vulnera Integridad y confidencialidad de la información**.**

Artículo 269G: Suplantación de sitios web para capturar datos personales: Utiliza una conducta como el grooming o ciberacoso sexual para ejercer un control sobre las victimas con los datos adquiridos y va encausado a cometer delitos como la pornografía infantil.

Artículo 269H Circunstancias de agravación punitiva: Aumenta la pena cuando alguno de los delitos ya tipificados se produce en un sistema informático o redes de comunicación estatales, de sector financiero ya sea nacional o extranjero, aprovechamiento de la confianza en un proveedor, revelar información en perjuicio de otro, con fines terroristas, utilizando a terceros de buena fe. Otros apartados enmarcados en esta ley se relacionan **Artículo 269I** Hurtos por medio informáticos y semejantes y el **Artículo 269J** Transferencia no consentida de activo que hace referencia cuando ciberdelincuente vulnera confidencialidad, integridad y disponibilidad de la información, por ejemplo, un ataque **BEC** (*Business Email Compromise*) son sofisticadas estafas dirigidas a las personas desde direcciones de email. Toda conducta enmarcada en la Ley 1273 de 2009 se considera delito informático, atentados informáticos y otras infracciones, el desconocimiento de la ley no exime de responsabilidad, por tal razón las empresas deben implementar políticas para la protección de información y además, capacitar a los funcionarios sobre todo aquellos funcionarios que en el ejercicio de sus funciones, distribuyan publiquen o destruyan de manera ilegal, información sensible o de tipo confidencial para la entidad la que pertenecen, aun cuando pertenezcan a entidades privadas o públicas.

4.3.3 Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales":[16]

La ley de protección de datos personales tiene como objeto el desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos. La ley será aplicada a cualquier base de datos que lo haga susceptibles a tratamiento de datos en todo el territorio colombiano por entidades públicas o privadas o por normas internacionales también llamada *Habeas data*.

[16] Ibid. Ley estatutaria 1581 de 2012.

4.3.4 Decreto 1377 de 2013 "Por el cual se reglamenta parcialmente la ley 1581 de 2012":[17] La protección de datos es un derecho del siglo XXI, el objeto de este decreto es reglamentar parcialmente la ley 1581 de 2012, donde se dictan disposiciones generales para la protección de datos personales. En el articulado se establece el tratamiento de datos en el ámbito personal o doméstico, recolección de datos personales, autorización para el tratamiento de datos y limitaciones.

[17] FUNCION PUBLICA. [Sitio web]. COLOMBIA: Decreto 1377 de 2013. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

5 DISEÑO METODOLÓGICO

5.1 ENFOQUE METODOLÓGICO.

Para este proyecto fue necesario aplicar el desarrollo por fases de gestión, dado que los delitos informáticos y en particular el ransomware es constante y repetible, incluso contiene diferentes tipos de ataques comprobados, que mutan a través del tiempo, por causa de los controles y herramientas que logran identificarlos para combatirlos. Este enfoque metodológico consistirá en la aplicación de los objetivos específicos en fases, puesto que el desarrollo de cada fase permitirá el avance a otro escenario del proyecto dando como resultado el alcance de cada objetivo planteado al inicio de la propuesta.

Es necesario establecer a través de este enfoque, factores de aspecto empírico, que no solo proviene de la teoría, sino también de la práctica, dando a entender con ello que la construcción de la metodología sistematiza y explica diferentes tipos de ataques, incluso aquellos que no se conocen, debido a la proliferación de código malicioso que es creado o modificado cada minuto en el mundo.

Fase I: Sistemas de protección ante ataques de ransomware que tiene actualmente la organización objeto de análisis, mediante la caracterización de cada uno de ellos con el fin de identificar con qué herramientas cuenta para enfrentar este tipo de incidentes.

En esta fase se establecerá un proceso para cumplir minuciosamente un método preciso para aumentar los sistemas de seguridad, mediante las siguientes etapas:

- Descubrimiento de vulnerabilidades de la topología actual.
- Descripción de los sistemas de protección ante ataques cibernéticos.

Cada una de estas etapas permitirán llevar a cabo un análisis de las condiciones actuales de la topología de red, que permitirán evidenciar las falencias de los sistemas de seguridad, herramientas tipo software para contrarrestar posibles ataques a la infraestructura corporativa, así como las brechas existentes en puertos y protocolos de los equipos informáticos.

Fase 2: Diseño de un escenario controlado simulando la arquitectura tecnológica de la organización objeto de análisis, con el fin de hacer pruebas de al menos 2 muestras de tipos de ransomware haciendo uso de los vectores de ataques más utilizados para su propagación y de esa manera identificar qué tan robustos son los mecanismos de defensa con que cuenta la empresa.

Esta fase representa gran importancia debido a su similitud con posibles ataques externos que se realizan por delincuentes informáticos. Estos dos vectores demostraron al cuerpo directivo y colaboradores la manera en que el ransomware ataca a sus víctimas, si no llevan a cabo protocolos de prevención de ataques cibernéticos; con técnicas de ingeniería social y la infiltración a la red por falta de sistemas de seguridad robustos, se realizó un ataque controlado, que convirtió algunos archivos útiles en material cifrado, destruyendo la integridad de la información corporativa y con ello los procesos que se realizan a través de esta información. Cuenta con las siguientes etapas para llevar a cabo el proceso:

- Caracterización y selección de tipos de ransomware.
- Tipos de ransomware utilizados para efectuar ataques controlados.
- Demostración del escenario controlado para ataques de ransomware.
- Tipos de vectores de ataque.
- Ingeniería social y sus fases.
- Propuesta de la nueva tipología de red.
- Estrategias y herramientas para mitigar ataques de ransomware.
- Aplicación de herramientas de pentesting.

Fase 3: Estrategias de protección y buenas prácticas que permitan ofrecer garantías de seguridad de la información a la organización objeto de análisis, a partir de los resultados obtenidos al aplicar pruebas sobre el escenario controlado.

En esta fase final, se realizan recomendaciones de tipo preventivo que representan un porcentaje significativo para evitar ataques cibernéticos. Por tanto, es necesario que el usuario final adquiera el conocimiento necesario para evitar que, por medio de sus acciones en la web, pueda poner en riesgo la seguridad de la información de la organización. Estas serán las etapas que permitirán a la organización cumplir con este logro de prevención y capacitación:

- Integración de protocolos de seguridad informática basados en la norma ISO/IEC 27035.
- Aplicación estrategias, medidas preventivas y buenas prácticas en el uso de las herramientas ofimáticas comunes.
- Protocolo en caso de ataque inminente.
- Políticas de ciberseguridad de la organización.

6 DESARROLLO DE LAS FASES DEL PROYECTO

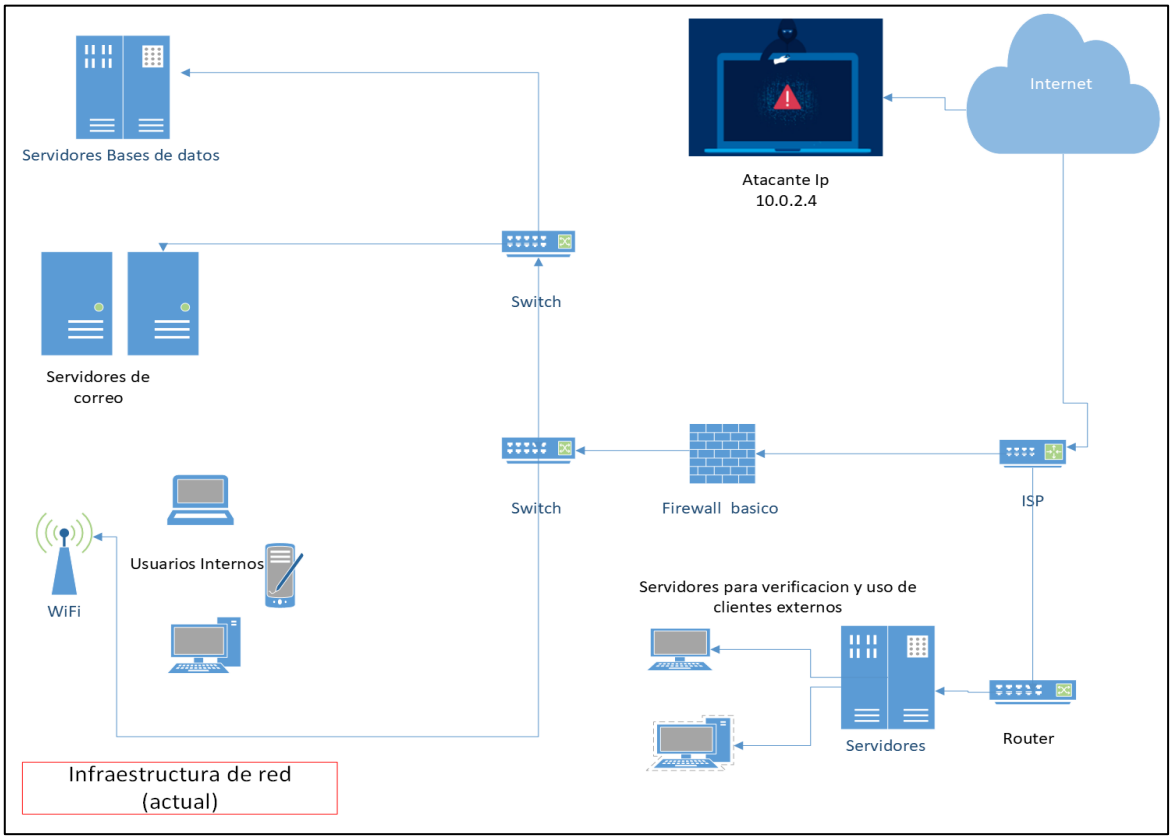
6.1 DESARROLLO DE LA FASE 1: SISTEMAS DE PROTECCIÓN ANTE ATAQUES DE RANSOMWARE QUE TIENE ACTUALMENTE LA ORGANIZACIÓN OBJETO DE ANÁLISIS, MEDIANTE LA CARACTERIZACIÓN DE CADA UNO DE ELLOS CON EL FIN DE IDENTIFICAR CON QUÉ HERRAMIENTAS CUENTA PARA ENFRENTAR ESTE TIPO DE INCIDENTES.

6.1.1 Sistemas de protección ante ataques de ransomware que tiene la organización objeto de análisis: La organización se ha propuesto a partir de este objetivo, estandarizar métodos con el fin de identificar vulnerabilidades en el componente informático de la entidad. A través del equipo de TI encargado de la seguridad informática, se ha dispuesto de personal especializado de ingenieros y técnicos para llevar a cabo métodos para el descubrimiento de vulnerabilidades.

Para empezar a descubrir las vulnerabilidades y falencias que pueden existir en la topología de red actual, fue necesario indagar con el Director general, quien es el encargado del equipo de las tecnologías de la información, para dar a conocer la estructura de la red, y como está compuesta, así como los elementos de hardware que tiene la empresa hoy en día para hacer frente ante una posible amenaza digital. Por tal motivo, el director de proyectos de la organización objeto de análisis, permitió el acceso a un archivo deteriorado de los planos de una tipología de red.

En la figura 1, según el análisis de la topología, no cumple con los requisitos mínimos de seguridad, por el contrario, es vulnerable ante cualquier ataque debido a la falta de segmentación de la red y por no acceder a dispositivos y herramientas que, pueden representar un avance significativo en la protección de los datos.

Ilustración 1. Topología de red actual.



Fuente: Elaboración propia

6.1.2 Descripción de las herramientas actuales de protección ante ataques cibernéticos: Basado en la gráfica, existen componentes importantes de seguridad, como un **firewall** en la entrada/salida de la red de internet **ISP**, que proporciona una barrera a algunos ataques cibernéticos que puedan surgir, además un software antivirus que a pesar de ser una licencia de pago, es básico en cuanto a su arquitectura se refiere, el cual no es visible en la gráfica debido a que es en esencia un componente lógico, convirtiéndose en un entorno exageradamente recursivo, siendo esta una falencia para el activo primordial de la red que es la información.

El cambio de red o su ampliación es indispensable para optimizar el intercambio de paquetes y de información, esta modificación además de rentable resulta ser innovadora, porque al igual que muchas organizaciones, esta entidad tiende al crecimiento y cada día aumenta sus usuarios, conexiones y requerimientos de tipo empresarial, por lo cual debe ir a la vanguardia de este tipo de mejoras con el objetivo de no ser presa fácil para la competencia.

Logro obtenido: Este análisis, tanto de la topología de red, como de los dispositivos que existen actualmente como método de protección ante ataques cibernéticos, permitió extraer la información suficiente para implementar medidas para mejorar tanto la red y su infraestructura, como aquellos dispositivos que no cumplen de manera efectiva, con la protección de la información de los elementos como computadores, servidores y otros, que pueden afectar la productividad de la empresa en caso de ataque cibernético.

6.2 DESARROLLO DE LA FASE 2: DISEÑO DE UN ESCENARIO CONTROLADO SIMULANDO LA ARQUITECTURA TECNOLÓGICA DE LA ORGANIZACIÓN OBJETO DE ANÁLISIS, CON EL FIN DE HACER PRUEBAS DE AL MENOS 2 MUESTRAS DE TIPOS DE RANSOMWARE HACIENDO USO DE LOS VECTORES DE ATAQUES MÁS UTILIZADOS PARA SU PROPAGACIÓN Y DE ESA MANERA IDENTIFICAR QUÉ TAN ROBUSTOS SON LOS MECANISMOS DE DEFENSA CON QUE CUENTA LA EMPRESA.

6.2.1 Caracterización y selección de tipos de ransomware: En los últimos años, con el avance de aplicaciones y dispositivos en el mercado, ha aumentado el uso del internet, por lo tanto, ha crecido de forma proporcional las vulnerabilidades.

La Tabla 1. Contiene la caracterización de los ataques más frecuentes en Latinoamérica y particularmente en Colombia. Dos de estos malware ***Wanna Cry y Cerber*** fueron utilizados en el escenario controlado de infección de la organización en análisis, además se explican las cepas ***Locky, CryptoLocker y Ryuk***, debido a los constantes ataques realizados en la región.

Tabla 1. Caracterización de ransomware.

Nombre	Resultado del ataque	Propagación	Recomendación
Locky	Utiliza engaños e ingeniería social a víctimas incautas y con pocos conocimientos de riesgos informáticos, para descargar archivos con este malware, el cual cifra los archivos de manera individual convirtiéndolos a la extensión Locky. posteriormente la víctima recibe notificaciones en el dispositivo para pagar el rescate de la información.	Este tipo de malware se propaga por medio de correos electrónicos, a través de un archivo adjunto infectado.	Desconecte el equipo de la red para evitar mayor propagación. Para algunos tipos de este malware, existen soluciones gratuitas en internet que pueden desencriptar la información.

Fuente: KASPERSKY, [Sitio web] Ciberseguridad que siempre está un paso por delante. 2022. Disponible en: https://www.kaspersky.es/

Tabla 1. (continuación)

Nombre	Resultado del ataque	Propagación	Recomendación
Wanna Cry	Ataca por medio del cifrado de archivos, del tipo ransomware de bloqueo. Se estima que las organizaciones que no actualizan de forma periódica los sistemas operativos Windows están expuestos a este ataque a través de exploit.	Basado en vulnerabilidades del sistema operativo Windows. Actualmente existen parches distribuidos a través de las actualizaciones del sistema operativo, con las cuales se puede evitar la entrada del malware.	Es necesario realizar actualizaciones contantes al sistema operativo y en todo caso, realizar copias de seguridad externas, cuando fallen los sistemas de seguridad o muten los vectores de este malware.
Crypto Locker	Para lograr ingresar al equipo, los delincuentes usan métodos como el correo electrónico, utilizando falsas ofertas y la ingeniería social como su principal arma. Este malware como la mayoría del ransomware Convencional.	Este tipo de malware se propaga por medio de correos electrónicos, a través de un archivo adjunto infectado, el cual descarga otros	Desconecte el equipo de la red para evitar mayor propagación. Para un método de desinfección existen dos formas que son efectivas.

Fuente: KASPERSKY, [Sitio web] Ciberseguridad que siempre está un paso por delante. 2022. Disponible en: https://www.kaspersky.es/

Tabla 1. (continuación)

Nombre	Resultado del ataque	Propagación	Recomendación
	Utiliza la técnica de cifrado, en archivos del sistema operativo Windows. Cuando el equipo está infectado después de un proceso de incubación el ciberdelincuente exige una suma de dinero. Posteriormente con el método conocido como cifrado asimétrico, el cual consiste en dos claves asociadas, una para cifrar y otra para descifrar, son utilizadas por el atacante para recuperar archivos después que la víctima accede a pagar la extorsión, para recuperar sus datos.	troyanos de diferentes tipos que se encargan de infectar el sistema de forma discreta, luego que está completamente incubado se procede a notificar la víctima con mensajes en la pantalla del dispositivo.	La primera consiste en instalar un software antivirus con la función de eliminar este tipo de malware del sistema. La segunda utilizar herramientas de descifrado en línea gratuitas de organizaciones que prestan este servicio a nivel mundial. No obstante, no se podrán descifrar algunos archivos debido a que algunos cifrados son irreversibles.

Fuente: KASPERSKY, [Sitio web] Ciberseguridad que siempre está un paso por delante. 2022. Disponible en: https://www.kaspersky.es/

Tabla 1. (continuación)

Nombre	Resultado del ataque	Propagación	Recomendación
Ryuk	Malware utilizado para el ataque de infraestructuras críticas u objetivos de alto valor, como entidades de nivel internacional. Se puede propagar con o sin intervención humana, lo que lo convierte en una cepa peligrosa. El ataque se ejecuta después que el delincuente realiza un análisis a la entidad para determinar su alto valor.	A través de correos electrónicos, envía mensajes fraudulentos llamativos que, al descargar el adjunto, liberan un grupo de malware troyano, los cuales permiten tomar el control del equipo por el atacante, quien después ejecuta el ransomware al obtener privilegios en el sistema. Además, está comprobado, filtran información de los funcionarios para enviar mensajes de spam.	Este ataque cifra los archivos, cuando la víctima no accede a pagar, es muy difícil recuperar datos. Por ello es importante realizar copias de seguridad y actualizarlas constantemente, de igual forma mejorar la seguridad en la topología de red con elementos de seguridad físicos y lógicos, para proteger el servidor.

Fuente: KASPERSKY, [Sitio web] Ciberseguridad que siempre está un paso por delante. 2022. Disponible en: https://www.kaspersky.es/

Tabla 1. (continuación)

Nombre	Resultado del ataque	Propagación	Recomendación
Cerber	Este tipo de malware tiene el mismo modo de propagación que los anteriores. Lo que lo hace esta cepa diferente es que funciona como un software de negocios, como SaaS o software de servicios. Este enfoque permite "alquilar" el malware y obtienen ganancias tanto el usuario, como quien ofrece el servicio.	Por medio de correos electrónicos con archivos infectados, phishing o sitios web que descargan automáticamente malware.	Reiniciar el equipo y desconectarlo de la red, posteriormente activar la función de búsqueda de malware en el software antivirus y este eliminará todo lo concerniente al malware.

Fuente: KASPERSKY, [Sitio web] Ciberseguridad que siempre está un paso por delante. 2022. Disponible en: https://www.kaspersky.es/

La infraestructura local es vulnerable al estar en conexión a internet y la convierte en una superficie de ataque digital, cuyo objetivo se centra en identificar las contraseñas débiles o sin el nivel de seguridad suficiente, con nombres o números fácilmente predecibles, con el fin de acceder al sistema bajo ataque sin la autorización del usuario, para dispersar *malware* o robar información. Al igual que los firewall o protocolos mal configurados permiten los ataques de intercambio o *man-in-the-middle*[18]

[18] ESET, [Sitio web] Qué es un ataque de *Man-in-the-Middle* y cómo funciona. 2022. Disponible en: https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/

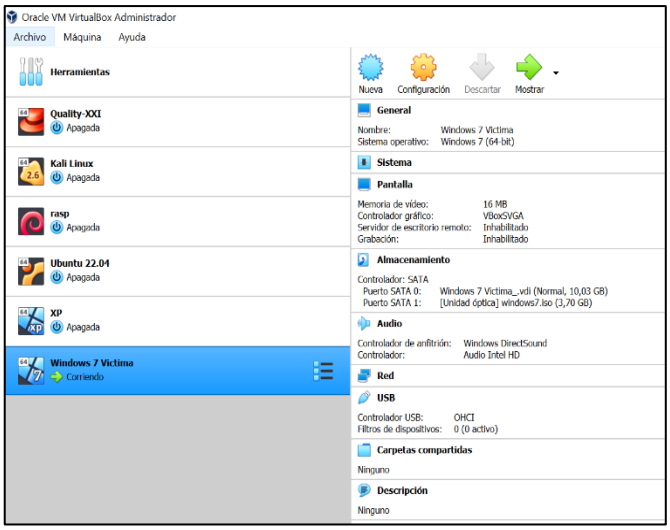
6.2.2 Tipos de ransomware utilizados: Para efectuar ataques controlados en la arquitectura de red, se utilizó el malware WannaCry de la clase **Trojan.Ransom*.Win 32.Wanna,*** debido a sus múltiples usos en diferentes ataques a corporaciones y entidades de Latinoamérica. Este malware además funciona a través del método SaaS, Software como servicio y ha sido identificado por diferentes autoridades que investigan estos ilícitos en sur América.

También se llevará a cabo un ataque en entornos controlados con el tipo malware Cerber, Trojan.Ransom***.Win 32.Blocker***, este malware también puede aplicarse bajo la modalidad de SaaS, su método de infección es diferente debido a que inicialmente instala un troyano, el cual se encarga de infectar todo el sistema y adquirir privilegios en el sistema y posteriormente, instala el malware con ransomware. Para cuando la víctima sea notificada, el malware ya habrá recopilado información y obtenido privilegios y con ello efectua un ataque contundente, en caso que la víctima no acceda a ser extorsionada para recuperar la información. [19]

6.2.3 Escenario controlado para ataques de ransomware: Para realizar el escenario controlado de ataque con ransomware, se utilizó una máquina virtual (Virtual Box) con el sistema operativo Windows 7, desactualizado y sin ningún tipo de software antivirus, para demostrar al gobierno corporativo la facilidad de ingreso de esta manera a la red de la entidad, además con base en estas pruebas, se realizaron capacitaciones a los funcionarios de la entidad, debido a que el ransomware utiliza técnicas de ingeniería social y engaño, para atacar el usuario final.

[19]KASPERSKY, [Sitio web] Amenazas 2022. Disponible en: https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Wanna/

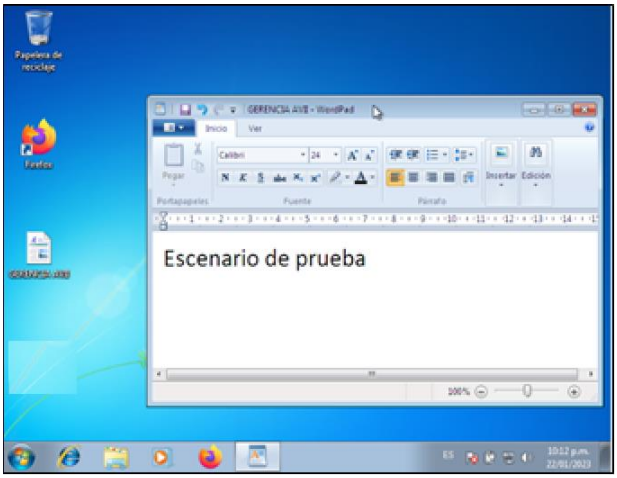
Ilustración 2. arquitectura del sistema operativo en la máquina virtual



Fuente: Elaboración propia

En la ilustración 2 y 3 es posible verificar el funcionamiento adecuado del sistema operativo y se apertura el documento, el cual demuestra que se puede editar sin problema por el usuario.

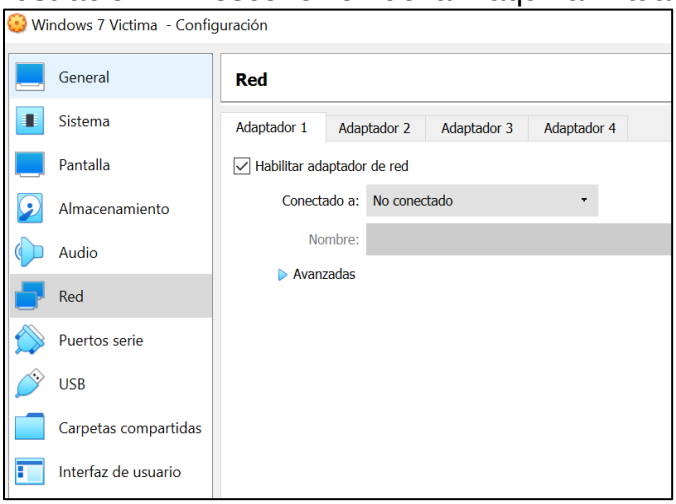
Ilustración 3. Funcionamiento adecuado del sistema operativo



Fuente: Elaboración propia

En la ilustración 4 debido a la alta probabilidad de contagio de este ransomware, se realiza la desconexión de la máquina virtual, con el fin de evitar que en la prueba se puedan infectar otros equipos conectados a la red interna.

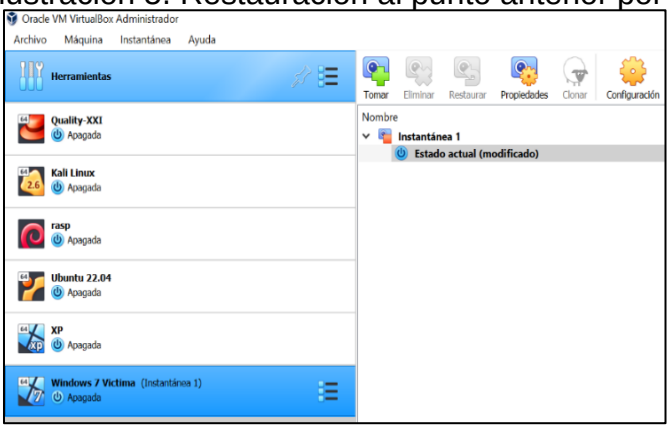
Ilustración 4. Desconexión de la máquina virtual de la red interna



Fuente: Elaboración propia

De igual forma se utiliza la herramienta instantánea en la máquina virtual para restaurar el sistema operativo tan pronto se realice la operación, como se puede ver en la ilustración 5.

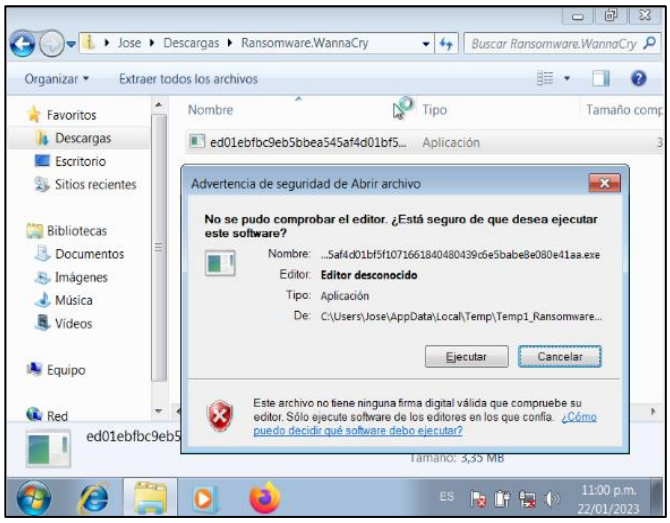
Ilustración 5. Restauración al punto anterior por la herramienta instantánea.



Fuente: Elaboración propia

6.2.4 Ataque con el malware WannaCry: Al tener todas las medidas de seguridad respectivas incluso, para la máquina anfitrión, se procede a ejecutar el malware, con los siguientes resultados, ver ilustración 6.

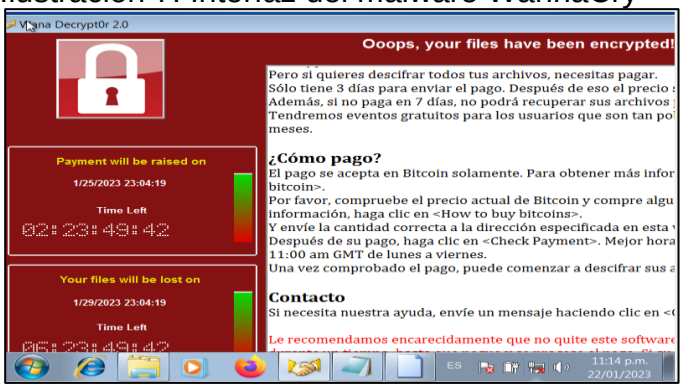
Ilustración 6. Interfaz de ejecución del malware WannaCry



Fuente: Elaboración propia

Al ejecutar se presenta la interfaz del malware a la hora de cifrar los archivos, ver ilustración 7.

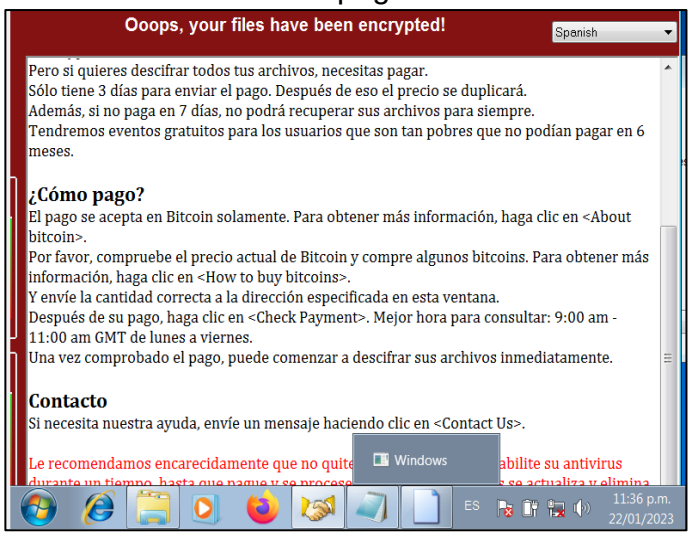
Ilustración 7. Interfaz del malware WannaCry



Fuente: Elaboración propia

Además, este ransomware utilizado con frecuencia en Latinoamérica, tiene instrucciones de pago del rescate de la información en español, ver ilustración 8.

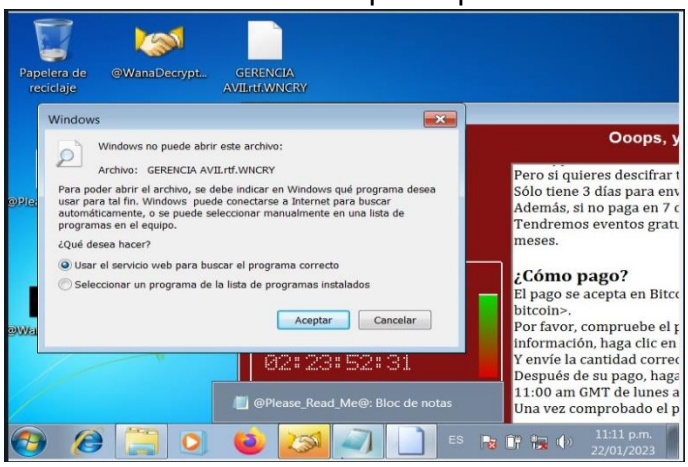
Ilustración 8. Método de pago del rescate de la información



Fuente: Elaboración propia

Para el ejemplo se crearon algunos documentos, estos son los resultados después del ataque de ransomware, ver ilustración 9.

Ilustración 9. Archivo encriptado por el ransomware WannaCry.

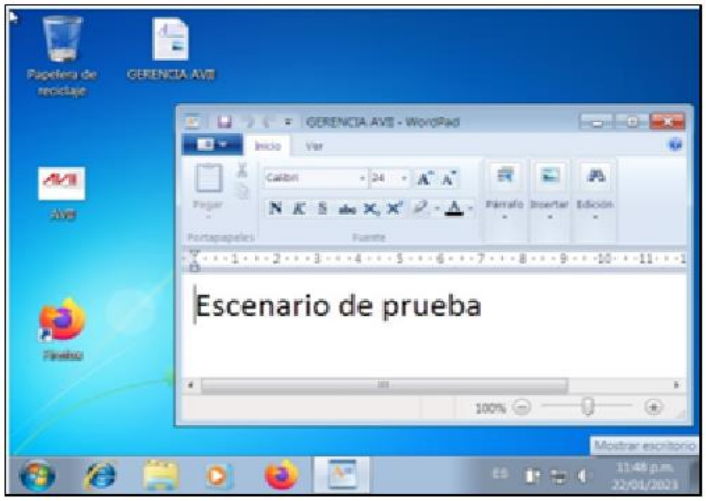


Fuente: Elaboración propia

En este punto ya la red de la entidad está infectada y no es posible desencriptar los archivos, sin ayuda de personal experto o en su defecto pagando la extorsión de los delincuentes, sin que esto asegure la recuperación total de los archivos.

Para finalizar la prueba del escenario controlado, se utiliza la herramienta Instantánea de la máquina virtual, para revertir el proceso, entonces es posible acceder de manera convencional al sistema operativo y a los archivos, ver ilustración 10.

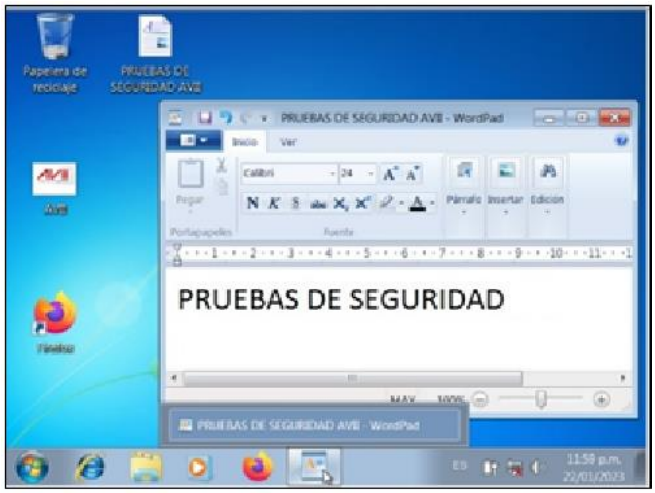
Ilustración 10. Restauración del escenario controlado



Fuente: Elaboración propia

6.2.5 Ataque con el malware Cerber: Para este ataque al igual que con el malware anterior, se deben tomar todas las medidas de seguridad tanto en la máquina virtual como en la máquina anfitrión, por ello es necesario desconectar de la red interna la máquina de prueba. Para este caso se cambiará el documento, el título como el mensaje interno, el cual será “pruebas de seguridad”, con el fin de verificar la manera en que actúa el malware Cerber, muy usado en Latinoamérica para causar daños a infraestructuras críticas y entidades gubernamentales (saboteo), ha sido responsable de múltiples ataques a empresas de sur América, ver ilustración 11.

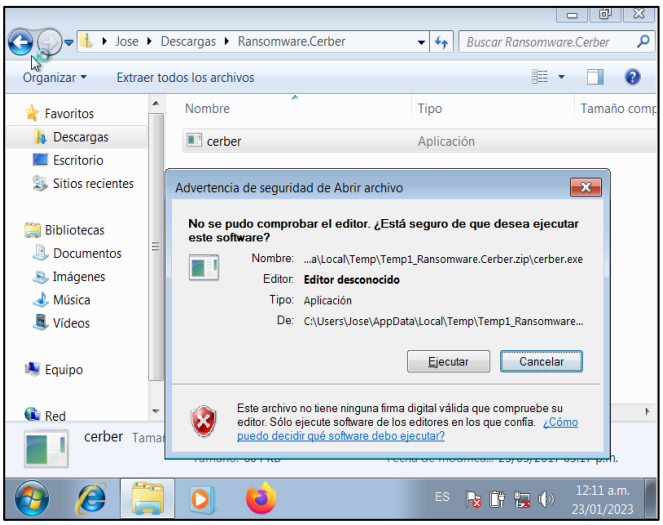
Ilustración 11. Archivos y funcionamiento antes del ataque con Cerber



Fuente: Elaboración propia

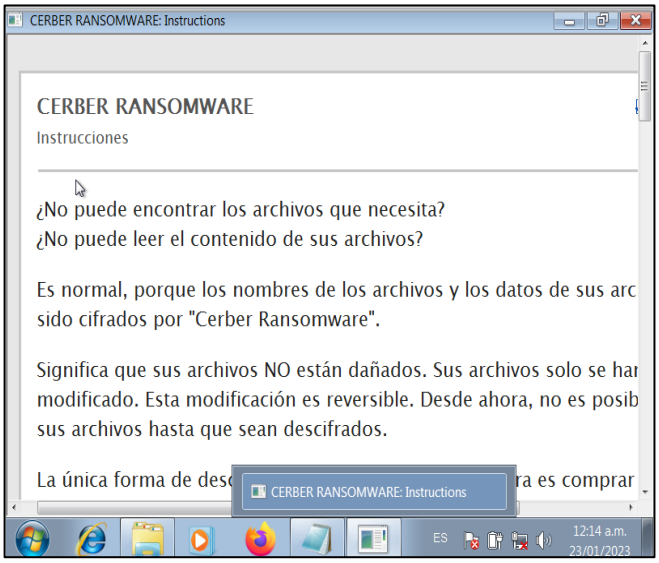
Para realizar este ataque, se descargó un repositorio controlado de la versión de Cerber, el cual puede ser introducido en un archivo ejecutable en un correo, utilizando técnicas de ingeniería social y de engaño, el usuario final puede descargar fácilmente, sin darse cuenta de que está bajo ataque de la ciberdelincuencia, ver ilustración 12.

Ilustración 12. Archivo ejecutable del malware Cerber



Fuente: Elaboración propia

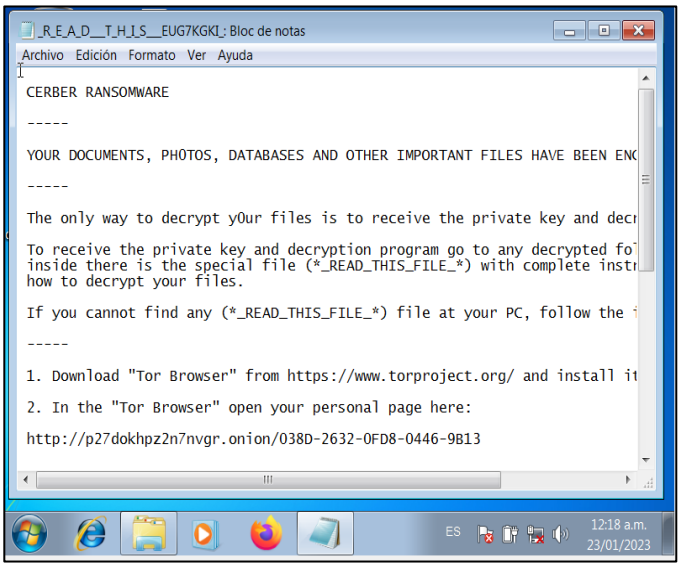
Ilustración 13. Interfaz del ataque por el malware Cerber



Fuente: Elaboración propia

Ver ilustración 13 y 14, automáticamente abre un bloc de notas con las instrucciones para el rescate de la información. Cabe resaltar, el uso del buscador ***TOR***, para la transacción.

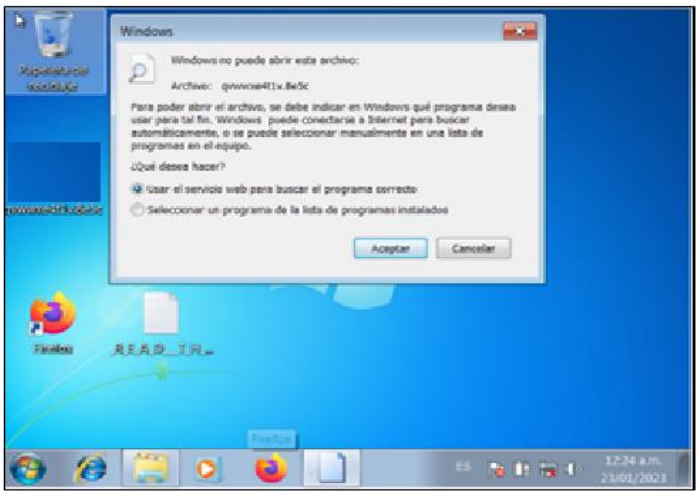
Ilustración 14. Texto con instrucciones del pago para el rescate de la información.



Fuente: Elaboración propia

Al intentar abrir los archivos, han cambiado de nombre y de extensión, por lo que es clara la forma inminente en que el malware ataca los archivos del usuario, cifrándolos y exigiendo una suma de dinero para recuperar la información,

Ilustración 15. Archivos cifrados por el malware Cerber



Fuente: Elaboración propia

Por último, se realiza la recuperación del sistema operativo en el entorno controlado, desde Virtual Box, evitando que al conectarse de nuevo a la red interna pueda transmitir el malware a la máquina anfitrión y se da por terminado el escenario controlado de ataques con ransomware.

6.2.6 Vectores de ataque: Los vectores de ataque son los métodos o estrategias que utiliza el atacante para obtener el ingreso no autorizado a la red o equipos de una entidad, existe dos clases de vectores que pueden ser utilizados para ejecutar un ataque, vectores pasivos o vectores activos[20]

[20] OPTICAL NETWORKS, [Sitio web]: ¿Qué son los vectores de ataque en ciberseguridad? 2023. Disponible en: https://www.optical.pe/blog/vectores-de-ataque ciberseguridad/#:~:text=Vectores%20de%20ataque%20pasivos%3A%20com%C3%BAnmente,afectar%20los%20recursos%20del%20mismo

6.2.6.1 Vector pasivo: son todos los ataques que no requieren afectar o manipular los recursos del sistema, entre ellos se cuentan el Phishing, el Spearphishing y otros ataques de este tipo que causan confusión y engaño a usuarios finales.

6.2.6.2 Vector activo: Son los ataques que requieren el uso de vulnerabilidades en los equipos o en la red organizacional, para implantar malware o exploit, que posteriormente dan lugar a ataques como el ransomware. Comúnmente las organizaciones dedicadas al cibercrimen utilizan los dos tipos de vectores para tener efectividad en sus ataques y lograr el daño suficiente a los archivos de entidades y personas, para extorsionar con cifras altas de dinero a sus víctimas.

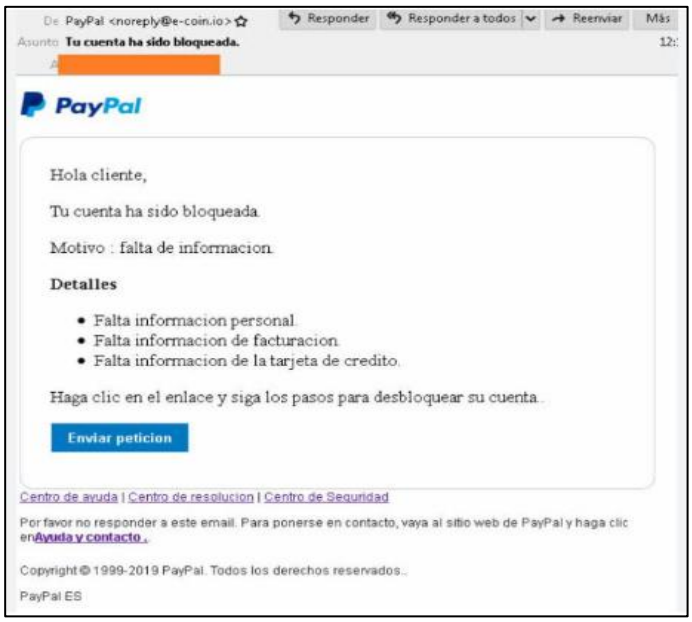
6.2.7 Ataques de ingeniería social Los ataques de ingeniería social o ataque informático humano[21] se relacionan directamente con el carácter, comportamiento y debilidades de las personas en cuanto a sus actividades en internet, pues los ciberdelincuentes pueden acceder a redes, dispositivos e información sin mayor esfuerzo, solo manipulando las emociones del usuario, apelando al miedo, codicia, curiosidad, buena voluntad etc.

Entonces, un vector de ataque de ingeniería social, de fácil ejecución y uno de los más utilizados, podría ser un vector de ataque pasivo como el Phishing, con el uso del correo electrónico, el cual puede contener información falsa que pueda cautivar a la víctima como una supuesta multa de tránsito o la entrada de dinero a su cuenta personal.

[21] IBM, [Sitio web]: ¿Qué es la ingeniería social? 2022. Disponible en: https://www.ibm.com/es-es/topics/social-engineering

En la ilustración 16 se plantea un ejemplo de un caso de aplicación del phishing, donde el personal que incauto y con poca capacitación relacionada con el tema puede ser presa fácil de un atacante:

Ilustración 16. Correo falso con el uso de vectores pasivos (phishing)



Fuente: Betech, [Sitio web]. Detectada una nueva estafa phishing usando correos de Pay Pal. 2023. Disponible en: https://as.com/meristation/2019/05/14/betech/1557870025_055503.html

Existen varios tipos de ingeniería social, por ejemplo, el *Phishing,* donde generalmente los ciberdelincuentes usan correo electrónico para hacer creer al destinatario que el mensaje es de alta importancia o que es emitido de una entidad financiera, empresas prestadoras de servicios públicos, empresas de salud o entidad pública gubernamental, con el fin que descargue malware, envié dinero, actualice datos y publique información sensible tanto personal, bancaria o empresarial. El *Spearphishing* es una estafa donde se identifica un usuario importante que tenga acceso a una red, un director ejecutivo o privilegios corporativos de alguna entidad o figura pública y se envía un correo aparentemente confiable con malware o con enlaces a una *webspoofing* donde se sustrae información personal y credenciales de acceso a cuentas bancarias etc.

6.2.7.1 Fases de ataque por medio de Ingeniería Social:

Fase de recolección de información o *footprinting,* donde el ciberdelincuente recopila información personal como correo electrónico, documento de identidad, número de teléfono, credenciales de cuentas bancarias etc.

Fase de manipulación psicológica donde el ciberdelincuente gana la confianza de su víctima para realizar posteriormente algún tipo de fraude.

Fase de salida o fase final de ataque, el ciberdelincuente busca ocultar el fraude causando mayor impacto a la empresa.

6.2.8 Estrategias para mitigar el impacto ante un posible ataque de ransomware: Después de realizar un análisis de vulnerabilidades en la arquitectura de red, es importante presentar una solución al gobierno corporativo, para aumentar de forma significativa y con el menor presupuesto posible, la seguridad de la información en la entidad. Por tal motivo, se adelantarán una serie de recomendaciones en lo que se refiere a la topología de red basado en la segmentación y virtualización de la red de área local, instalación de nuevos dispositivos de seguridad, tanto lógicos como físicos y por último la implementación de herramientas para el análisis y reconocimiento.

6.2.8.1 Segmentación de la red LAN: La segmentación de redes consiste en volver las redes existentes en subredes (redes más cortas), se realiza este cambio para mejorar la velocidad y la seguridad de la red. A medida que van formándose nuevas subredes, se deben aplicar políticas o controles, según sean los privilegios de usuario, con el fin de gestionar privilegios a determinados usuarios para las labores que tiene asignadas.

En lo referente a la seguridad, cada nuevo segmento se debe acoplar a las políticas y normas establecidas, con el fin de preservar o mantener la seguridad incluso en puntos débiles. Es decir, al segmentar la red, el atacante puede infectar cierto sector, pero no la red completa y no puede ingresar al componente administrativo para generar cambios, logrando una barrera adecuada impidiendo que afecte otros usuarios.

Se realizó una segmentación de red en tres redes VLAN, cada subred contiene elementos estratégicos, que permitirán generar una protección avanzada de los dispositivos, servidores y otro tipo de dispositivos que se utilicen en la red interna de la entidad. El rendimiento es importante y sobre todo en una organización en crecimiento, por ello la segmentación produce un efecto de liberación de tráfico en red. En vista que opta por otros caminos para reducir el tráfico en otros factores, dando como resultado menos host que congestionen la red**.**

Es conveniente entonces, realizar la virtualización de la red o VLAN, además de mejorar el rendimiento de la red, cada segmentación debe tener sus propias políticas con el fin de limitar el tráfico entre cada segmento. Se debe tener en cuenta el acceso de tecnologías basadas en la nube, elementos personales como laptops, smartphones, entre otros, la segmentación a través de redes virtuales es primordial dando mayor rendimiento al no tener que contar con infraestructura física, es posible virtualizar toda la red.

6.2.8.2 VLAN 1: Contiene todos los elementos y servicios utilizados por el equipo de encargados de las tecnologías de la información, los servidores de bases de datos, DNS y otros que revisten importancia para la organización y que deben ser protegidos de manera especial por la información que contienen.

6.2.8.3 VLAN2: Para mantener la nueva infraestructura segura, se implementaron diferentes dispositivos y software estratégicos, así como el uso de segmentación de redes y otras herramientas adecuadas para proteger los usuarios y sus dispositivos de ataques cibernéticos, esta red virtual se encarga exclusivamente de los aspectos relacionados con las áreas internas de la empresa (gerencia, talento humano, contabilidad entre otras) que deben realizar labores cotidianas en la entidad, pero no están exentos de ataques cibernéticos. Como medida especial en esta segmentación, cada funcionario tendrá usuario y contraseña único, con privilegios específicos otorgados por los responsables de las tecnologías de la información, acción que permitirá el control de algún sabotaje a la red por parte de funcionarios inescrupulosos, los cuales serán bloqueados de manera inmediata.

6.2.8.4 *VLAN 3:* Esta red está ubicada en una zona desmilitarizada o DMZ, acción estratégica que también será el lugar adecuado para instalar el servidor web, permitiendo además la conexión vía Wifi a clientes que visiten las instalaciones físicas de la entidad. La implementación de una DMZ que permita el ingreso de todo público es necesaria debido a los servicios que ofrece la entidad por medio de internet, porque usuarios como clientes, proveedores y otros interesados utilizan la plataforma de servicios; por ello, es necesario hacer énfasis en las ventajas de realizar una DMZ o zona desmilitarizada, para ofrecer este tipo de servicios a la vez que se preserva la seguridad de la red local o interna de la compañía.

Preservar la integridad de la información es posible, pero cuando se brindan servicios por internet es complejo mantenerla, por ello es conveniente dividir la red, estableciendo dos perfiles, uno privado para la red local y uno público para los servicios a través de internet.

Al formar una DMZ es posible minimizar los riesgos de ataques externos que quieran ingresar a la red local, para ello se utilizará un cortafuegos que se configurará de manera que no permita el ingreso a la red privada, sino exclusivamente a información como página web (servidor web), los cuales además deberán contener políticas organizacionales para que no se vean afectados por otro tipo de ataques como el ransomware a través de correos infectados.

6.2.8.5 Implementar NGFW (next generation firewall): Para mejorar la seguridad de los paquetes de datos que entran y salen de la red interna, es necesario instalar un NGFW. Son elementos de última tecnología que contribuyen a controlar el acceso no permitido de cierto tipo de paquetes que, por lo general contienen virus y otro tipo de amenazas, que ya no son detectadas por los firewalls convencionales en vista que los atacantes crean códigos maliciosos más sofisticados e indetectables, dejando obsoletos a los cortafuegos que se utilizan comúnmente.

Los firewalls de nueva generación contribuyen a gestionar diferentes tipos de filtros y mejoran las redes LAN, es decir, autorizan o rechazan ciertas conexiones que puedan representar un riesgo para la red o para otros usuarios, por ello se obtendrán los siguientes parámetros de seguridad al momento de la activación de esta herramienta:

- Antivirus
- Control de aplicaciones
- Detección y prevención de intrusos
- Control de pérdida de datos
- Autenticación de usuarios
- Centralizador de VPN
- Filtrado a sitios web

Otros beneficios con la aplicación de los *NGFW* son de gran apoyo a la seguridad digital de la organización, dado que la identificación de aplicaciones es su objetivo, dejando de lado la validación de puertos; de igual forma no es necesario tener en cuenta el protocolo, en vista que la reputación e identificación son primordiales y hacen parte de las políticas de seguridad del NGFW[22]. Cuando se realizan consultas tipo web no se identificarán las direcciones IP, se certificarán los usuarios los cuales deben ser identificados y deben estar en los directorios o bases de datos de la entidad, con el fin de otorgar responsabilidades en investigaciones posteriores de las acciones del usuario.

Cuando los firewalls de nueva generación encuentran una amenaza o riesgo inminente, bloquea inmediatamente cualquier tipo de vulnerabilidad activa, llámese software malicioso, URL con mala reputación o cualquier archivo que represente una amenaza. Algunos trabajadores deben cumplir con sus actividades fuera del entorno laboral, dejando así brechas de seguridad al activar mecanismos que requieren mayor protección, en redes domésticas de los usuarios e incluso algunas redes públicas, generando vulnerabilidades en el activo de la información. Esto puede ser controlado con los firewalls de nueva generación, habilitando un perímetro lógico que permite a todos los usuarios, seguridad constante.

6.2.8.6 Implementar de soporte Cloud: Servidores para efectuar copias de seguridad directamente enlazados con una nube de tipo empresarial de pago, en la cual se realizarán las copias de seguridad que tendrán soporte físico y en la nube, en caso de que un ataque de ransomware sea inminente.

[22] SILVA, Diego. [Sitio web]. Evaluación de Tecnologías UTM (Unified Threatment Management) y NGFW (Next Generation Firewall) para detección de vulnerabilidades en la red. 2020.p.30. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/14080

6.2.8.7 Implementar una solución de IDS/IPS: Es necesario la implementación de IDS (sistema de detección de intrusiones) o de una IPS (sistema de prevención de intrusiones) teniendo en cuenta la modernización de la red. Por lo tanto, según investigaciones, la herramienta IDS no realiza acción en contra de una amenaza, excepto generar alarmas de posible intrusión. Por tal motivo y en vista que este tipo de sistemas son requeridos a todo momento, no es posible mantener un funcionario encargado de este tipo de amenazas que pueda evitarlas. De tal forma que se aplicará la herramienta IPS, que permite desviar ciertos paquetes que puedan contener algún riesgo para la red. Otras cualidades de este sistema de seguridad son:

- La acción de la IPS es preventiva y realiza análisis con protocolos y todo tipo de conexiones en tiempo real, cuando se está bajo ataque determina cuales son las acciones sospechosas y basado en las políticas configuradas anteriormente, puede realizar alarmas, desviando paquetes y evitando cualquier conexión sospechosa[23].
- La IPS es una ventaja efectiva contra ataques de fuerza bruta, modificación de sistemas de archivos, malware, entre otras. Desafortunadamente esta herramienta es susceptible a los ataques de DDOS y puede generar graves problemas en su normal funcionamiento.

6.2.9 Implementación de la herramienta para el análisis reconocimiento de vulnerabilidades Nexpose: Software de análisis y búsqueda de vulnerabilidades, por el cual es posible identificar el riesgo en tiempo real, debido a su conexión a la red, priorizando algunas vulnerabilidades que presentan un mayor riesgo y que a su vez, proporciona soluciones al encargado de las TI de la entidad, para verificar posibles fallos de seguridad de manera eficiente.

[23] COYLA Yony. [Sitio web]. Implementación de un sistema de detección y prevención de intrusos IDS/IPS. 2019.p.24. Disponible en: http://hdl.handle.net/20.500.12840/2002

6.2.9.1 Servicios afectados por la operación del escáner de vulnerabilidades: Según los registros otorgados por la herramienta Nexpose, después de escanear el recurso virtual, es notorio que las vulnerabilidades afectan en su mayoría a los servicios web tales como:

- Los servidores web y aplicaciones relacionadas a PHP.
- Las aplicaciones relacionadas con SSH.
- Los servidores HTTP (apache).

6.2.9.2 Severidad de las vulnerabilidades encontradas por la herramienta Nexpose: Es claro que, hay muchas posibles brechas, o escenarios descubiertos por el escáner, para efectuar un ataque que vulnere la seguridad de la información, por distintos métodos, tales como: exploit, o cualquier otro tipo de daños que sean posibles de manera remota, ataques que pueden ser robo de información o simplemente sabotaje. El objetivo de estas herramientas se basa en brindar información a los usuarios para que identifiquen que tipo de amenazas surgen y evitarlas, de manera preventiva.

6.2.10 Metodología para el descubrimiento de vulnerabilidades. Las pruebas de intrusión son un mecanismo para determinar si existen brechas de seguridad que puedan comprometer los activos de la empresa. Teniendo en cuenta la importancia de las pruebas de intrusión, consiste específicamente en realizar un ataque real, con el cual se permita identificar los métodos o los mecanismos que posee el atacante para entrar en el sistema, De esta manera se logra comprender las metodologías utilizadas por el atacante, que quiera causar un daño real a la organización, el cual utilizará todos los métodos disponibles para vulnerar la seguridad y permitir que su ataque cause los efectos esperados.

6.2.10.1 **PTES:** Metodología que contiene 7 fases[24], describe eficazmente las posibles amenazas que se pueden presentar, dando como resultado un informe, útil para ser utilizado por el gobierno corporativo, con el cual tomar decisiones fundamentales orientadas a mejorar la seguridad informática de la organización.

6.2.10.1.1 Fase 1. Interacción previa: Establece los parámetros de la ejecución de la prueba, si requiere que sea un análisis completo o enfocado a cierta vulnerabilidad de la cual se tenga algún antecedente, de igual forma el gobierno corporativo debe establecer los límites del ataque, si es posible suministrar toda la información para encontrar la herramienta específica y enfocarse en determinar las causas por las que ha sido atacado.

6.2.10.1.2 Fase 2. Recolección de información: Después de contar con la información basada en ataques, amenazas o vulnerabilidades descubiertos anteriormente, se puede establecer qué ataques informáticos ha sufrido la entidad.

6.2.10.1.3 Fase 3. Modelado de amenazas En esta fase se debe realizar una identificación de los activos primarios y secundarios con el objetivo de clasificarlos y priorizar aquellos que revistan mayor importancia a la hora de un ataque, esto determina el impacto que podría causar en una situación previamente establecida, basados en información de ataques anteriores o aquellos que hayan afectado el entorno de la organización o su actividad empresarial.

[24] PÁRAMO, Angélica et, al. [Sitio web]. Servicio de Pentesting, basados en la propuesta de auditoría interna con la norma ISO 27001. *Investigación y Ciencia Aplicada a la Ingeniería*, 2021, vol. 4, no 24, p. 35-44. Disponible en: http://ojs.incaing.com.mx/index.php/ediciones/article/view/13/servicio

6.2.10.1.4 Fase 4. Análisis de vulnerabilidades Al detectar las vulnerabilidades que se pueden presentar en un caso hipotético, según información recolectada, posteriormente se realiza un plan o un protocolo basado en políticas organizacionales y las acciones que se deben realizar por el personal experto en hardware, redes, software y encargados del área de TI; identificando principalmente las formas de ataque, información de privilegios de usuarios, los equipos informáticos y sus direcciones IP, claves de usuarios y otros métodos de identificación con ello se aplicará la prueba pentest a los equipos con riesgo.

6.2.10.1.5 Fase 5. Explotación La información de la fase anterior es el preámbulo de las acciones realizadas durante esta etapa, aquí es donde se aplican los métodos de pentest, se ataca directamente el sistema, descubriendo las falencias existentes en todos los dispositivos y redes, con ello se determina además las barreras de seguridad eficaces durante un ataque. En definitiva, se realizan una serie de ataques que exploten las vulnerabilidades existentes en el componente informático de la organización.

6.2.10.1.6 Fase 6. Post-Explotación Consiste en postergar el acceso al sistema operativo, aplicaciones y redes vulneradas para obtener información de los sitios qué puede modificar, que tipo de privilegios de usuario alcanza y qué cambios puede realizar incluso de forma administrativa en los componentes del sistema. Al analizar la información extraída se obtiene que tipo de usuarios o elementos del sistema, no cumplen con las políticas de seguridad en TI.

6.2.10.1.7 Fase 7. Informe final Es conveniente aclarar que esta metodología no tiene un formato específico para la entrega de este informe, aunque debe cumplir con parámetros de información como, tipo de vulnerabilidades encontradas, usuarios y responsabilidades en materia de riesgos y la explicación del exploit utilizado para encontrar las vulnerabilidades.

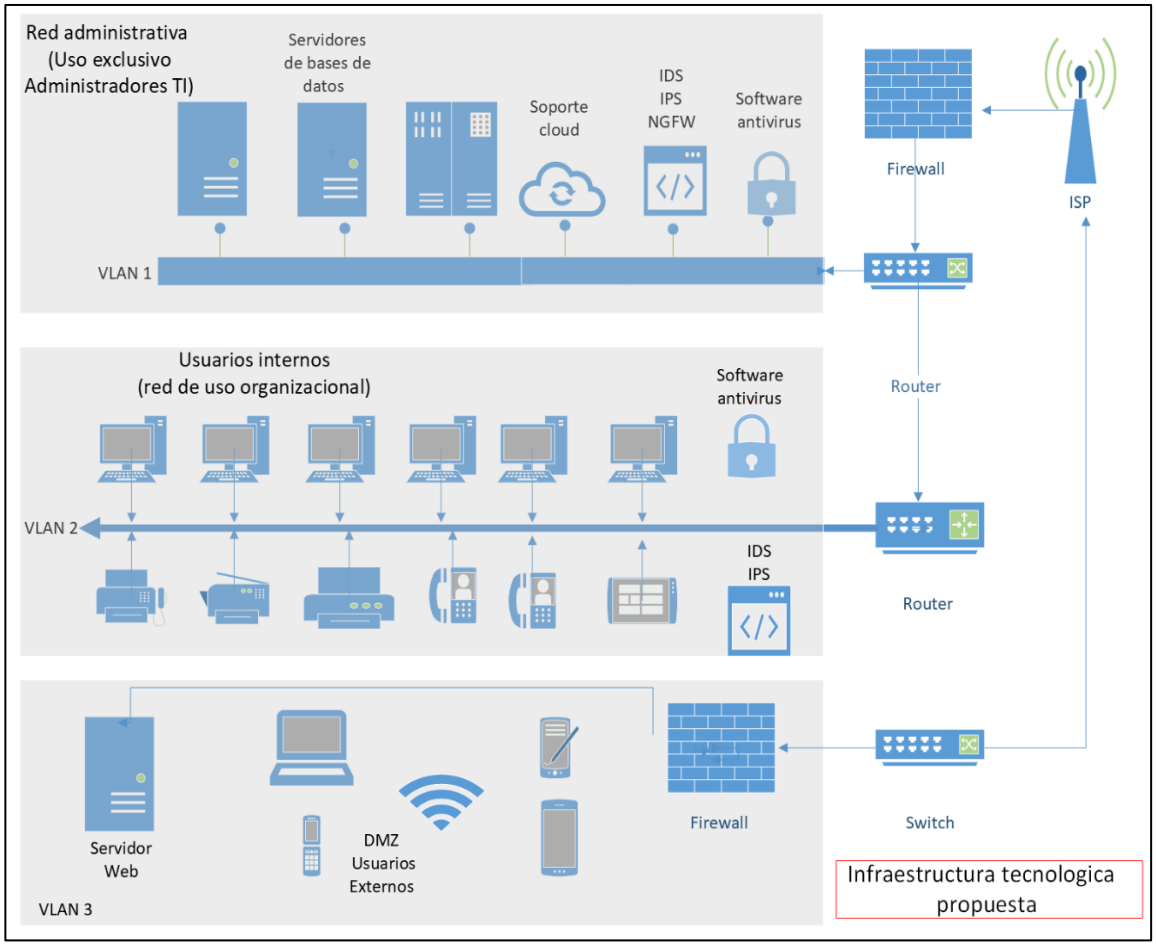
Logro obtenido: La aplicación de esta metodología permitió establecer el proceso adecuado para llevar a cabo una actualización de los componentes de una red exitoso, especificando los detalles, demostrando que innovar las barreras y dispositivos de detección temprana de vulnerabilidades disminuye el factor de riesgo al implementar niveles altos de seguridad. Una estrategia importante, debido al análisis de situación realizado, consiste en capacitar al personal de la empresa en técnicas para prevenir los ataques de ingeniería social y evaluar constantemente la reacción ante un evento simulado, minimizando el riesgo de propagación de ransomware puede afectar seriamente a la entidad. Para evitar que, por intermedio de un funcionario la empresa sea víctima de un ataque de ingeniería social, se debe aplicar los protocolos de seguridad sugeridos por el personal de las tecnologías de la información de la empresa y adoptar una postura preventiva en cuanto al uso de los sistemas de información. No obstante, la asignación de usuarios exclusivos con privilegios limitados, permitirán ejercer control a las actividades realizadas individualmente por cada persona en su entorno laboral.

6.2.11 Propuesta del diseño del escenario controlado a la arquitectura tecnológica a la organización objeto de análisis: En ilustración 17, se expone la propuesta formulada al gobierno corporativo de la organización, en la cual existen varios métodos de seguridad en red, los cuales permitirán hacer frente a un número indeterminado de ataques de ransomware, debido a la cantidad de posibles vectores.

Cada uno de los métodos implementados en esta propuesta, contiene herramientas que pueden contrarrestar cualquier tipo de ataque o amenaza, sin dejar de lado las vulnerabilidades que se presentan en el día a día de las empresas similares.

A través de este diseño, la organización va a contar con una red completamente virtualizada y moderna, con dispositivos de hardware y software que cumplirán adecuadamente la filtración de paquetes de datos, así como hacer pruebas y auditorias que permitan la mejora constante de la red, evidenciando posibles fallas o vulnerabilidades.

Ilustración 17. Propuesta topología de red



Fuente: Elaboración propia

6.3 DESARROLLO DE LA FASE 3: ESTRATEGIAS DE PROTECCIÓN Y BUENAS PRÁCTICAS QUE PERMITAN OFRECER GARANTÍAS SEGURIDAD DE LA INFORMACIÓN A LA ORGANIZACIÓN OBJETO DE ANALISIS, A PARTIR DE LOS RESULTADOS OBTENIDOS AL APLICAR PRUEBAS SOBRE EL ESCENARIO CONTROLADO.

A partir del análisis expuesto y de los resultados de la investigación hasta este punto, es necesario realizar una serie de recomendaciones que sirvan como la primera defensa y la más importante, ante los ataques cibernéticos de diferentes fuentes que se podrían ejecutar en una organización. Por consiguiente, es importante recalcar que el usuario final e inexperto en cuanto a la seguridad informática se refiere, como se ha expuesto durante este documento, puede significar fácil acceso para un atacante que utilizará una serie de vectores de ataque basados en la ingeniería social para acceder de manera abusiva a la información interna de la entidad. Por lo tanto, reviste de especial importancia que la entidad capacite a sus funcionarios de forma constante, para evitar que, por medio de este canal, surtan efecto las estrategias realizadas por los ciberdelincuentes que solo buscan adquirir ganancias con este lucrativo negocio ilegal.

6.3.1 Integrar protocolos de seguridad informática basados en la norma ISO/IEC 27035 como defensa de ataques cibernéticos: la organización ha requerido del uso constante del internet, como puerta de entrada de clientes y los interesados en la organización, situación que conlleva a mejorar sus sistemas de seguridad, además que evolucionen, protejan la integridad de la información y permitan gestionar incidentes para evitar delitos informáticos y minimizar el impacto de riesgo. Para dar cumplimiento a este objetivo, se adoptaron buenas prácticas basados en la norma ISO/IEC 27035, esta norma se alinea a los objetivos de la empresa teniendo en cuenta la gestión y respuesta del incidente.

6.3.2 Protocolo para contrarrestar ataques informáticos

- Plantear políticas de seguridad de la información, soporte técnico, protección de la red, actualización del sistema de Información y capacitación al personal operativo y organizacional sobre incidentes de seguridad de la información.

- Detección y reporte de sucesos que permitan identificar actividades irregulares, sospechosas o de *malware* que afecten los pilares de la integridad de la información. Conviene destacar que, en el evento que ocurra un ataque cibernético, el personal del área de las tecnologías de Información, debe suministrar un informe detallado a las autoridades competentes de la amenaza encontrada, con el fin que haga parte de la base de datos de vulnerabilidades y pueda ser contrarrestada eficazmente.

- Una parte esencial del protocolo se basa en la evaluación inicial y decisión que permite determinar si el evento es un incidente de seguridad de la información, o un hecho inusual que no sea una amenaza específica, debido a un fallo en la actualización de algún software que presente fallas o una posible anomalía del sistema operativo, para lo cual se debe implementar una segunda evolución que confirme la categoría implicada, naturaleza e impacto.

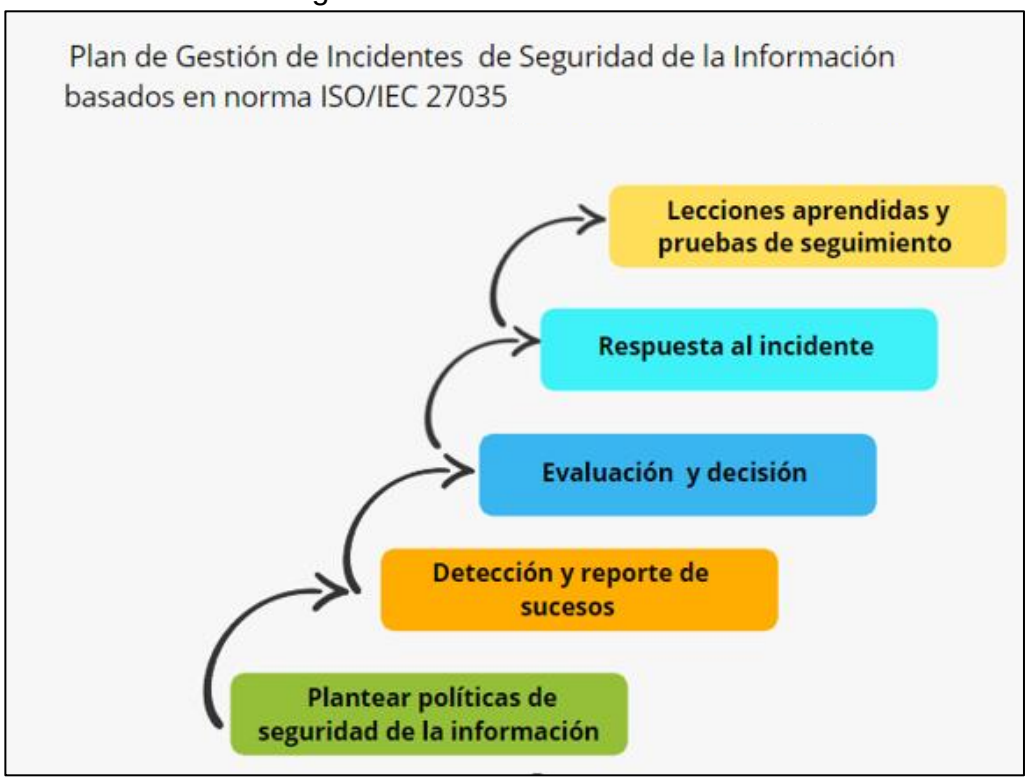
- Con base en la información obtenida durante la aplicación de los pasos anteriores del protocolo, se generará una respuesta al incidente que incluye el análisis del mapeo del sistema de TI, servicios de la red, detección de la naturaleza del incidente e impacto que genera sobre la empresa para proceder a la erradicación como procedimiento de mitigación, esto permite ejecutar el plan de recuperación, restauración de imágenes, actualización de parches y endurecimiento informático (hardening), garantizando la continuidad de la operatividad de empresa en el menor tiempo posible.

- Por consiguiente, las lecciones aprendidas identificables permitirán hallar un sinnúmero de mejoras en el sistema de seguridad de la información, así como estrategias en el plan de gestión y efectividad en la evaluación del riesgo, factor clave en la evolución y tratamiento de posibles vulnerabilidades relacionadas directamente, con el fortalecimiento del cibercrimen, el cual se convirtió en un negocio lucrativo que ha llevado a gran cantidad de organizaciones, a un colapso económico debido a la falencia en lo que se refiere a los sistemas de seguridad de la información de la entidad, no solamente a la perdida de prestigio y credibilidad, también al activo intangible de mayor costo en cualquier organización como es la información.

- Por último, realizar pruebas de seguimiento y revisión continua que no interrumpan la operatividad, hace parte de un chequeo constante del buen funcionamiento de la plataforma tecnológica. De igual forma, documentar cada uno de los hallazgos en el escenario de la prueba como el objetivo, tipo de prueba, duración de la prueba, quienes participan, medida de éxito o fracaso y los recursos utilizados para la implementación, darán como resultado, la optimización del proceso y uso adecuado de los recursos informáticos, creando una solución adecuada a los problemas de seguridad en la organización.

En la ilustración 18, se encuentran las diferentes fases del proceso de gestión de incidentes, fundamentados en la ISO/IEC 27035, aplicables cuando existan posibles fallos en cuanto a la seguridad de la información, sobre todo para enfrentar futuras amenazas, las cuales se transforman y evolucionan conforme avanza las nuevas tecnologías.

Ilustración 18. Plan de gestión de incidentes.



Fuente: Elaboración propia

6.3.3 **Aplicar estrategias, medidas preventivas, buenas prácticas en el uso cotidiano del correo electrónico y de las herramientas ofimáticas comunes**. Para cumplir este objetivo se propone a el gobierno corporativo implementar estrategias y medidas preventivas que permitan detectar y mitigar el riesgo de un ataque de ransomware mediante el siguiente protocolo:

- Realizar copias de seguridad de forma periódica las cuales deben permanecer en un lugar seguro, sin conexión a internet o una red pública, evitando el acceso desde los equipos empresariales no autorizados.
- Realizar una lista de chequeo con la implementación de políticas de actualización de software, f*irmwar*e y aplicaciones.

- Integrar parámetros específicos para la configuración de *firewall,* según los paquetes de información, fuentes y reputación de los sitios que pretendan ingresar a la red.
- Ejecutar herramientas que permitan mitigar los ataques con exploit.
- Bloquear dominios y servidores usando IDS/IPS que identifican actividades no autorizadas evitando que los ciberdelincuentes tomen control del servidor.
- Realizar una lista de control de accesos al mapeo de la red y realizar revisión usando el visor de eventos de Windows.
- Desactivar *Windows Script Host* con el fin de evitar que se ejecuten *scripts* con *malware y* documentos ofimáticos con macros*.*
- Desactivar macros de ficheros o habilitar el modo lectura de adjuntos enviados por correo electrónico.
- Una estrategia preponderante para la verificación de archivos y otro tipo de enlaces sospechosos en el uso de entornos virtualizados, o máquinas virtuales, debido a su alta efectividad y la disminución del riesgo en cuanto a la afectación de la máquina fija o los dispositivos en red.
- Aplicar políticas al firewall, que desactiven la ejecución automática de unidades de almacenamiento externo, a su vez, eliminar el uso de unidades compartidas, e incluso implementar control al acceso en las carpetas por medio de comandos administrativos.
- Desactivar los componentes innecesarios del sistema operativo principalmente el de escritorio remoto y cerrar los puertos de servicios no utilizados por los usuarios.
- Realizar auditorías periódicas para identificar las vulnerabilidades.
- Utilizar VPN (Virtual Private Networking), para la recepción y envío de información sensible.
- Establecer políticas en cuanto al uso de contraseñas, estableciendo privilegios para el acceso de archivos a personal calificado, limitando utilizar

el usuario administrador, exclusivamente a quien tenga la responsabilidad del componente TI.

- En efecto, la mayoría de los funcionarios reacciona de forma similar al uso de publicidad y material visual de empresas que ofrecen algún producto oferta. Para el caso de distribuir la información ransomware por medios electrónicos, se utilizarán canales con carteles, banners y producciones de tipo audiovisual como videos, proyectados en pasillos y lugares estratégicos de la entidad, para cumplir el objetivo de la capacitación constante de los funcionarios de la entidad.

6.3.4 Protocolo en caso de ataque inminente: La detección oportuna de un ataque de ransomware permite que los encargados de las TI puedan responder de forma eficaz. En una empresa común, sin controles de seguridad informática adecuados, el malware puede permanecer en los equipos y redes extrayendo información sin que el usuario o la organización lo sepan. Para cuando haya solicitudes de dinero por el secuestro de la información o un aviso del delincuente que él tiene bajo su poder el sistema, la mayoría de la información ya está cifrada, comprometidos redes y equipos, con un daño a la información.

En el evento que el ataque de ransomware se haya perpetrado, es conveniente seguir los siguientes pasos para disminuir los daños, evitando la propagación a otros equipos y mayores daños a la información alojada en el equipo infectado.

- No apagar el dispositivo o equipo que haya sido atacado por ransomware, por el contrario, debe aislarlo y desconectarlo de la red y de conexiones a elementos periféricos.
- Evaluar que la copia de respaldo no haya sido comprometida por ransomware, existen vectores que atacan también las copias de seguridad,

por ende, es necesario realizar la verificación de la información en computadores que no tengan conexión a otros dispositivos.

- Identificar la causa y vulnerabilidad por donde fue propagado el ransomware, esto permitirá tomar acciones para otros dispositivos, o en su defecto con la red, siendo este un evento que debe ser documentado y evaluado para futuros análisis de seguridad.
- De igual manera, al restaurar la información después de un ataque de ransomware, el equipo de TI debe certificar que cuenta con las garantías de uso del dispositivo, con el fin de preservar la información con integridad, sin que afecte posteriormente a otros dispositivos o archivos.
- Es conveniente identificar y documentar los equipos y redes afectados, preservar esta información por si el malware persiste después de la restauración, con el fin de encontrar la vulnerabilidad o malware y hallar una posible solución, después del análisis del vector de ataque.

6.3.4.1 Recomendaciones de seguridad:

- Establecer una política de contraseñas seguras, de igual forma cambiarlas constantemente según un cronograma previamente establecido.

- Deshabilitar usuarios que ya no trabajen en la empresa, o aquellos que por otras circunstancias no les deba ser concedido privilegios en lo que se refiere al acceso, modificación o lo relacionado con la integridad de la información.

- Realizar Backup constantes, según cronograma específico en la política de preservación de la información, con el objetivo de hacer frente al daño o secuestro de la información.

- Verificar puertos y protocolos, con el fin de establecer cambios en aquellos que no son necesarios, o aquellos que no se han utilizado por cambios en el sistema, en lo posible con herramientas de escaneo que sean efectivas y suministren información.

- El equipo de TI debe realizar actualizaciones constantes y verificar aquellos sistemas operativos, software y aplicaciones que no sean seguros para realizar un cambio progresivo de este tipo de herramientas que se convierten en vulnerabilidades.

Logro obtenido: La aplicación de las anteriores directrices basadas en la norma técnica ISO/IEC 27035, permite describir y gestionar posibles riesgos y amenazas en una organización, esta norma se basa en proteger tanto la confidencialidad, la integridad y la disponibilidad de la información, para lograrlo se apoya tanto en la evaluación como en el análisis de los posibles riesgos y estandarización de protocolos de buenas prácticas en una organización.

6.3.5 Políticas de ciberseguridad de la organización

Para la organización es de gran importancia el aplicar las políticas de ciberseguridad, debido a los múltiples ataques recibidos, en otras entidades que, al no prestar la suficiente atención a esta problemática, se convirtieron en presa fácil de la ciberdelincuencia y por si no fuera poco, tuvieron que pagar las extorsiones para no verse inmiscuidos en problemas legales debido a la confidencialidad. Por ello la organización adoptó 8 políticas aplicables en todas las áreas de la empresa por el personal que utiliza las herramientas informáticas, con el fin de evitar crear una brecha de seguridad por falta de normas claras. Por lo tanto y para disminuir el riesgo se llevó a cabo la creación y aplicación de las siguientes políticas de seguridad informática en la organización:

- **Lista de chequeo:** Es la política más importante de la organización, pues a través de su cumplimiento, será posible establecer en un tiempo determinado, la aplicación de cada una de las medidas en beneficio de la organización se debe realizar por el área o equipo de informática de la organización o en su defecto por personal calificado.

- **Actualización de software**: Es necesario disminuir el riesgo de amenaza y posibles ataques, de tal manera que, la actualización de los sistemas operativos a su versión más reciente, la aplicación de parches de seguridad y la renovación de licencias antivirus se convertirán en una estrategia eficaz para reducir el escaneo de redes por atacantes y la posibilidad de su acceso abusivo al sistema.

- **Contraseñas seguras:** Es una de las medidas más importantes en la organización, pues determina los privilegios otorgados a cada usuario, con el fin de mantener la integridad de la información. Así mismo, a través de la autenticación se puede establecer que tipo acciones realizan los funcionarios en sus cuentas e imponer responsabilidades en caso de que haya fuga o daño en la información a la cual tienen acceso. Para mayor efectividad es necesario modificarla en forma regular y debe incluir parámetros como letras números, símbolos o caracteres especiales, mayúsculas y minúsculas.

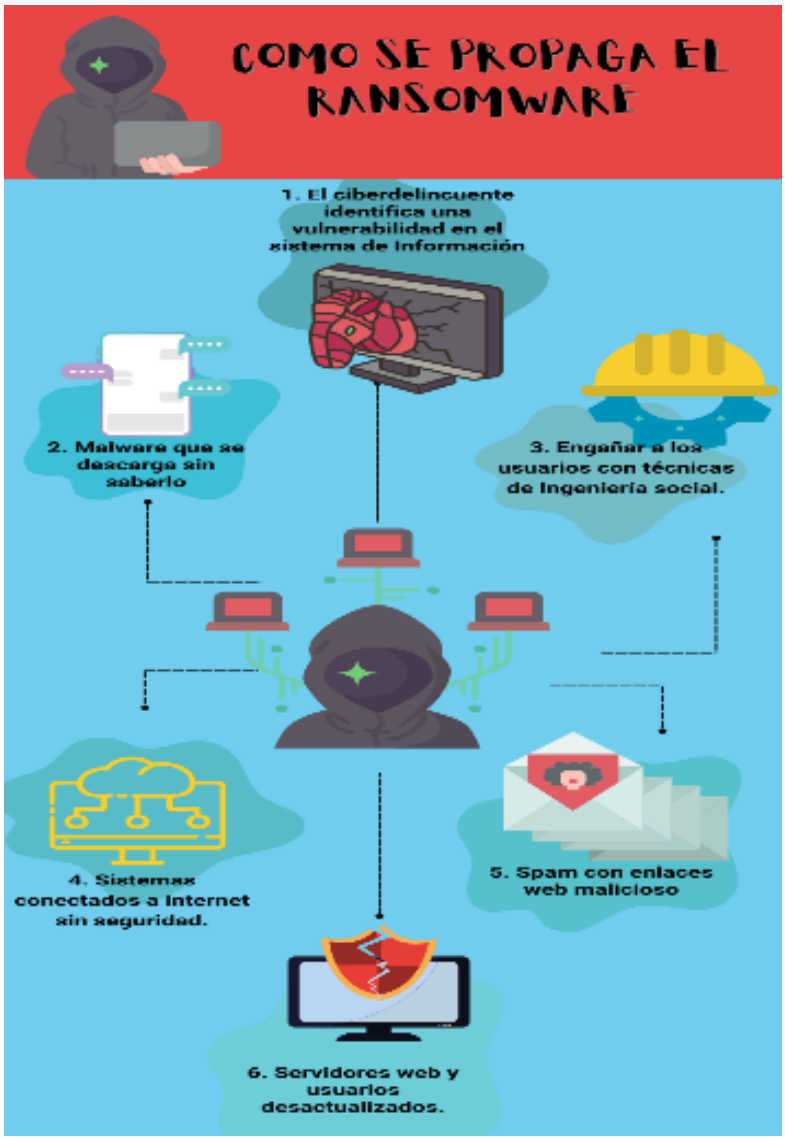
- **Verificar puertos y protocolos abiertos**: Por parte del área de informática es necesario revisar minuciosamente cada uno de los servicios abiertos, en servidores y equipos, con el fin de encontrar aquellos puertos que no sean necesarios o no se usen constantemente para reducir el campo de acción de la ciberdelincuencia.

- **Plan de capacitaciones**: Es necesario reforzar los conocimientos de los colaboradores de la organización, debido a que representan el eslabón más débil en la cadena de la ciberseguridad, pues muchos no cuentan con los conocimientos básicos para evitar un ciberataque. El uso adecuado del correo electrónico, instalación de aplicaciones antimalware/antispam, firma digital, contraseña del correo electrónico segura, identificación de correos sospechosos e identificación de enlaces no seguros, es el lenguaje que todos los usuarios finales deben manejar en ciberseguridad.

- **Copias de seguridad**: Las copias de seguridad se han convertido en el factor clave para preservar la información, pueden ocurrir eventos de ciberseguridad, catastróficos o de otra índole no determinada que afecten la seguridad de la información. De tal manera que, se realizará Backup con una periodicidad determinada, en servidores físicos y a través del uso de la tecnología *cloud*, con el cual se tendrá soporte basado en la nube.

En la ilustración 19. se observa una infografía como estrategia simple y de bajo costo, que contribuye a reconocer el ransomware como una amenaza que se adquiere fácilmente, al no tomar las suficientes precauciones, desde los equipos de cómputo de cada área de la empresa, además se constituye como una de las formas pedagógicas adecuadas para informar a todos los usuarios de los sistemas informáticos de la entidad a tomar comportamientos responsables a la hora de recibir mensajes en correo electrónico o redes sociales de dudosa procedencia.

Ilustración 19. Infografía de propagación del malware



Fuente: Elaboración propia.

En la ilustración 20 se encuentra una infografía con información importante, la cual les permitirá identificar correos fraudulentos, o con archivos maliciosos que pueden ser enviados a la entidad con el fin de realizar ingeniería social y por medio del phishing engañar a personas con bajos conocimientos informáticos o personas incautas que aun creen en ofertas y dinero fácil.

Ilustración 20. Infografía identificación de correos maliciosos

Fuente: Elaboración propia.

7 CONCLUSIONES

- Los procesos de seguridad de la organización en análisis se modernizaron de manera proporcional a los posibles ataques que se podrían generar en los equipos y redes de la empresa. El gobierno corporativo de la entidad destinó recursos suficientes para modernizar aspectos como los sistemas operativos obsoletos y que no contaban con actualizaciones, así como algunos softwares que no tenían soporte del fabricante documentado. Además fue posible llevar a cabo una exploración completa de los dispositivos de la entidad, así como los elementos que soportan la red, realizado cambios a la infraestructura de las conexiones, router de última generación y otros dispositivos que hacen parte de la red, con el apoyo de un equipo técnico que, por medio de auditorías externas lograron comprobar brechas de seguridad tales como, puertos abiertos no utilizados en los equipos los cuales se convierten en la puerta de entrada de los atacantes. Por lo tanto, el alcance de los objetivos, así como la implementación de herramientas y dispositivos de última tecnología que protegen la red de ataques, se convirtió en uno de los logros alcanzados por parte del departamento de las tecnologías de la información de la entidad.

- A través del escenario controlado, diagramas y pruebas realizadas en algunos dispositivos de la organización objeto de análisis, se logró demostrar ante la mayoría de los funcionarios, los aspectos devastadores de este malware, que no conforme con secuestrar archivos, fotografías, documentos e información de alto valor, en muchas ocasiones termina ocasionando daños irreversibles a los equipos de cómputo y en el peor de los casos, infectando a varios dispositivos de la red de la cual hace parte.

En el primer caso se logró demostrar que, a través de las técnicas de Ingeniera social, con base en engaños y mensajes fraudulentos, utilizando el correo electrónico, con archivos adjuntos que simulan ingresos a las cuentas bancarias de los funcionarios a través de Pay Pal o multas del tránsito, muchos funcionarios incautos, descargaron el malware, causando el bloqueo del sistema operativo por el método del malware WannaCry.

El segundo caso, se efectuó en un computador propiedad de un funcionario conectado a la red de la entidad, el cual no hacía parte del inventario de la empresa. Este dispositivo además de tener un sistema operativo desactualizado no contaba con un software antivirus vigente. Este funcionario fue engañado mediante la técnica de ingeniería social de Phishing, al momento de intentar comprar una póliza de seguros para vehículos, fue víctima del robo de datos sensibles como usuarios, contraseñas; información que luego utilizó el atacante para implantar un troyano el cual otorgó privilegios para acceder a la red de manera fraudulenta e infectar otros dispositivos, para obtener información que pudiera generar ganancias o secuestrar los datos para posteriormente cobrar por desencriptar la información.

- Se propuso realizar capacitaciones constantes a personal ajeno al área de las tecnologías de la información, pero que debido a sus funciones se relaciona con ella, con el fin de brindar información oportuna de los diferentes métodos y vectores de ataque y lograr por medio de la prevención, no ser víctima de los ciberdelincuentes a través de la ingeniería social, descarga de archivos con software malicioso, o sitios web inseguros visitados. De igual forma, se realizó un escaneo con el equipo de las TI de la entidad, para establecer por medio de herramientas de penetración y pruebas, las posibles vulnerabilidades en cuanto a puertos abiertos y otras anomalías.

8 RECOMENDACIONES

- Realizar copias de respaldo constantes a través de una nube segura y de manera local, con personal calificado. Si la entidad es víctima de ataque, se debe desconectar los equipos informáticos infectados de la red local, Así mismo, es necesario realizar un formato completo del disco duro. Posteriormente, un equipo de expertos en tecnologías de la información de la entidad utilizará una de las copias de seguridad para recuperar la información, permitiendo continuar con los procesos laborales para los cuales estaba instalado este equipo en el área o entidad. Por último, los ciberdelincuentes perderán las posibilidades de adquirir ganancias, puesto que no recibirán ningún dinero por el rescate de la información.

- Es importante que el gobierno corporativo realice una actualización de sistemas operativos a su última versión, instalación y actualización de software ofimáticos y otros, dejando el antecedente en el área informática que esta clase de vacíos o brechas tecnológicas pueden ser aprovechadas por los ciberdelincuentes.

- El antivirus es parte fundamental de la seguridad informática, cabe aclarar que las licencias de pago, son mucho más efectivas ya que contienen mayores filtros de protección contra diferentes tipos de amenazas, entre ellas el ransomware, por esto es necesario que el área de informática realice un seguimiento constante a este tipo de software para asegurar su vigencia y verificar que tipos de ataques ha recibido la organización y reforzar de esta manera, si es necesario, posibles vulnerabilidades.

BIBLIOGRAFÍA

AZIZOV, Danís. [Sitio web]. Arquitectura DMZ Perimetral: una implementación corporativa. 2020. [Consultado el 17 de octubre de 2022]. Disponible en: https://ddd.uab.cat/record/231488

Betech, [Sitio web]. Detectada una nueva estafa phishing usando correos de Pay Pal. 2023. [Consultado el 23 de enero de 2023]. Disponible en: https://as.com/meristation/2019/05/14/betech/1557870025_055503.html

CASTRO, Martha Irene Romero, et al. Introducción a la seguridad informática y el análisis de vulnerabilidades.2018. [Consultado el 18 de octubre de 2022].

COYLA JARITA, Yony. [Sitio web]. Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión–Filial Juliaca. 2019. [Consultado el 19 de octubre de 2022]. Disponible en: http://hdl.handle.net/20.500.12840/2002

DEN, EN, [Sitio web] et al. Informe De Amenaza Cibernética De Sonicwall. 2021.pag. 31[Consultado el 28 de octubre de 2022]. Disponible en: https://www.sonicwall.com/es-mx/2022-cyber-threat-report/ .

ESET, [Sitio web] Shadow IT: Qué es y cuáles son los riesgos que puede causar a una empresa. 2022. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.welivesecurity.com/la-es/2020/08/20/shadow-it-que-es-riesgos-puede-causar-empresa/

ESET, [Sitio web]: Qué es un ataque de *Man-in-the-Middle* y cómo funciona. 2022 [Consultado el 11 de noviembre de 2022]. Disponible en: *https://www.welivesecurity.com/la-es/2021/12/28/que-es-ataque-man-in-the-middle-como-funciona/*

FUNCION PUBLICA**.** Decreto 1377 de 2013.2022. [Consultado el 28 de octubre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

GUTIÉRREZ TORO, Dayro Luis, et al. Amenazas cibernéticas y su impacto en las organizaciones del sector industrial y servicios de Colombia en la última década. 2022. [Consultado el 28 de octubre de 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/31937 .

IBM, [Sitio web]: Qué es una superficie de ataque. 2022. [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.ibm.com/es-es/topics/attack-surface

IBM, [Sitio web]: ¿Qué es la ingeniería social? 2022 [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.ibm.com/es-es/topics/social-engineering

INCIBE [Sitio web]..Ransomware: una guía de aproximación para el empresario. 2022. p. 7 [Consultado el 11 de noviembre de 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

KASPERSKY, [Sitio web] Ciberseguridad que siempre está un paso por delante. 2022. [Consultado el 23 de enero de 2023]. Disponible en: https://www.kaspersky.es/

KASPERSKY, [Sitio web] Amenazas 2022. [Consultado el 23 de enero de 2023]. Disponible en: https://threats.kaspersky.com/en/threat/Trojan-Ransom.Win32.Wanna/

MAIMÓ, Lorenzo Fernández. Detección de botnets y ransomware en redes de datos mediante técnicas de aprendizaje automático. 2019[Consultado el 28 de octubre de 2022]. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=289541.

NARVÁEZ, Folker, et al. [Sitio web]. Revisión del estado del arte en técnicas para prevención y detección temprana de Ransomware. 2022. [Consultado 21 de octubre de 2022] Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/26932/2/RESUMEN%20ANALITICO%20EN%20EDUCACION%20RAE%20-%20FOLKER%20NARVAEZ.pdf

NO-MORE-RANSOMWARE, [Sitio web]. La batalla contra el ransomware.2021. [Consultado el 26 de octubre de 2022]. Disponible en: https://www.nomoreransom.org/

OPTICAL NETWORKS, [Sitio web]: ¿Qué son los vectores de ataque en ciberseguridad? 2023. [Consultado el 23 de enero de 2023]. Disponible en:https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/#:~:text=Vectores%20de%20ataque%20pasivos%3A%20com%C3%BAnmente,afectar%20los%20recursos%20del%20mismo

PÁRAMO, Angélica et, al. [Sitio web]. Servicio de Pentesting, basados en la propuesta de auditoría interna con la norma ISO 27001. *Investigación y Ciencia Aplicada a la Ingeniería*, 2021, vol. 4, no 24, p. 35-44. [Consultado el 23 de enero de 2023]. Disponible en: http://ojs.incaing.com.mx/index.php/ediciones/article/view/13/servicio

POLICIA DE COLOMBIA [Sitio web]. Tendencias cibercrimen Colombia 2019 – 2020, informe pág.15 [Consultado el 26 de octubre de 2022]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

POLICIA DE COLOMBIA [Sitio web]. Tendencias cibercrimen Colombia 2019 – 2020, informe pág.19 [Consultado el 26 de octubre de 2022]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

REYES, Javier Fernández. El virus" Wannacry". Quadernos de criminología: revista de criminología y ciencias forenses, 2017, no 38, p. 32-37 [Consultado el 23 de noviembre de 2022]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6147649.pdf

SECRETARIA SENADO COLOMBIA. Ley estatutaria 1581 de 2012. [Consultado el 28 de octubre de 2022]. Disponible en: http://www.secretariasenado.gov.co/constitucion-politica

SECRETARIA SENADO COLOMBIA. Constitución Política de 1991. [Consultado el 28 de octubre de 2022]. Disponible en: http://www.secretariasenado.gov.co/constitucion-politica

SECRETARIA SENADO COLOMBIA. Ley 1273 de 2009.[Consultado el 28 de octubre de 2022]. Disponible en: http://www.secretariasenado.gov.co/constitucion-politica

SILVA Diego. [Sitio Web]. Evaluación de Tecnologías UTM (Unified Threatment Management) y NGFW (Next Generation Firewall) para detección de vulnerabilidades en la red. 2020. [Consultado 22 de octubre 2022]. Disponible en:http://dspace.espoch.edu.ec/handle/123456789/14080

SGANDURRA, Daniele*, et al*. [Sitio Web]. Análisis Dinámico Automatizado de Ransomware: Beneficios, Limitaciones y uso para la Detección. 2016.[Consultado el 28 de octubre de 2022]. Disponible en: https://arxiv.org/pdf/1609.03020

Anexos

Lista de chequeo

Ítem	ESTRATEGIAS GENERALES	SI	NO
1	Plantear políticas de seguridad de información, soporte técnico, protección de la red.		
2	Plan de detección y soporte de sucesos (ataque de malware)		
3	Protocolo de evaluación inicial con informe del suceso.		
4	Análisis del mapeo del sistema TI.		
5	Actualización de sistemas de Información (software y firewall)		
6	Protocolo para actualización de firewall, configuración de cortafuegos para la protección de la red.		
7	Verificar puertos y protocolos		
8	Ejecutar herramientas que permitan mitigar los ataques con exploit.		
9	Bloquear dominios y servidores usando IDS/IPS.		
10	Desactivar Windows Script Host.		
11	Desactivar macros de ficheros o habilitar el modo lectura de adjuntos enviados por correo electrónico.		
12	Utilizar VPN (Virtual Private Networking), para la recepción y envió de información sensible.		
13	Plantear políticas para el uso de contraseñas.		
14	Deshabilitar usuarios que ya no trabajen en la empresa		
15	Plan de capacitaciones para prevención contra ataques ingeniería social y fishing.		
16	Realizar copias de seguridad, físicas y con soporte a la nube		