OFICINA DE POSGRADOS

Tema:

GUÍA DE BUENAS PRÁCTICAS PARA PREVENIR Y REACCIONAR ANTE UN ATAQUE DE RANSOMWARE

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de Investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Ángel Mauricio Salinas Zambrano

Director:

Mg. Paul Fernando Bernal Barzallo

Ambato – Ecuador

Noviembre 2023

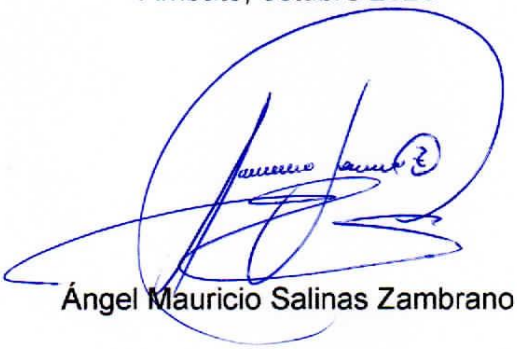
DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ÁNGEL MAURICIO SALINAS ZAMBRANO**, con cédula de ciudadanía **1804242756**, autor del trabajo de graduación titulado: "GUÍA DE BUENAS PRÁCTICAS PARA PREVENIR Y REACCIONAR ANTE UN ATAQUE DE RANSOMWARE", previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la **OFICINA DE POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, octubre 2023



Ángel Mauricio Salinas Zambrano

CC. 1804242756

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

GUÍA DE BUENAS PRÁCTICAS PARA PREVENIR Y REACCIONAR ANTE UN ATAQUE DE RANSOMWARE

Línea de Investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Ángel Mauricio Salinas Zambrano

Paúl Fernando Bernal Barzallo, Ing. Mg. f._____

CALIFICADOR

Verónica Maribel Pailiacho Mena, Ing. Mg. f._____

CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato - Ecuador

Octubre 2023

DEDICATORIA

El presente trabajo está dedicado en primer lugar a Dios, que es mi fortaleza y pilar fundamental de mi vida.

A mis padres, Ángel y Margarita, quienes han creído en mi y han realizado todos los sacrificios necesarios para que nunca me falte nada, los amo inmensamente.

De manera especial dedico este trabajo, a mi esposa Tannia quien siempre me brinda su amor incondicional y está conmigo apoyándome en cada momento de mi vida, a mi hijo Maury Andrés quien es mi fuente de inspiración y lucha, pues me ha enseñado que el amor es un sentimiento indescriptible, que contigo aprendo cada día a ser padre, te lo dedico para que siempre te sientas orgulloso de mi y sepas que todo este esfuerzo requiere un sacrificio para conseguir algo en la vida.

A mis hermanos Franklin, Freddy y Mariela quienes con su ejemplo han sabido mostrarme el camino correcto para seguir adelante en mis proyectos.

Para Anita y Gilbertito, quienes siempre creyeron en mí, pero en especial para ti Gilbertito que desde el cielo sigues siendo una fuente de inspiración.

RESUMEN

Los ataques de Malware, se han convertido en una amenaza global para las organizaciones, causando pérdidas millonarias, explícitamente los de tipo *Ransomware*, los cuáles secuestran la información y tienen como finalidad la extorsión. Estos ataques provocan la pérdida y secuestro de información a nivel mundial, que según el sitio web oficial del Instituto de Investigación Independiente de Alemania (AV-Test), las estadísticas de software malicioso muestran un aumento de 450.000 programas maliciosos diariamente, lo que se convierte en pérdidas económicas millonarias y que representan un valor aproximado de 6 mil millones de dólares anuales a nivel global, por lo tanto, evaluar la efectividad de los métodos que utilizan las empresas para prevenir este tipo de ataques resulta importante. El objetivo general del trabajo de titulación es elaborar una guía de buenas prácticas para prevenir y reaccionar ante un ataque de *ransomware*, con un tipo de investigación exploratoria y no experimental y con un enfoque cualitativo con información recolectada en bases de datos académicas y repositorios de conocimiento. Una vez elaborada la guía de buenas prácticas ante un ataque de *ransomware*, se espera presentarla para que esta sea sujeta a una evaluación de un experto en seguridad.

Palabras claves: malware, ransomware, prevención, reacción, seguridad

ABSTRACT

Malware attacks have become a threat for targeted organizations, leaving them with huge economic losses, especially Ransomware attacks, as they hijack information and demand a ransom payment as extortion. Ransomware attacks cause losses by hijacking information worldwide. According to the statistics from the German Independent Research Institute (AV-Test) malware attacks on websites have increased and there are 450,000 malicious programs daily. This represents an approximate value of 6 billion dollars of annual losses globally; therefore, assessing the effectiveness of methods used by companies to prevent this type of attack is important. The general objective of this thesis is to develop a guide of good practices to prevent and react to a Ransomware attack by following exploratory research rather than an experimental one. It will have a qualitative approach by collecting information from academic and knowledge databases. Once the guide of good practices for Ransomware attack has been created, it is expected to be presented and an evaluation could be conducted by a security expert.

Keywords: malware, ransomware, prevention, reaction, security

INDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El aumento en los ataques de Ransomware a nivel mundial, se han convertido en una de las amenazas más importantes en la actualidad, puesto que los más recurrentes son los de cifrado de archivos, de manera que la cantidad de personas y organizaciones afectadas, tienen que acceder a pagar cantidades de dinero que aumentan de acuerdo a la información, que se necesita recuperar por este motivo es necesario contar con las herramientas adecuadas que permitan mitigar o neutralizar estas amenazas.

La información ha sido siempre importante para la sociedad, más aún si en la actualidad es considerado un activo de vital importancia estratégica, debido a que, se ha digitalizado y depende de equipos de telecomunicaciones y de cómputo para su transmisión, procesamiento y almacenamiento. Según Baidal et al. (2021) los ataques de Ransomware han evolucionado hasta convertirse en uno de los principales motores de ataque a las empresas y usuarios en general, muchas de las veces es imposible revertir el daño causado por este tipo de Malware, debido a que por un lado es un locker-*ransomware* el cual está dirigido a bloquear al acceso a una estación de trabajo para no poder utilizarla, y por otro lado el crypto-*ransomware* el cuál cifra los archivos para hacerlos inaccesibles a las víctimas.

En la actualidad existen soluciones que permiten disminuir este tipo de incidentes, pero no garantizan la seguridad en su totalidad, debido a que todas las amenazas de tipo zero-day utilizan nuevas técnicas de ataque que les permiten vulnerar las infraestructuras de seguridad en una organización, todo esto porque no existen aún registros de ellos y plantean la generación de nuevas soluciones, las cuales están enfocadas en el usuario final, por ejemplo, antivirus, firewalls, proxys, sistemas antispam, entre otras.

Aun así, esta constante aparición de nuevos ataques de tipo Ransomware mejoran cada día sus técnicas de ocultamiento, dificulta así la prevención y detección de este

tipo de amenazas, aún el software especializado más actualizado, se ve poco eficaz frente al uso inadecuado de las funciones que presentan los sistemas informáticos por parte de los usuarios. El impacto que esto produce a nivel mundial según AV-TEST - The Independent IT-Security Institute *Malware | AV-TEST* (2021), dedicado a la seguridad de la tecnología, cada día, se producen más de 450.000 nuevos programas maliciosos.

Según el Comercio en su edición digital del 29 de julio de 2021 publica Ortiz (2021): "Solo durante 2020, según ESET, en Ecuador hubo más de 51 mil registros relacionados con cryptominers (malware utilizado para la minería de criptomonedas), alrededor de 140 mil detecciones de exploits (código utilizado para aprovechar vulnerabilidades en software), cerca de seis mil detecciones de *ransomware* (malware para el secuestro de información) y casi ocho mil detecciones de spyware (software espía), como datos de algunos tipos de software malicioso."

Como muestra de la problemática que representan estas amenazas en el Ecuador, el Municipio de Quito fue objetivo de un ataque de *Ransomware* de tipo BlackCat según lo informó su director de Tecnologías de información Franz Enríquez Pozo, en la edición digital de diario el Comercio del 22 de abril del 2022: "Ante la Comisión de Conectividad, él determinó que el malware que ha inhabilitado varios servicios es de tipo BlackCat. Se trata de un *ransomware* que empezó a circular desde finales del 2021 a escala mundial y que, se encuentra entre los más agresivos de este año." Así mismo mencionó: "el direccionamiento de este ataque era dejar inservible la infraestructura y dejar inservible la información con la que cuenta el Municipio. Añadió que BlackCat estaba orientado a encriptar la información; a encriptar las máquinas virtuales". (Ortiz, El Comercio, 2022)

Ante la problemática que vive el mundo con los ataques de malware, la idea a defender en el presente proyecto es conocer si con la creación de la guía, se mejora la prevención y reacción ante un ataque de tipo Ransomware, esto puede ayudar a

minimizar vulnerabilidades, fortalecer la seguridad y ejecutar acciones de respuesta rápida.

Para cumplir con lo propuesto en el párrafo anterior, se pretende que con la elaboración de una guía de buenas prácticas para prevenir y reaccionar ante un ataque de Ransomware, las organizaciones y personas mejoren la seguridad de su información. Dentro de la elaboración de la guía, se procede con la ejecución de las siguientes actividades: analizar el estado del arte actual ante los ataques de tipo Ransomware, diagnosticar las técnicas y prácticas existentes para la detección y prevención, aplicar una metodología de recolección documental para la elaboración de la guía, finalmente, presentarla ante un profesional afín al área de seguridad de la información, para que pueda cualificar la utilidad de la misma.

Para la recolección documental, se basa en la revisión de libros, artículos y fuentes de información comprobada, para determinar las mejores prácticas en temas de prevención de ataques de malware, todo esto sirve para la fundamentación teórica y la elaboración del estado del arte, también, se plantea utilizar una Metodología de Investigación Cualitativa, puesto que parte del descubrimiento de ideas y conocimiento en un tema que es aún desconocido o poco estudiado, la cual permite evidenciar a través de la elaboración de la guía los posibles mecanismos que mitiguen las vulnerabilidades a las que están encuentran expuestas las organizaciones, así el resultado final es una serie de buenas prácticas que permitan prevenir y reaccionar ante este tipo de ataques, mas no mitigarlos en su totalidad debido a que las variantes de malware, se hacen más numerosas de manera diaria y sus técnicas de ocultación tienen mayor efectividad.

El presente proyecto, se basa en la necesidad de entender la estructura y el comportamiento de un malware, por lo cual a través del uso de una estrategia de análisis dinámico en palabras de Gonzalez & Hayajneh (2017), se obtiene información de los archivos infectados en el sistema operativo, los cambios en el registro, las conexiones de red que llegan a escalar, entre otras. Para poder detener el impacto

que producen los ataques de malware, específicamente los de tipo *Ransomware*, se requiere comprender su comportamiento y las técnicas que utilizan en sus diferentes fases, logra así que los Analistas de Seguridad ejecuten acciones y controles en aquellos archivos que evidencien un comportamiento de malware.

Ecuador es uno de los países que ha sido víctima de los ciberataques, por tal motivo es fundamental contar con una infraestructura tecnológica que permita brindar una respuesta contra este tipo de incidentes de seguridad, proponer el desarrollo de una guía en la cual permita tomar las medidas orientadas a las buenas prácticas del día a día, por ejemplo, la instalación de listas blancas de correo, no abrir enlaces seguros o descargar archivos adjuntos sospechosos, bloquear *plugins* de navegadores, capacitación a empleados, actualizaciones de seguridad en sistemas operativos y equipos, programas de detección de malware, respaldos de información, entre otros.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1 Seguridad Informática

Desde la perspectiva que “la seguridad de la información tiene por objeto proteger a los sistemas informáticos de las amenazas a los que están expuestos, la aplicación de medidas de seguridad se realiza de manera planificada y racional, para evitar dirigir esfuerzos e invertir recursos en áreas que no lo requieren” (Gil & Gil , 2017, pág. 193). Cabe mencionar que los incidentes de seguridad que, se presentan alrededor del mundo han hecho que las organizaciones tomen conciencia de la importancia en la administración de riesgos para contrarrestar el riesgo informático.

Según Quiroz & Macías (2018), la seguridad informática tiene como objetivo principal mantener un riesgo mínimo de los recursos informáticos para garantizar la continuidad de las operaciones de una organización y administrar adecuadamente el riesgo informático.

Cabe indicar que los sistemas de detección de intrusiones forman parte de las herramientas indispensables para salvaguardar la información y datos, los cuales han adquirido una mayor importancia en los diferentes modelos y estrategias defensivas.

Ciberseguridad

La ciberseguridad es “la protección y defensa del ciberespacio y ciberataques, donde ciberespacio es el dominio global de propagación de información basado en infraestructuras de redes de comunicaciones independientes y sistemas de computación; y los ciberataques son vulneraciones de la seguridad de la información haciendo uso del ciberespacio” (Maestre, 2018)

Es así que la Ciberseguridad, se refiere a las medidas y técnicas utilizadas para proteger los sistemas informáticos y los datos de amenazas como ataques de *malware,*

involucra el uso de firewalls, encriptación, autenticación y políticas de acceso para garantizar la seguridad de la información.

Ciberespacio

Los ataques informáticos hacen uso de las debilidades de seguridad que presentan las diferentes infraestructuras de red, logra así acceder y manipular la información de la víctima, incluye la posibilidad de copiar, borrar o alterar su contenido. Estos ataques, se aprovechan de las vulnerabilidades que son comunes en la mayoría de las estructuras cibernéticas, como las redes sociales. (Machín, 2016, pág. 53)

El ciberespacio es así un entorno digital donde convergen personas, sistemas, dispositivos, sitios de interacción social, entre otros; se encuentran expuestos a riesgos y amenazas que necesitan ser mitigados a través de medidas de seguridad adecuadas.

Vulnerabilidades o riesgos de la información

Según Parra & Yánez (2017) citado por Lara (2019) “Las vulnerabilidades son puntos débiles en la seguridad de un sistema informático o de un proceso, a través de estos se presentan cierto tipo de amenazas que ponen en peligro la confidencialidad, integridad y autenticación de la información” (pág. 14).

Malware

Según las palabras de Oldfield & Borghello (2008) citado por Mata & Guevara (2010), mencionan que el Malware es uno de los principales riesgos de la ciberseguridad, pues tiene sus raíces en los comienzos de la era de la computación. En 1951, John Louis Von Neuman, un destacado matemático húngaro, estableció los fundamentos de la auto propagación, idea que tuvo miles de aplicaciones beneficiosas en favor de la

ciencia, como por ejemplo el modelado y simulación de sistemas, pero también tuvo una aplicación muy negativa, el malware. (pág. 58).

Según Correa et al. (2016) los virus poseen otra característica adicional, aunque ésta no siempre es indispensable, y esa es la de causar daño a la información y/o hardware.

Existen infinidad de programadores de virus, todos difieren entre sí por su objetivo, el tipo de infección, el comportamiento, así como el alcance de ataque. Se subestiman las soluciones técnicas, minimiza las acciones preventivas, finalmente, el usuario continúa desprotegido y no previene posibles ataques y con ello la pérdida de la información.

Se considera fundamental indicar que existen varios tipos de malware, a continuación, se mencionan los más importantes que según las palabras de Aranton (2008) los clasifica de la siguiente manera:

Tabla 1. Tipos de Malware

TIPO DE MALWARE	DEFINICION
Virus Convencionales	Programas maliciosos con capacidad de reproducirse, se encuentran en archivos ejecutables con extensión ".exe"; su objetivo es dañar a los equipos que logran acceder, borran archivos, bloquean el uso de programas, ejecutan mensajes en pantalla entre otras acciones que interrumpen.
Troyanos	Son aplicaciones que esconden un código malicioso el cual, se activa al instalar el programa principal; recopila información privada para terceros, abre vías de acceso "traseras" que permiten el control del equipo de manera remota, se ejecutan en el usuario instala el programa huésped.
Gusanos	Son programas que ocultos en correos electrónicos, se ejecutan automáticamente, y reenviarse sin autorización del usuario a las direcciones de correo electrónico que aparezcan en la agenda.
Dialer	Son programas, que se generan mediante conexiones telefónicas no solicitadas dan dar lugar a facturas con costos elevados. Se dan solo en conexiones a través de modem (no en ADSL).
Backdoor	Se ejecuta mediante la configuración del equipo informático que permite dejar abierta una puerta de entrada al ordenador, así el atacante espía datos personales copiar archivos, instalar programas o tomar el control remoto del equipo.
Exploit	Son programas que envían programas dañinos, o permiten espiar información privada y, se ejecutan cuando existe un fallo en la seguridad.
Keylogger	Software desarrollado para capturar lo que el usuario escribe en el teclado del sistema e incluso algunos registran movimientos del mouse y cualquier otro elemento de entrada, esta información la recibe el desarrollador para utilizarla con fines de ingresar a sitios o contraseñas que digita la víctima.
Spyware	Son programas, que se instalan al mismo tiempo que otros, copian información, aficiones, historiales de navegación sin consentimiento del usuario.
Ransomware	Es una aplicación que retiene o secuestra la información del usuario o realiza restricciones al sistema para luego solicitar al usuario un pago económico por el rescate de la

	información, este es el tipo de malware sobre el cual, se enfoca este trabajo.
Botnet	Es un grupo de sistemas informáticos infectados por un código malicioso, esto permite al atacante controlar el equipo para realizar determinadas como el envío masivo de spam o masivos ataques de denegación de servicio (DDoS).
Rouge	Son programas informáticos (o sitios web) que no son lo que dicen ser, estos generalmente, se anuncian como software de seguridad gratuitos (antivirus que garantizan eliminar falsas infecciones detectadas) y al ser ejecutados por el usuario, instalan otro tipo de malware en el sistema informático infectado.
Adware	Son programas que se ocultan en otros y se instalan conjuntamente; con el objetivo de mostrar publicidad

Fuente: Arantón (2008)

1.2 Ransomware

Según Moreno et al. (2019), el *ransomware* es una de las nuevas amenazas a la que somos vulnerables. Principalmente, se encuentran amenazados los sistemas operativos de escritorio Windows, lo que pone en riesgo la seguridad personal, también, los dispositivos móviles y microcomputadores expuestos al robo, fuga de información y secuestro de los datos.

Cabe mencionar que decenas de miles de usuarios, se ven afectados por la pérdida de información, fuga de datos; existe un gran número de empresas, personas con altos perfiles y organismos públicos que sufren este tipo de ataques e implican un riesgo mayor en cuanto a pérdida y sigilo de la información.

“El *ransomware* ha evolucionado a través de la implementación de técnicas criptográficas que utilizan algoritmos de cifrado asimétrico. Además, utiliza la ingeniería social como principal método de propagación de malware, en este trabajo se presenta el análisis del *ransomware*, los lineamientos de detección y prevención, además, buenas prácticas y recomendaciones” Moreno (2019).

Clasificación de Ransomware

De acuerdo con Moreno et al. (2019), se clasifica:

- **Por el comportamiento**:

"Bloquea el acceso al sistema operativo, a su vez cifra archivos y datos del sistema operativo infectado".

- **Por la tecnología**:

FAKEAV: Malware que engaña a los usuarios a comprar antimalware falsos, mediante mensajes falsos con resultados falsos.

Ransomware de compresión: Programas que permiten comprimir archivos de ciertos formatos como .DOC, .EXE, .DLL, .PPT, deja una nota de la extorsión con la solicitud del pago.

SMS Ransomware: Programas que envían continuamente una notificación de extorción mientras el usuario no efectué el pago con el objetivo de infectar el MBR de un sistema vulnerable y no permite que el sistema operativo inicie.

Police Ransomware: Personifica las autoridades de autoridades, muestra notificaciones y engaños a la víctima con avisos de actividades ilícitas.

Reconocimiento de anomalías en la detección de ransomware

"El reconocimiento de anomalías juega un papel esencial en la lucha contra esta amenaza, permite descubrir sus procesos de enumeración de la víctima, cifrado de activos, y eliminación. Por lo tanto, se trata de un problema emergente que plantea otro interesante escenario emergente de monitorización" (Maestre, 2018, pág. 218).

El monitoreo constante es una tarea que debe realizarse de manera diaria, pues permite que la detección de algún posible cambio en el tráfico de la red,

comportamientos en equipos de usuario, entre otros medios, se pueda establecer mecanismos de reacción ante un posible ataque.

Esquema de Funcionamiento

“Durante el análisis dinámico del *ransomware* se observa que tienen una estructura y comportamiento similares a otros tipos malware, como troyanos o gusanos que contienen técnicas de ofuscación, similitud en los *payload*, auto replicación, técnicas de ocultamiento, persistencia, creación de registros, creación de carpetas, generar tráfico en red y cifrado.” Osorio (2019).

Si bien es cierto el comportamiento del *ransomware* es similar al de otros tipos de malware, sin embargo, es realmente importante conocer su esquema de funcionamiento.

Según Osorio (2019), para la creación de archivos en el registro de Windows que permiten al *ransomware* funcionar de manera persistente, se requiere alterar y modificar el registro de Windows en donde, se almacenarán las cadenas de registro y para cuando, se reinicie el ordenador y mantenga la posibilidad de auto ejecutarse para poder tener control del equipo. Los archivos del registro, comúnmente utilizados por los *ransomware* son:
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit

Cabe indicar que, con el objetivo de crear su propia estructura de carpetas, se encuentra incluida en cada *ransomware*, como: C:\DocumentsandSettings \user\Start Menu\Programs\Startup.

El *ransomware* habilita o deshabilita los servicios del sistema para dañar y persuadir al sistema operativo. Busca los servicios y procesos que detectan, para posteriormente habilitar o deshabilitarlos (Osorio, 2019).

Los *ransomware* generan una entrada de registro en las siguientes rutas:
HKLM\SYSTEM\CurrentControlSet\services
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Services
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Services\Once
Finalmente, cuando ya, se generó las llaves, se enviarán hacia un centro de comandos y control (C&C), en donde, se opera y envían las instrucciones u otros datos al malware que está en el equipo víctima; algunas funciones del servidor de C&C es que el malware, se actualiza con sus nuevas versiones desde el servidor, reciben la clave para cifrar desde el servidor y es utilizado en *botnets* para el control de equipos *zombies*.

Ciclo de vida del ransomware

Reconocimiento: Como primer paso requiere reconocer los sistemas atacar y buscar los recursos, vulnerabilidades y estrategias que se encuentren al alcance del desarrollador para comenzar con la codificación (Villegas , 2018).
Este reconocimiento permite elaborar técnicas de ingeniería social para poder llegar a los usuarios, logrando así tener información importante que permite agregar nuevas características a los *ransomware.*

Armamento: “Una vez identificado el entorno que se va a asaltar y las vulnerabilidades que se aprovechan, hay que buscar los recursos necesarios para lograr los objetivos que tiene el Malware y construirlo para ser difundido. Los objetivos más comunes suelen ser: Ocultación, propagación, escala de privilegios, robo de información” (Villegas , 2018, pág. 19).

Actualmente el robo de información es el más común los objetivos, pues ha permitido generar recompensas económicas que ayudan a seguir creando nuevas variantes con mejores técnicas.

Envío: con el Malware ya construido y listo para funcionar empieza la difusión. A pesar de que el programa cuente con gran capacidad de infección y replicación, a grandes rasgos requiere de un foco de infección para la difusión ir a en función de la forma de propagación para su desarrollo (Villegas , 2018).

Las técnicas de ingeniería social son las más efectivas para difundir el *ransomware,* pues llegar de manera común a usuarios sin experiencia que no han sido capacitados en cuanto a temas de seguridad de la información.

Explotación. Esta fase de explotación funciona debido a algún fallo de diseño, actualización de seguridad, medidas de prevención que no haya tomado la víctima. Cuando detecten las vulnerabilidades estas serán explotadas y tomarán control del código que, se ejecuta en la maquina y todo el sistema.

Instalación. De acuerdo con Villegas (2018), cuando el sistema ha sido infectado y explotado, se trata de mantener el control sobre el sistema asaltado y establecer una vía de comunicación. Y a pesar de que las vulnerabilidades que han permitido la intrusión se reparen, el Malware opera. Los métodos más comunes para mantener esa comunicación son el uso de Troyano o Covert Channel.

Control y envío de órdenes. Al mantener el canal de comunicación desplegado y el Malware instalado, ya se toma el control sobre el sistema y opera e introduce distintos Software maliciosos (Villegas , 2018).

Acciones y objetivos. Una vez concluidos correctamente los pasos anteriores, el o los Malware comienzan a explotar los recursos del sistema en su tarea principal para empezar a obtener beneficio ya bien de los datos o de la capacidad de computación.

Un ejemplo común es el Malware que lleve a cabo operaciones de minería de criptomonedas aprovecha la capacidad de computación de las víctimas para contribuir en el proceso de Block-Chain, y así obtener beneficio económico (Villegas , 2018).

Reciclaje y/o Muerte. **"**El Malware puede entrar en un punto muerto y quedar completamente obsoleto, o adaptarse a los cambios acontecidos. En este punto puede, volver a la fase de reconocimiento y armamento, pero solo para la adaptación, o que ya no merezca la pena actualizarlo y sea más eficiente crear un nuevo proyecto desde cero para un nuevo fin" (Villegas , 2018, pág. 20)..

Ingeniería Social: Es fundamental indicar que la ingeniería social permite obtener información confidencial mediante la manipulación de usuarios legítimos. Esta técnica es utilizada por criminales o delincuentes computacionales, para tener acceso en sistemas diversos sistemas de información para realizar algún acto ilícito.

El phishing. Mediante mensajes supuestamente de origen conocido (spam spoofing) por plataformas diseñadas para enviar mensajes fraudulentos de correo electrónico, que se anuncian como provenientes de bancos u otros sitios legítimos para engañar a los usuarios con el objetivo de obtener datos financieros, datos personales o contraseñas.

1.3 Técnicas de detección y prevención para *ransomware*

De acuerdo con Osorio (2019), en la prevención y detección de *ransomware*, se busca desarrollar un esquema metodológico para la gestión de incidentes de malware.
Inicialmente, se probó mediante entornos controlados y el uso de herramientas forenses para realizar un análisis estático o dinámico del comportamiento del *ransomware*, además, ingeniería inversa determina las características más comunes y obtener resultados para tener una mayor comprensión de estos.

Arquitectura de Seguridad

El objetivo de la arquitectura de seguridad de la información es garantizar la seguridad de las Tecnologías de la información y salvaguardarla al mantener un nivel de riesgo muy bajo sobre los puntos críticos de la organización, una arquitectura bien diseñada incorpora medidas de protección en todas las capas de la red y sistemas, asegurando que existan barreras de seguridad para evitar la propagación y ejecución del ransomware. Además, permite una rápida respuesta ante posibles incidentes, facilitando la identificación y contención temprana de amenazas.

Al implementar soluciones como firewalls, sistemas de detección de intrusos, cifrado de datos y una política robusta de respaldo, la arquitectura de seguridad contribuye significativamente a reducir la superficie de ataque y minimizar el impacto de los ataques de ransomware, protegiendo así los activos y la integridad de la organización.

Gestión de Parches de Seguridad

Según Christopher M Frenz & Christian Diaz (2018) citado por Osorio (2019), actualizar el sistema operativo y las aplicaciones ayudan a proteger contra ataques de malware y *ransomware* debido a que en algunos casos, se aprovechan de las vulnerabilidades en el sistema operativo como en el caso de Wannacry, las actualizaciones automáticas corrigen errores o fallas en el sistema y se tiene cuidado con aplicaciones como Adobe Flash, Microsoft Silverlight y navegadores web.

WannaCry se propagó de manera global en mayo de 2017, este se aprovechó de un malware llamado EternalBlue, el cuál atacaba sistemas operativos Windows, sin embargo, Microsoft lanzó un parche de seguridad dos mesas antes del ataque de WannaCry, pero, debido a que varios equipos no estaban actualizados, se propagó rápidamente y afectó a 230.000 equipos en todo el mundo según datos presentados en el sitio oficial Kaspersky.

Aplicar los parches de manera oportuna, cierra posibles puertas de entrada para ataques maliciosos, reduciendo significativamente la probabilidad de sufrir brechas de seguridad, como ataques de *ransomware* o robo de datos sensibles. Además, los parches contribuyen a mejorar el rendimiento y estabilidad del sistema, asegurando un entorno más seguro y confiable para usuarios y organizaciones.

Honeypot File

Una manera sencilla para prevenir *ransomware* es con la creación de un *honeypot*, los cuales están diseñados para identificar el modo de operación del atacante. Esta herramienta flexible y su implementación no demanda costos altos. Sin embargo, representa múltiples ventajas para las empresas, logra identificar vulnerabilidades no conocidas y descubre riesgos de afectación en los sistemas.

Los *Honeypot* según las palabras de Mairh et al. (2011) se parecen a un sistema informático real, muestran datos y aplicaciones, a menudo son configurados en entornos virtuales o servidores en la nube, pero siempre aislados de la red principal, su objetivo es que sean vulnerados de manera intencional, dejando puertos abiertos, programas desactualizados, contraseñas débiles, entre otros.

Si el atacante logró encontrar el objetivo vulnerable, intentará lanzar el ataque y escalar privilegios, pero desconoce que existe un administrador del *honeypot,* quien está observando y analizando cada acción, recopilando datos importantes que permiten crear técnicas de prevención contra amenazas. Finalmente existen diferentes tipos, de investigación para desarrolladores, administradores de sistemas, o equipos azules, que pueden ser puestos en marcha en entornos emulados como por ejemplo en *sandbox* o a su vez en dispositivos reales, todo esto con la facilidad de que ya existen diseñados varios tipos de *honeypot* que contribuyen en la identificación de amenazas.

Indicadores de compromiso (IoC)

Según Lord (2017) citado por Osorio (2019), el indicador de compromiso son piezas de datos forenses cuyo objetivo en una red o en un sistema operativo es identificar una intrusión informática. Los IOCs comunes son firmas de virus y direcciones IP, hash MD5 de archivos de malware o urls o nombres de dominio de servidores de control y comando de botnet. Después de que los IOCs hayan sido identificados en un proceso de respuesta a incidentes e informática forense, son usados para la detección temprana de futuros intentos de ataque al usar sistemas de detección de intrusos y software antivirus. Algunos ejemplos de indicadores de compromiso a considerar son:

- Tráficos de red inusual
- Intentos repetidos de solicitudes a una BDD
- Cambios sospechosos en los archivos de registro
- Anomalías en privilegios de cuentas de usuario
- Solicitudes de DNS inusuales
- Solicitudes HTTP fuera de lo común

Documentar estos indicadores de acuerdo al giro de negocio de la organización es un aporte significativo en la detección y prevención de malware.

1.4 Prácticas de prevención de *ransomware*

Análisis de Comportamiento de Usuario (UBA – User Behaviour Analysis)

El UBA permite identificar actividades sospechosas, toma como base los comandos más frecuentes, aplicaciones que el usuario utiliza, la velocidad a la que trabaja, la rutina, las que permite identificar el comportamiento usual del usuario frente al comportamiento inusual del usuario. Ciertas empresas víctimas de *ransomware* como CTB Locker y Cryptolocker, utilizan como estrategia el análisis de comportamiento para evitar este tipo de ataques.

Se realiza un monitoreo de las actividades y patrones de comportamiento de los usuarios dentro de una red o sistema, esto en base a las funciones que desempeña, se crean perfiles de comportamiento normal para cada usuario, cualquier desviación significativa de estos patrones establecidos se identifica como un posible indicio de actividad maliciosa, entre ellas la propagación de ransomware. En algunos casos los ataques pueden ser internos, en consecuencia, es primordial conocer las funciones y actividades que los usuarios realizan.

Defensas en redes de próxima generación (NGN)

"Se trata de construir herramientas de software, o combinaciones de hardware y software, que cumplan con requisitos como la seguridad en el código, adecuado tratamiento de errores, empleo del paradigma AAA, protección ante ataques DoS y demás intentos de intrusión comunes, entre otros. Las soluciones de seguridad no introducen nuevas vulnerabilidades en el sistema o red" (Baluja & Anías, 2016, pág. 14).

La operación segura es considerada como uno los requerimientos que deben cumplir las redes de próxima generación (*Next Generation Networks*), y es fundamental porque menciona características que deben cumplir las herramientas ya sean de hardware o software, de tal modo que de acuerdo a Baluja et al. (2016) son: trabajo distribuído, escalabilidad, portabilidad, tecnologías avanzadas y administración centralizada, lo que permite que las redes de próxima generación garanticen transferencia basada en paquetes, capacidad de banda ancha con calidad de servicio, movilidad generalizada, esquemas de identificación de usuarios y dispositivos, entre otros.

Programas antivirus

Módulo de control. Mediante la técnica de verificación de integridad permite el hallazgo de cambios en los archivos ejecutables y zonas críticas de un disco rígido, así como la identificación de los virus. Esto significa que utiliza varias técnicas para la

detección de virus informáticos y de códigos dañinos, busca instrucciones peligrosas incluidas en programas para garantizar la integridad de la información del disco rígido.

Lo que significa que descompila o desensambla automáticamente archivos almacenados y tratar de ubicar sentencias o grupos de instrucciones peligrosas; así el módulo de control monitorea las rutinas mediante el acceso al hardware de la computadora. Al restringir el uso de estos recursos, por ejemplo, cuando se impide el acceso a la escritura de zonas críticas del disco o se evita que se ejecuten funciones para su formateo, se limita la acción de un programa (Armas , 2003).

Módulo de respuesta: Permite detener las acciones y bloquear la ejecución ante la presencia sospechoso de un virus mediante la función alarma que incluyen todos los programas antivirus y que advierte con un aviso en la pantalla.

Gestión de la Seguridad

De acuerdo con Maestre (2018) en la etapa de contextualización, se establece la tolerancia a riesgos del sistema de gestión de incidencias y las prioridades en la toma de decisiones. Las tareas de contextualización se alinearán con los objetivos de las empresas o el entorno de monitorización; en esta etapa, se establece las premisas iniciales y limitaciones del sistema, que se asumen antes de su desarrollo.

Por otro lado, la evaluación de riesgos “se centra en identificar las posibles amenazas dirigidas contra el sistema a proteger, el establecimiento de métricas que permitan valorar su impacto en base a los activos que se comprometan, y la definición del conjunto de contramedidas” (Maestre, 2018, pág. 44)

Posteriormente, se inicia la etapa de monitorización en la cual, se analiza y busca los intentos de intrusión o riesgos capaces de afectar la información. En este proceso, se compila información, se aplican métricas ya establecidas en la fase de evaluación de riesgos y analizan las consecuencias de las amenazas encontradas.

Finalmente, “la etapa de respuesta se activa una vez detectado un riesgo o cada cierto intervalo de tiempo. En ella se decide si aplicarán contramedidas, y en ese caso, cuales de ellas son las más apropiadas. Asimismo, esta tarea se encarga la elaboración de informes periódicos sobre el estado del sistema a proteger, además, si se detectan riesgos los comunica a los administradores de seguridad” (Maestre, 2018, pág. 44).

De acuerdo con lo anterior, se dice que la implementación adecuada de dichas fases en las organizaciones permite garantizar la confidencialidad, integridad y disponibilidad de los activos en los sistemas de información, también, para la prevención de riesgos de ciberseguridad, existen un sin número de herramientas y es necesario que las organizaciones tomen conciencias y gestionen eficientemente y de acuerdo a sus necesidades la implementación, mediante controles preventivos, políticas, y procedimientos adecuados.

CAPÍTULO II. METODOLOGÍA DE INVESTIGACIÓN

2.1 Metodología de Investigación

Para poder seleccionar de manera adecuada la Metodología a utilizar, es importante comprender cual es el resultado a obtener en el presente proyecto, por tal motivo, se ha considerado que para elaboración de la guía de buenas prácticas, es necesario reunir una evidencia documental de los ataques de tipo Ransomware, con el objetivo de poder hacer un análisis cualitativo y bibliográfico y en base al mismo obtener como producto final un manual práctico que nos permita realizar una prevención y reacción ante este tipo de ataques, es así, que se utiliza el Método Analítico Sintético.

Enfoque de la Investigación

Enfoque Cualitativo

De acuerdo a Vega et al. (2014) este tipo de enfoque, se basa en un esquema inductivo, dado que no utiliza un análisis estadístico, lo que busca es entender el entorno de un ambiente, conocerlo, analizarlo para así poder recolectar nuevos datos; permite realizar el análisis profundo de conceptos subjetivos, los cuáles son aclarados en base a la investigación a realizar, asimismo, en el proyecto se pretende obtener la mejor información relacionada a los ataques de Malware, específicamente los de tipo Ransomware, para así definir las mejores técnicas de prevención y reacción ante ataques de este tipo.

Método general de la investigación

Investigación basada en la literatura

Este tipo de Investigación es necesaria para aprender nuevos conocimientos o a su vez excluir investigaciones caducas, es uno de las más utilizados, puesto que nos permite encontrar una gran cantidad de información a través de diferentes fuentes, estas incluyen periódicos, revistas, libros, artículos relacionados, literatura o estadísticas publicadas por diferentes organizaciones, esto nos permite tomar dichas referencias para así tener una idea más clara del tema al revisar los artículos que hablen sobre Malware, específicamente los de tipo Ransomware.

Investigación basada en Casos de Estudio

Este tipo de investigación nos permite realizar un análisis cuidadoso de trabajos o casos ya existentes, o a su vez problemas similares a los planteados en el proyecto, para ello hay que basarse en que los temas principales coincidan con los del proyecto puesto que así serán de aporte al desarrollo del mismo. Dentro de esta etapa, se obtienen casos de estudio en los cuáles, se utilizan herramientas y técnicas para entender el comportamiento del Ransomware.

Método Analítico - Sintético

Para entender este tipo de Investigación, es importante definir que, se lo considera Analítico porque se encarga de descomponer o estudiar de manera minuciosa un tema para poder entenderlo, es Sintético, puesto que luego de realizar el estudio de las partes que fueron separadas de manera analítica, se encarga de sintetizarlas para obtener un conocimiento nuevo. Al aplicar este tipo de investigación al presente proyecto de desarrollo, se cataloga al Malware como un todo, donde, se separa al Ransomware para analizar los elementos que lo constituyen y como se relacionan para que logre propagarse de manera eficaz ante usuarios y organizaciones, el objetivo es entender su comportamiento y en base a ello sintetizar las mejores prácticas que permitan mitigar estos ataques.

2.2 Metodología de Desarrollo

Modelo Kanban

Según lo manifiesta Salhuana Albitres (2020), la Metodología Kanban permite mejorar el tiempo de desarrollo de un proyecto, mejorar su eficiencia a través de un flujo de entrega que limita la cantidad de trabajo en progreso a través de tableros de Kanban, en donde, se determinan las tareas a realizar, se las ubica en forma de tarjetas de manera que cambien de estado conforme avanza el proyecto desde su inicio hasta su finalización.

De acuerdo a Kanbanize (2021), se establece que esta metodología propone las mejores prácticas en base a los siguientes principios:

- **Visualizar el flujo de trabajo:** se refiere a identificar cual es el objetivo principal del proyecto, las tareas necesarias que ejecutarán para su finalización.

- **Eliminar las interrupciones:** en este principio, se requiere delimitar las tareas que están en proceso, de tal manera que, para arrastrar una tarjeta al siguiente paso o estado, existe disponibilidad.

- **Gestionar el Flujo:** en esta etapa, se trata de garantizar la velocidad y continuidad del movimiento de las tarjetas, por lo cual tener un flujo ininterrumpido de actividades disminuye el retraso.

- **Hacer Políticas Explícitas:** se enfoca en que, antes de iniciar con las tareas del proyecto, estarán bien definidas y comprendidas para poder entender su resultado final.

- **Circuitos de Retroalimentación:** se refiere a la revisión en sí de las tareas que deben ser ejecutadas para que sean de utilidad como modelo de retroalimentación continua.

- **Mejorar colaboración:** la idea de esta parte del proceso es que a través de la realización del proyecto, se logre una mejora continua con las tareas, que se han realizado para que cada una sirva de aporte a la consecución de la que sigue.

Proceso Kanban

Esta metodología, se basa en un tablero, que como primer aspecto define un flujo de trabajo, en el cuál todas las tareas definidas en el proyecto pasan por diferentes etapas como se observa en la Figura 1: por hacer, en curso y listo.

Figura 1. Tablero Kanban - Herramienta Kanban Tool

Fuente: Elaboración propia

Para conseguir lo propuesto, se ha definido que para el manejo del tablero de Kanban, se utiliza la herramienta *Kanban Tool*, la cual nos permite desarrollar proyectos ágiles, asimismo, tiene una versión gratuita y en la nube, que presenta como una de sus

funcionalidades los tableros Kanban, a continuación, se propone la ejecución de las siguientes tareas para la elaboración de la guía:

Tabla 2. Definición de Tareas

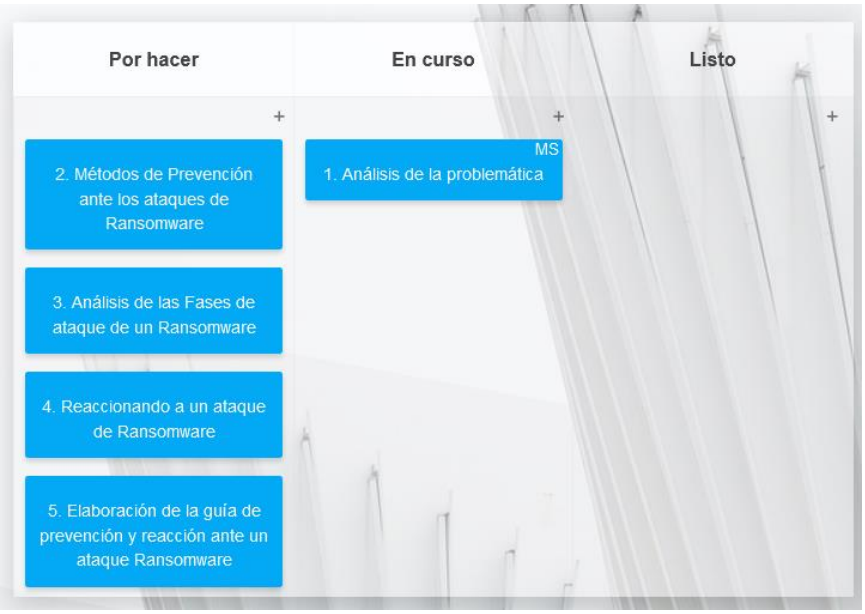
Tareas	Definición
1. Análisis de la Problemática	En esta parte se establece o realiza el reconocimiento del Ransomware como la amenaza y el potencial daño que ocasiona a las organizaciones.
2. Métodos de Prevención ante los ataques de Ransomware.	A través de medidas de prevención se logra mejorar la infraestructura de seguridad interna de una organización.
3. Análisis de las Fases de ataque de un Ransomware	Hacer un análisis de los pasos que sigue un *ransomware* para generar un ataque.
4. Reaccionando a un ataque de Ransomware	Identificar los pasos para reaccionar a un ataque.
5. Elaboración de la guía de prevención y reacción ante un ataque Ransomware	Materializar la guía que permita prevenir y reaccionar antes ataques de tipo *ransomware*.

Fuente: Elaboración propia

Tarea 1. Análisis de la Problemática:

Para iniciar según la metodología propuesta a través de la herramienta *Kanban Tool*, se empieza a mover esta tarea, a la columna en **curso** como muestra la figura 2:

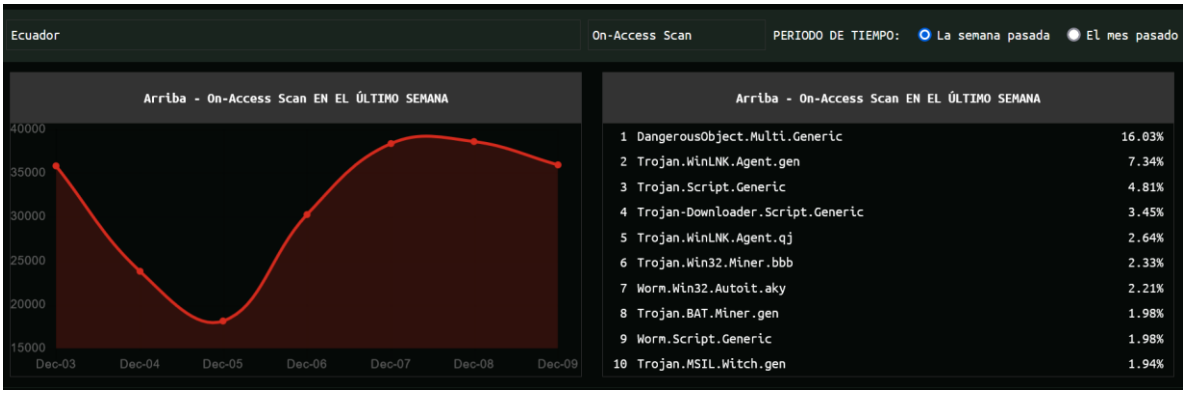
Figura 2. Tablero Kanban: Análisis de la Problemática - EN CURSO



Fuente: Elaboración propia

El mundo, se enfrenta diariamente a diferentes tipos de malware, específicamente los de *zeroday,* los cuáles provocan la mayor cantidad de ataques a nivel mundial, para entender esta problemática, se ha tomado una estadística en tiempo real del sitio web de *Kaspersky*, en donde nos muestra datos de Ecuador en cuanto a los tipos de ataque:

Figura 3. Análisis en tiempo real de amenazas de seguridad en Ecuador



Fuente: Sitio Oficial *Kaspersky* (https://cybermap.kaspersky.com)

Con la finalización de la presente tarea, es necesario moverla al estado **listo** en el tablero de Kanban:

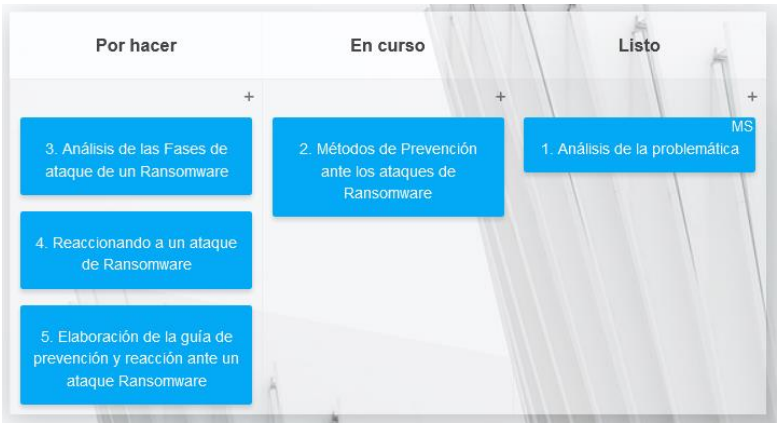
Figura 4. Tablero Kanban: Análisis de la Problemática - LISTO

Fuente: Elaboración propia

Tarea 2. Métodos de Prevención ante los ataques de Ransomware

En el tablero de Kanban, esta tarea pasa al estado **curso** como muestra la Figura 5:

Figura 5. Tablero Kanban: Métodos de prevención ante ataques *ransomware* - EN CURSO



Fuente: Elaboración propia

Para que un ataque de Ransomware sea exitoso, busca diferentes métodos que le permitan tener una puerta de ingreso hacia la víctima, por lo tanto, al tomar las palabras de Richardson & North (2017), los expertos coinciden en algunas recomendaciones para usuarios y organizaciones que permitan prevenir un ataque de este tipo:

Paso 1. Respaldos: Si la información está respaldada, no es necesario pagar por un rescate, pues es necesario restaurar dicho respaldo. Hay que considerar que estos respaldos estarán actualizados y son generados en algún equipo, que se conecte a la red solo para dicho propósito, o a su vez respaldos basados en la nube, todo esto debido a que los ataques de Ransomware son más sofisticados y no evidencian un contagio ante el usuario, así, en segundo plano siguen cifrándose los respaldos y se ubican en esa misma ruta.

Paso 2. Evitar los enlaces y archivos adjuntos de correo electrónico: el Ransomware utiliza como medio más común los ataques de Pishing o publicidad maliciosa para propagarse, por lo tanto, evitar abrir enlaces sospechosos es una

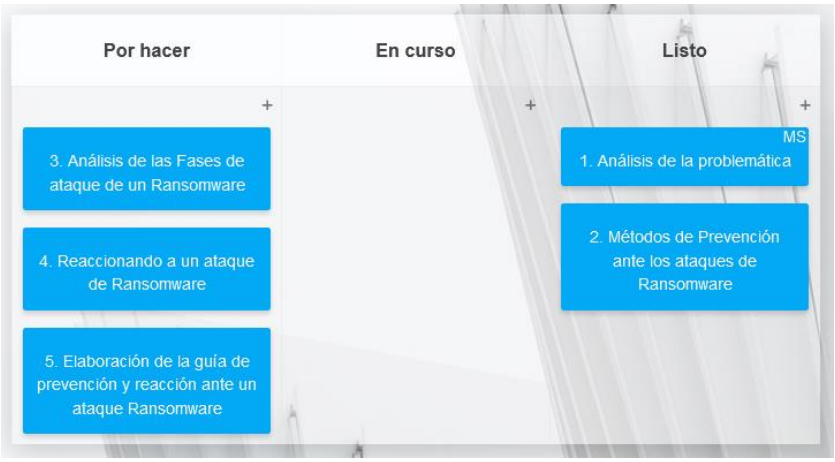
técnica de prevención básica pero imprescindible; en este contexto los bloqueadores de anuncios son un medio de protección, al igual que desactivar Java y JavaScript.

Paso 3. Parches y bloqueo: todo sistema operativo, navegador o software de seguridad de cualquier dispositivo, requiere estar actualizado, ser parchados los complementos como Java el cual permite visualizar el contenido en una web. Los privilegios mínimos son una estrategia adecuada de seguridad en usuarios finales, pues evita la instalación y uso de software innecesario.

Paso 4. Eliminar y Avanzar: una vez que un equipo ha sido infectado, el primer paso es separar dicho equipo de la red, si es necesario, se baja la red para evitar la propagación del Ransomware, de esa manera el avance de las operaciones de la organización, se reanudan en un tiempo menor.

Con la finalización de la presente tarea, es necesario moverla al estado **listo** en el tablero de Kanban

Figura 6. Tablero Kanban: Métodos de prevención ante ataques *ransomware* - LISTO

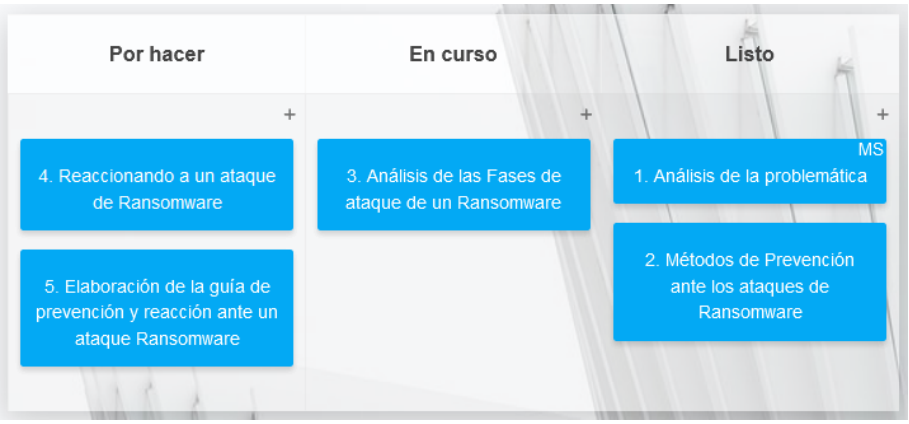


Fuente: Elaboración propia

Tarea 3. Análisis de las fases de ataque de un Ransomware:

En el tablero de Kanban, esta tarea pasa al estado **curso** como muestra la Figura 7:

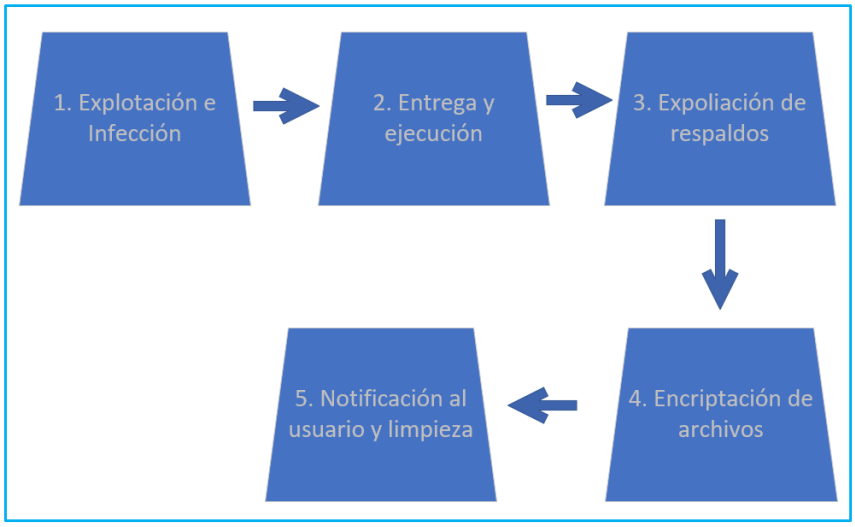
Figura 7. Tablero Kanban: Análisis de las fases de ataque de un *ransomware* - EN CURSO



Fuente: Elaboración propia

Según lo manifiesta Brewer (2016), independiente de que tipo de ataque, ya sea de distribución masiva o dirigida, es importante conocer las fases que atraviesa y al conocer los indicadores de compromiso adecuados, aumenta la probabilidad de mitigar o defenderse ante un ataque de Ransomware según muestra la Figura 8:

Figura 8. Tablero Kanban: Fases de ataque de un *ransomware* – EN CURSO



Fuente: Elaboración propia

Una vez, que se conocen las etapas de un ataque, es primordial describirlas, puesto que así, se comprende el enfoque que cada una tiene:

1. **Explotación e infección:**

El éxito de un ataque es que logre ejecutarse en el equipo de la víctima, para esto utiliza diferentes técnicas, pero la más común es a través del correo electrónico de phishing, también, puede ejecutarse por medio de un *exploit kit,* que es un grupo de herramientas que permiten explotar problemas de seguridad que poseen ciertas aplicaciones de software inseguras o que son obsoletas. Son la forma más común de infección los enlaces y archivos adjuntos maliciosos, los cuales envían a la víctima a una página o servidor que al aprovechar las vulnerabilidades del navegador para descargar y ejecutar el Ransomware.

2. Entrega y ejecución:

Una vez culminado el proceso de explotación, cuando la víctima accede al archivo o enlace infectado con *ransomware*, se ejecuta y da inicio a completar una serie de pasos obligatorios para recuperar la información, para el pago del rescate, se usa Bitcoin de manera más común, puesto que ofrece anonimato para los atacantes. La ejecución de este proceso dura algunos segundos, lo que depende de la latencia de la red, los ejecutables, se entregan por medio de un canal cifrado, y son colocados en la ruta de “APPDATA” o “TEMP” debido a que son carpetas que no son comunes revisar y son de bajo perfil del usuario.

Las organizaciones previenen estos eventos al configurar una línea de defensa que permita monitorearlos, puesto que la mayor parte del malware criptográfico utiliza diferentes mecanismos de persistencia, por ejemplo, si el usuario en su intento de frenar el ataque reinicia el equipo, el *ransomware* continúa el proceso y continuar elcifrado de la información hasta que el proceso termine.

3. Expoliación de Respaldos:

Luego de que el malware es ejecutado, un *ransomware* normalmente apunta a cifrar los respaldos que tiene una organización, apunta a eliminar las instantáneas o puntos de restauración de un sistema operativo, con el propósito de evitar, que se restaure dichas copias de seguridad. La mayoría de *ransomware* tiene como objetivo principal el secuestro de información mas no le eliminación de la misma, por lo cual busca siempre la manera de evitar, que se recupere de un ataque sin que antes pague por el rescate.

Los Ransomware CryptoLocker y Locky ejecutan comandos que eliminan las instantáneas de volumen de un sistema, de la misma forma muchas variantes buscan las carpetas que contienen copias de seguridad y tratar de eliminarlas, especialmente cuando son ataques dirigidos.

4. **Encriptación de archivos:**

Una vez las copias de seguridad son eliminadas por el malware, este genera una llave segura la cual permite una comunicación constante entre la víctima y el comando y control *C2* o *C&C (Command & Control)*, el cuál posee una variedad de herramientas y técnicas que el atacante utiliza para garantizar el control incluso luego del ataque inicial, adicional utilizan el protocolo HTTP sin cifrar, HTTPS cifrado y TOR anónimo, este último es muy complejo rastrear la ubicación del atacante. Muy a menudo, el malware asigna al sistema una etiqueta local o identificador único, que se presenta al usuario en las instrucciones al final, es por ello que un C2 logra diferenciar las claves de cifrado utilizadas para diferentes víctimas.

La mayoría de malware actuales utilizan un cifrado AES 256, por lo cual hace imposible a la víctima romper el cifrado por su cuenta. Por otro lado, se destaca el mecanismo utilizado por el Malware SamSam el cual representa una nueva tendencia de ataque dirigido, por lo general algunos tipos de *ransomware* requieren contactarse con un servidor C2 para intercambiar claves, pero para SamSam la aplicación de software logra cifrar de manera local todos los archivos sin tener contacto con el Internet, este es un mecanismo novedoso, en una organización la comunicación con un servidor C2 es un IOC (Indicadores de compromiso) que es monitoreado constantemente en el hecho de prevenir un posible ataque, pero dado que este no genera tráfico no significa que el *ransomware* no esté presente.

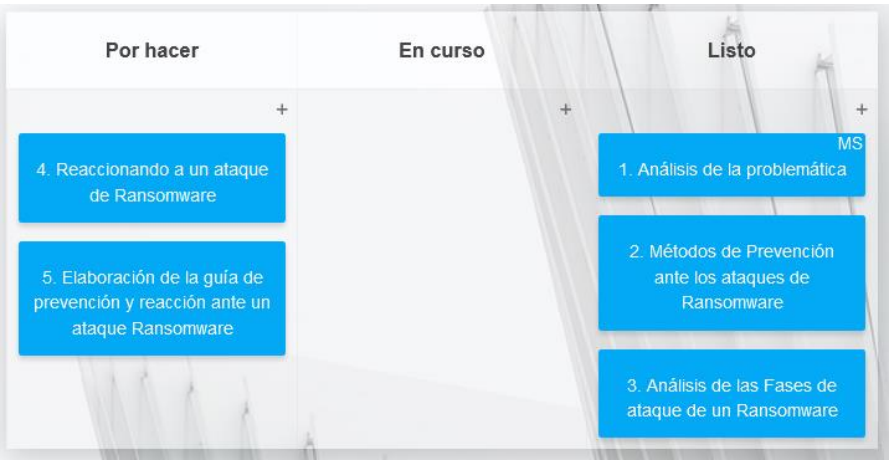
5. **Notificación al Usuario y Limpieza:**

Cuando el proceso de cifrado de la información termina, el usuario ve los mensajes que el atacante genera con las instrucciones de pago que realiza, normalmente, se brinda una cantidad de días, pero el rescate aumenta si no cumple ese plazo, estas instrucciones de demanda, se guardan a menudo en las carpetas de los archivos cifrados. En el malware CryptoWall 3 usa un archivo con el nombre *“HELP_DECRYPT”*

para almacenar las instrucciones de pago, pero en su versión 4 cambió el mismo por “AYUDAR A SUS ARCHIVOS”, en los cuales existen ciertas variaciones, pero el tema central de esta guía es para encontrar la variante exacta de malware. Como parte final de esta fase, el malware trata de eliminar todas las evidencias, esto con el objetivo de no dejar ningún rastro, puesto que el equipo contagiado podría ser llevado a un análisis forense del disco, para así lograr encontrar el mecanismo de funcionamiento del malware, lo cual significaría, que se construyan mejores estrategias de defensa en un posible nuevo ataque.

Con la finalización de la presente tarea, es necesario moverla al estado **listo** en el tablero de Kanban.

Figura 9. Tablero Kanban: Análisis de las fases de un ataque de *ransomware* - LISTO

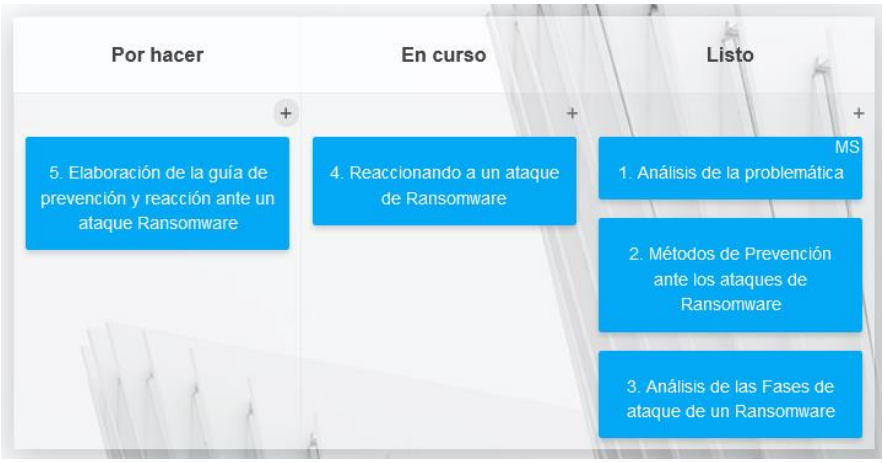


Fuente: Elaboración propia

Tarea 3. Reaccionando a un ataque de Ransomware

Una vez finalizada la tarea anterior, en el tablero Kanban esta tarea pasa al estado de en **curso**.

Figura 10. Tablero Kanban: Reaccionando a un ataque de *ransomware* - EN CURSO



Fuente: Elaboración propia

Los ataques de Malware han evolucionado sus mecanismos de ataque de manera constante, y en ese sentido los de tipo *Ransomware* son los más usados hoy en día para el robo y secuestro de información, debido a que utilizan nuevos métodos para vulnerar la seguridad de las infraestructuras de red al establecer como vector de ataque a varias organizaciones públicas y gubernamentales debido a la importancia de la información que manejan; en consecuencia para el desarrollo del presente proyecto es fundamental conocer los pasos, que se requieren para reaccionar cuando un ataque de Ransomware ya fue perpetrado, es así, que se toma en cuenta lo mencionado por Brewer (2016) es primordial disponer de un **Plan de Respuesta a Incidentes** que contempla las siguientes etapas:

- **Preparación:**

Uno de los mecanismos más comunes que utiliza un Malware para ingresar a los diferentes sistemas es aprovechar las vulnerabilidades que estos presentan, por lo cual es imperativo reforzar las defensas a través de la instalación de parches de seguridad y actualizaciones en todos los equipos y sistemas que incluye la infraestructura de red, dicho esto, hay que considerar que estas actualizaciones,

principalmente las de seguridad, serán programadas en horarios que no generen interrupción durante las jornadas laborables, muchas veces este proceso tarda varios minutos y no es interrumpido.

El contar con sistemas actualizados, aumenta la probabilidad de que el malware no avance en los computadores, así mismo, es importante crear y proteger las copias de seguridad disponibles, realizar copias frecuentes de documentos e información relevante, todo esto en una ubicación que no sea afectada, una buena opción es que respaldos estén fuera de línea, adicional, se verifica de manera periódica que estos sean restauados fácilmente en caso de ser necesario.

Los recursos compartidos en una red o a su vez los almacenamientos ubicados en la nube no llegan a ser del todo seguros puesto que la sincronización siempre es inmediata y podrían respaldarse archivos que estén infectados y estos corromper a su vez aquellos disponibles en la misma ubicación.

Finalmente, la concientización a los usuarios es una piedra angular en el contexto de preparación ante un ataque, dado que actualmente la mayoría de ataques de malware son propagados a través de correos electrónicos de *Pishing* o diferentes tácticas de Ingeniería Social, por esa razón el usuario aprende a identificar los mensajes que provoque una infección.

- **Detección:**

Para poder asegurar y mantener una infraestructura de red, es fundamental monitorearla de manera constante y por consiguiente analizar que sucede con las estaciones de trabajo de los usuarios, en tanto que el administrador de red o Analistas de Seguridad de tecnología identifican tráfico inusual, el cuál posiblemente esté asociado a una amenaza o actividad sospechosa presente dentro de la red corporativa.

Para enfrentar este tipo de eventos los Analistas de Seguridad unirían las piezas de varios escenarios, los cuales estarán relacionados con nuevas amenazas para así poder reaccionar rápidamente ante un incidente de Ciberseguridad.

Estas piezas son simplemente observables, es decir, desde una IP o URL sospechosa, o casos más complejos en los cuáles sería necesario realizar ingeniería inversa o análisis forense, esta reunión de patrones son conocidos como Indicadores de Compromiso *(IOC´s – Indicators of Compromise)* y algunos de sus casos de uso son:

- Análisis de un correo electrónico que intenta inyectar Malware
- Vulnerabilidades y cómo combatirlas
- Reconocimiento de patrones de comportamiento de un Malware
- Identificar un listado de direcciones IP que estén relacionadas con C2.

Una vez establecidos estos casos de uso, se elabora un listado de indicadores o a su vez describir un incidente completo para poder realizar un análisis e investigación y de esa forma obtener una respuesta para combatirlo.

Cuando están definidos los indicadores de compromiso, se los podría complementar con la utilización de un Sistema de Detección de Intrusos (*IDS - Intrusion Detection System),* el cual, se encarga de detectar accesos no autorizados dentro de una red o servidor en específico, genera alertas o *logs* que podrían ser gestionados por los Analistas de Seguridad.

- **Contención:**

Al asumir que el ataque de malware ha sido perpetrado, se seguirán pasos concretos para contener la propagación del mismo:

1. **Separar el equipo infectado y detener la infección:** cuando un solo equipo ha sido contagiado es un problema controlable, pero al llegar a infectarse más equipos, pueden detenerse las operaciones, por ese motivo desconectar el equipo de todos los sistemas es crucial en los primeros indicios de un ataque.

2. **Evaluar los daños causados:** es importante, que se detecte los equipos que han sido contagiados y así validar si los archivos cuentan con extensiones fuera de lo común o a su vez procesos, que se ejecuten en el sistema de manera inusual.

3. **Investigar el origen del ataque:** revisar las herramientas de seguridad para identificar los posibles medios de contagio, solo así, se toma indicios del malware que logró evadir las defensas o su vez encontró vulnerabilidades en los dispositivos, otra posibilidad es someter dicho equipo a un análisis forense para determinar las causas exactas del contagio y como logró evadir las medidas de seguridad, de esta forma es necesario documentar la información para implementar mejoras.

4. **Identificar el tipo de Ransomware:** cuando es determinado el origen, se determina la variante, para ello, se realiza una búsqueda en el Internet en base a la nota de rescate que encuentra en pantalla o algún correo electrónico que muestre en los archivos cifrados, para indagar en el tipo de *Ransomware* y buscar si existen herramientas de descifrado; en caso de ser necesario el caso escala a expertos externos y una buena opción son los equipos de respuesta ante incidentes de seguridad (CSIRT).

- **Erradicación:**

Una vez identificados los equipos afectados por el ataque, el próximo paso a seguir es erradicarlo de la red, por ello es más seguro que los equipos sean reemplazados o formateados por completo en lugar de solo desinfectarlos, considerar que el malware contiene rutinas de persistencia con daños residuales que re- infecten los equipos. También es posible seguir instrucciones que los proveedores de soluciones antivirus, proveen en sus sitios.

- **Recuperación:**

Si la organización está preparada para este tipo de incidentes, el paso número uno es restaurar los respaldos generados en las copias de seguridad, por ello es importante mantener copias verificadas y aisladas de la red para que no sean un objetivo de cifrado. La verificación de copias es fundamental, y los siguientes pasos pueden ser importantes a la hora de recuperar la información:

- Configuraciones de backup, frecuencia y lugar de respaldo.
- Pruebas periódicas de restauración para validar las copias y verificar que estén legibles y completas.
- Activar notificaciones que permitan conocer si existen errores en el proceso de backup.
- Mantener una política de retención de acuerdo a la importancia de la información, se considera crítico.
- El uso de checksum o suma de comprobación, se utiliza para verificar la integridad de los datos, de tal manera que usa un algoritmo como SHA-256, SHA-512 o MD5, se calcula el valor numérico del archivo original, para luego compararlo con el de respaldo y así comprobar si el hash es correcto.

Los planes de contingencia y recuperación son fundamentales y acortan el tiempo de inactividad; la vía más rápida es restaurar los equipos e información de las copias limpias de infección y hayan sido generadas recientemente.

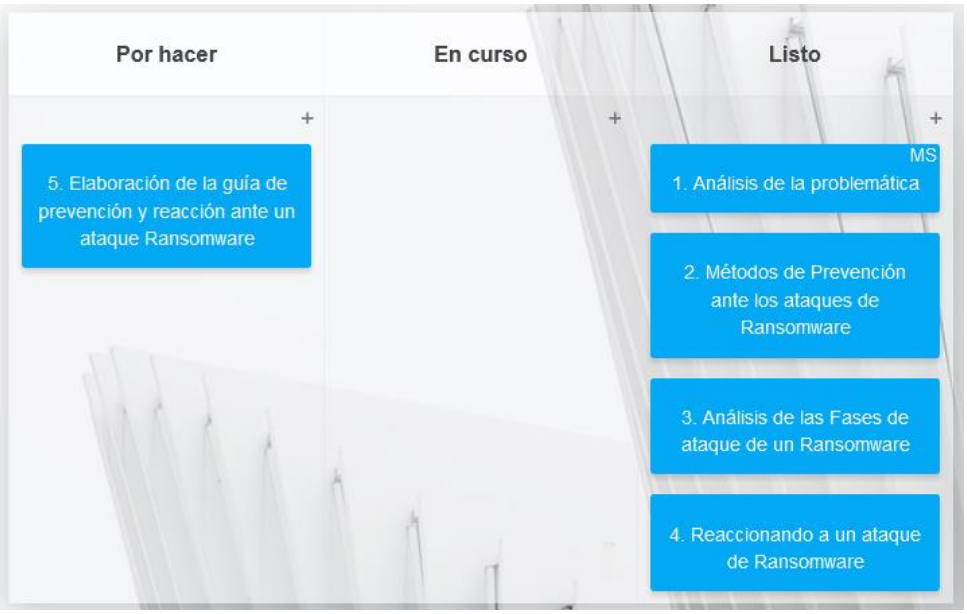
Así mismo según Celiktas (2018) “la detección proactiva de Ransomware incluye una respuesta activa a incidentes, continuidad del negocio y un plan para la recuperación ante desastres”, por lo cual es importante agregar las siguientes consideraciones adicionales:

- Determinar que equipos podrían comprar o alquilar en el caso de tener una pérdida de hardware para que las operaciones, no se detengan.

- Elaborar un manual, que muestre de manera explícita las rutas o dispositivos en donde están las copias de seguridad y cómo restaurarlas.
- Elaborar una política de seguridad que defina realizar respaldos de manera regular para evitar gran pérdida de datos.
- Definir una cadena de comunicación de las personas que intervienen en la solución del problema.
- En caso de tener un Centro de Datos externo, asegurarse que este sea confiable y garantice la seguridad de la información.

Con la finalización de la presente tarea, es necesario moverla al estado **listo** en el tablero de Kanban:

Figura 11. Tablero Kanban: Reaccionando a un ataque de *ransomware* - LISTO

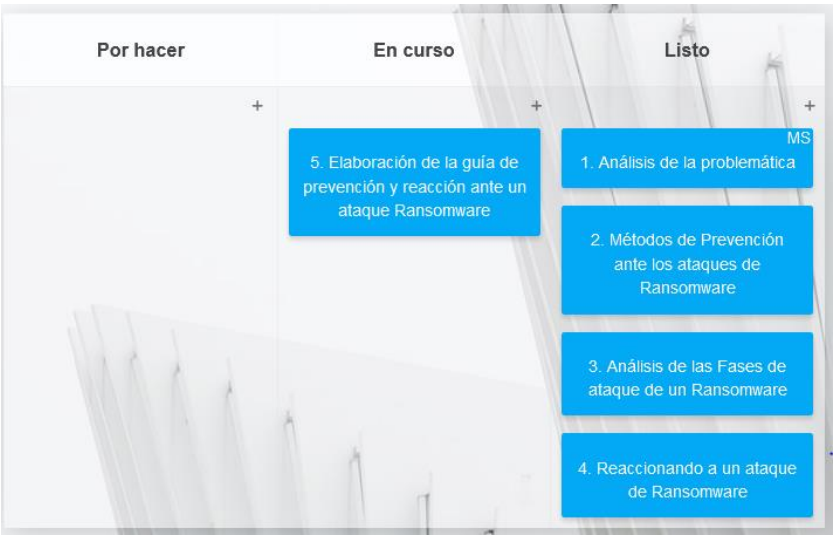


Fuente: Elaboración propia

Tarea 4. Elaboración de la guía de prevención y reacción ante un ataque Ransomware

Para la finalización del proyecto, la última tarea consiste en iniciar con la elaboración de la guía, por lo cual en el tablero Kanban esta pasa al estado en **curso.**

Figura 12. Tablero Kanban: Elaboración de la guía - EN CURSO



Fuente: Elaboración propia

En esta etapa final, se plasma de manera ordenada una serie de pasos a seguir para mejorar la ciberseguridad en una organización, específicamente ante ataques de tipo Ransomware.

- **Objetivo de la guía:**

Mejorar la capacidad de una organización en la prevención y reacción a los ataques de tipo Ransomware, a través de la implementación de mejores prácticas y estrategias eficaces que sean aplicables a cualquier tipo de arquitectura, con el fin de proteger los sistemas y datos críticos de la organización y evitar cualquier posible impacto negativo en la continuidad del negocio.

- **Estructura de la guía:**

A continuación, en base a la estructura propuesta, se pretende separar la guía en dos secciones principales, técnicas de prevención y técnicas de reacción:

TÉCNICAS DE PREVENCIÓN

1. Protección del perímetro

Al considerarse la primera línea de defensa, es importante mantenerla con una configuración adecuada, para evitar accesos mal intencionados:

Firewalls: todas las organizaciones requieren de una conexión a internet para poder desarrollar sus actividades cotidianas, por lo que el uso de un servidor Proxy es indispensable, proporciona la facilidad de filtrar el tráfico de red siempre y cuando esté configurado con reglas que garanticen que cada conexión http y https saliente, pase obligatoriamente por este. Es importante que al menos exista un dispositivo de filtrado, permite bloquear el acceso a sitios web considerados maliciosos y que no son necesarios para para que la organización desarrolle sus operaciones.

En la actualidad existen soluciones de Firewall que han mejorado sus funcionalidades con el objetivo de mejorar el nivel de Ciberseguridad, dado que tienen varias opciones de configuración que permiten monitorear de mejor manera el tráfico de red, se utilizarán sus funciones de acuerdo con el tamaño de la organización y las necesidades que presenta:

- **UTM:**

Un dispositivo UTM (*Unified Threat Management*), se encarga de la gestión unificada de amenazas y hace referencia a un dispositivo de hardware que ofrece una solución

de seguridad que tiene varias opciones de protección en un solo dispositivo y está dedicado a organizaciones Pymes y de mediano tamaño. A menudo contienen funciones tales como: firewall de red, antivirus, antispyware, antispam, prevención y detección de intrusiones, filtrado de contenido y prevención de ataques.

Adicionalmente es importante mencionar que un UTM, es una gran herramienta de seguridad, pero a la vez posee una desventaja, al ser el único punto de defensa, se convierte en el único punto de falla.

- **NGFW:**

Los NGFW (*Next Generation Firewalls*), son considerados dispositivos que manejan en general herramientas y funciones similares a los UTM pero que están orientados a implementarse en redes empresariales más grandes debido a su capacidad de manejar grandes cantidades de datos y conexiones, como son los *Datacenter* o servicios que son ofrecidos en la nube, todo gracias a que utilizan políticas de seguridad a nivel de aplicación, es decir, el nivel 7 de la capa OSI.

Para la implementación de herramientas Firewall, se contempla el tamaño de la organización, puesto que tanto los UTM y NGFW cumplen funciones similares, pero varían esencialmente en la cantidad de conexiones y datos que procesarán, para ello cada organización estudia su arquitectura de seguridad y elige la mejor opción, que se adapte a los objetivos.

Adicionalmente cabe mencionar que ante los costos que podrían implicar este tipo de soluciones, existen opciones como herramientas Firewall de software libre que aportarán de manera importante a la gestión de la seguridad:

Herramientas Sugeridas:

UTM:

- Check Point
- Sophos
- Mikrotik

Tabla 3. Comparación de herramientas UTM

Características	Check Point	Sophos	MicroTik
Firewall	Potente y gran capacidad de escalabilidad	Características avanzadas de Firewall de filtrado	Características avanzadas de Firewall de filtrado
Seguridad de correos electrónicos	Protección contra amenazas de pishing y malware	Protección contra amenazas de pishing y malware	No
Funciones de seguridad	Prevención de fuga de datos, filtro de correo no deseado, seguridad de azure para servicios en la nube	Inspección detallada de paquetes, Cloud Sandbox, tráfico cifrado, machine learning y prevención de ataques día cero,	Control de calidad de servicio, protocolos de ruteo, Scripting avanzado, antivirus y antispam, filtrado de contenido, protección ataques DDoS
Protocolos de enrutamiento	Static Routing, OSPF, BGP, RIP	RIP, EIGRP, IGRP, OSPF	BGP, RIP,OSPF, MPLS
Seguridad en la nube	CloudGuard ofrece seguridad nativa en la nube con prevención avanzada de amenazas	Cloud Native Security, con cobertura completa de seguridad en la nube en múltiples entornos y cargas de trabajo	No posee un módulo de seguridad en la nube
Respuesta a incidentes	Servicio de respuesta a incidentes inmediato 24/7	Posee un módulo MDR (Managed Detection and Response) que maneja la ciberseguridad como un servicio y analiza 24/7 los servicios de prevención y de brechas.	Soporte 24/7 de acuerdo a las necesidades del usuario
VPN	Si	Si	Si
Protección contra malware	Si	Si	Si
Control de Inteligencia de amenazas	Si	Si	No
Autenticación Multifactor	Si	Si	No

Fuente: Elaboración propia

NGFW:

- Fortinet FortiGate
- Cisco Firepower
- SonicWall

Tabla 4. Comparación de herramientas NFGW

Características	Fortinet FortiGate	Cisco Firepower	SonicWall
Rendimiento	Ofrece un alto rendimiento en la inspección de tráfico de red gracias a su procesamiento ASIC	Buen rendimiento gracias a la capacidad de procesamiento de su hardware	Rendimiento aceptable, aunque no es tan rápido como FortiGate o Cisco Firepower
Funciones de Seguridad	Amplia variedad de funciones de seguridad, incluye firewall, VPN, filtrado web, antivirus, antispam, prevención de intrusiones y más	También ofrece una amplia gama de características de seguridad, como firewall, VPN, IPS, antivirus, antispam, filtrado de URL y más	Ofrece funciones de seguridad sólidas, como firewall, VPN, prevención de intrusiones, filtrado de URL, protección contra amenazas avanzadas y más
Gestión y monitoreo	Viene con una interfaz de usuario fácil de usar y una variedad de herramientas de monitoreo y gestión centralizadas	Cisco Firepower Management Center es una plataforma de gestión potente y fácil de usar con una amplia gama de herramientas de monitoreo y gestión	SonicWall Global Management System ofrece una plataforma de gestión sólida con una variedad de herramientas de monitoreo y gestión, pero no es tan fácil de usar como las otras opciones
Integración y escalabilidad	Integración sólida con otras soluciones de seguridad de Fortinet, así como una escalabilidad excelente para adaptarse a empresas de todos los tamaños	Buena integración con otros productos de seguridad de Cisco y escalabilidad suficiente para adaptarse a empresas de todos los tamaños	Buena integración con otras soluciones de seguridad y escalabilidad para adaptarse a empresas de tamaño mediano, pero no es tan escalable como las otras opciones

Fuente: Elaboración propia

FIREWALL POR SOFTWARE:

- PFSENSE Firewall
- Endian Firewall

Tabla 5. Comparación de herramientas Firewall por software

CARACTERÍSTICAS	PFSENSE	ENDIAN
Plataforma	Basada en FreeBSD	Basada en Linux
Interfaz de usuario	WebGUI	WebGUI
Soporte de VPN	OpenVPN, IPsec, L2TP, PPTP	OpenVPN, IPSec, SSL
Soporte de alta disponibilidad	Sí	Sí
Soporte de filtrado de contenido	Sí	Sí
Soporte de prevención de intrusiones	Snort, Suricata	Snort
Soporte de balanceo de carga	Sí	Sí
Soporte de enrutamiento dinámico	OSPF, BGP, RIP	OSPF, RIP
Open VPN	Si	Si

Fuente: Elaboración propia

Filtro Web: dentro del servidor proxy, se definen cuáles son los accesos que poseerán los usuarios de una organización para de esa manera tomar medidas preventivas en el filtrado de la web, por ejemplo, bloquear accesos a cuentas de correo personales, redes sociales, incluso sitios de intercambio de archivos, entre otras. En algunos casos es necesario agregar exclusiones debido a ciertas necesidades institucionales, pero es fundamental que dentro del tráfico web, en el servidor proxy, se bloqueen algunos dominios de nivel superior (TLD), los cuáles son considerados como los de la tasa más alta de dominios maliciosos según el sitio oficial de Paloalto Networks:

Tabla 6. Dominios de Nivel Superior con tasa alta de dominios maliciosos

MALICIOSOS	PISHING	MALWARE	GRAYWARE	C2(COMANDO & CONTROL)
zw	pw	zw	sbs	cyou
Bd	Quest	Bd	Tokyo	Pw
ke	ke	ke	Xyz	Ws
Am	date	Am	cam	Gq
Sbs	cyou	cd	Date	Cf
Date	support	Date	Cm	Ml
Pw	win	Bid	Casa	Ga
Quest	rest	Ml	Uno	Info
Cd	casa	Ms	Email	Su
Bid	help	icu	Stream	best

Fuente: Adaptado del Sitio Oficial de Palosanto Networks (https://unit42.paloaltonetworks.com/top-level-domains-cybercrime/)

Filtro de Spam: su función es detectar y bloquear correos electrónicos no deseados o maliciosos, al combinarlo con un *firewall,* se convierten en un buen medio de protección de la red, el firewall por su lado bloquea el tráfico de red sospechoso o no autorizado, filtran correos electrónicos entrantes y salientes en función de ciertas reglas, por su lado el servidor de filtrado de spam realiza análisis heurísticos y aprendizaje automático para identificar y bloquear correos sospechosos, esto a través de palabras clave o frases comunes que utilizan los correos de *pishing,* analizan ciertas características del remitente, por ejemplo, su dirección IP o dominio de donde proviene; una vez realizado el análisis, si el dominio es desconocido o está configurado dentro de la lista negra que posee el servidor de *spam*, se bloquean automáticamente.

Para cumplir con este objetivo es necesario implementar un servidor de filtrado de correo, configurar el software que administra el correo electrónico para que envíe los correos entrantes al servidor de filtrado, posteriormente, se crearán las reglas para que el servidor detecte y bloquee los correos no deseados, finalmente, realizar pruebas de rendimiento y funcionamiento para poder implementarlo dentro de la red.

Cuando las pruebas sean exitosas, el servidor bloquea correos que tienen enlaces sospechosos, así como adjuntos ejecutables con diferentes extensiones que ejecuten un malware, a continuación, se detallan algunas de las principales extensiones de tipo maliciosas:

Tabla 7. Extensiones comunes de programas maliciosos

Extensiones comunes de programas maliciosos	
.exe	Archivos de programa
.com	Programa MS-DOS
.pif	Acceso directo a programa MS-DOS
.bat	Archivo por lotes
.scr	Archivo de protector de pantalla
.bin	Archivos binarios
.class	Archivos de Java que permite ejecutar Java Virtual Machine
.au3	Archivo de audio que incluye malware

Fuente: Elaboración propia

2. Defensas y monitoreo en la red

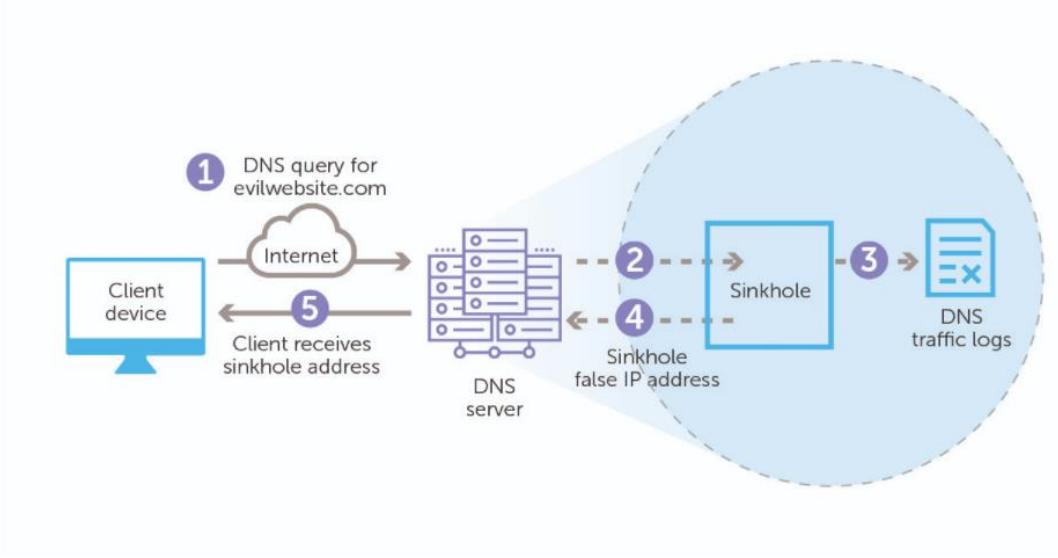
Para mantener protegida una organización, es necesario protegerla de amenazas internas y externas, por tal motivo es recomendable que dentro de la red LAN, se implemente seguridad que permita detectar y mitigar ataques por lo cual es importante considerar lo siguiente:

- ***DNS Sinkhole* (*Domain Name Server*):** Un sumidero de DNS es un servidor que bloquea el acceso a sitios web o dominios que son considerados maliciosos o no deseados, de tal manera que cuando un usuario intenta acceder a este tipo de sitios, el servidor DNS interfiere y bloquea la resolución del dominio correcto. A continuación, se explica un resumen de su funcionamiento:

1. Consulta DNS: el usuario intenta acceder a un sitio web mediante su navegador o una aplicación.
2. Consulta al servidor DNS: el equipo del usuario envía una consulta DNS al servidor configurado dentro de la red para que este resuelva el nombre de dominio.
3. Búsqueda dentro del servidor DNS: el servidor verifica si la consulta corresponde a un dominio bloqueado en su lista de dominios no deseados o maliciosos.
4. Bloqueo de la resolución: si el dominio está bloqueado, el servidor DNS responde con una dirección IP falsa o nula, así logra impedir que el usuario acceda al dominio.

Dentro de los sitios web que serán considerados como maliciosos o no deseados están los de Malware, Pishing, contenido para adultos, juegos en línea, redes sociales, *streaming* de vídeo o música, juegos de azar, entre otros.

Figura 13. Funcionamiento de servidor DNS Sinkhole



Fuente: Sitio BlueCat Networks (https://bluecatnetworks.com/blog/dns-sinkhole-a-tool-to-help-thwart-cyberattacks/)

- **Microsegmentación de la red:** si bien es cierto, mediante la segmentación de red con VLANs (*Virtual Local Area Network*) y configuración de ACLs (*Acces Control List*) no es suficiente para evitar un ataque de malware, pero sirve como medio de ayuda para su prevención. La creación de VLANs permite que cuando una infección logre ejecutarse en un equipo de un determinado segmento de red, esta infección permanezca aislada en los dispositivos que estén dentro del mismo para que no infecte a toda la organización.

Es ahí donde surge la importancia de implementar la microsegmentación de red, pues aplica específicamente dentro de un centro de datos para controlar las políticas y privilegios de los usuarios de quienes lo administran, esto genera un nivel de seguridad óptimo debido a los controles de acceso, todo ello basado en herramientas definidas por software las cuales permite obtener ventajas, que se consideran representativas y que cambian la manera tradicional de manejar la seguridad.

Las ventajas de dividir la red, permite reducir costos de las operaciones a través del uso de la misma infraestructura que posee, pero con servicios de seguridad avanzada, los cuáles permiten reducir los riesgos contra accesos no autorizados a la red local o centro de datos, esto garantiza características de autorización, autenticación y registro, seguridad, cumplimiento, redes en varias nubes y automatización:

Herramientas sugeridas:

- Vmware NSX Data Center
- Guardicore (incluye un módulo específico para evitar ataques de Ransomware)
- Nutanix

Tabla 8. Comparación de herramientas de Microsegmentación de la red

Característica	Vmware NSX Data Center	Guardicore	Nutanix
Tipo de herramienta	Plataforma de virtualización de redes con infraestructura hiperconvergente	Firewall de microsegmentación	Plataforma de infraestructura hiperconvergente
Enfoque	Virtualización de redes y centros de datos	Protección de cargas de trabajo en entornos de nube	Integración de computación, almacenamiento y virtualización
Funciones	Gestión centralizada de políticas, capacidad de integrarse con entornos de nube	Micro segmenta la red, visualización de tráfico de red, pero no es compatible con todos los hipervisores	Micro segmenta la red, se integra con servicios en la nube y es compatible con diferentes hipervisores
Características de seguridad	Microsegmentación de red, inspección profunda de paquetes y aislamiento de red	Microsegmentación, detección de anomalías, seguridad Zero Trust, protección contra ataques DDoS	Autenticación multi factor, protección de datos en reposo, cifrado de red, análisis de vulnerabilidades, parcheo de software

Fuente: Elaboración propia

- **Sistemas de detección de Intrusos de red:** Los sistemas de detección de intrusos NIDS *(Network Intrusion Detection System)* son utilizados para detectar intrusiones en tiempo real, estas son intentos de comunicación a sitios web, direcciones IP que son consideradas maliciosas o sitios de generación de claves que usan los *Ransomware*. Entre los principales están los HIDS (*HostIDS*) quienes monitorean tráfico entrante y saliente de un host específico, por ejemplo, en servidores los NIDS (*NetworkIDS)* que capturan todo el tráfico de la red y detecta tráfico inusual.

- **IDS *(Intrusion Detection System*):** es una aplicación de software que sirve para detectar anomalías o su vez accesos no autorizados dentro de una red, para ello lo que hacen es monitorear el tráfico de red entrante y compararlo con una base de datos que está actualizada con las más conocidas formas de ataque, una vez detectada la anomalía emite alarmas que permitirán al administrador de red, tomar acciones para evitar el posible ataque.

Herramientas sugeridas:

- Snort
- Suricata
- Security Onion

Tabla 9. Comparación de herramientas de Sistemas IDS

CARACTERÍSTICAS	SNORT	SURICATA	SECURITY ONION
Funciones principales	Detección y prevención de intrusiones	Detección y prevención de intrusiones	Detección y prevención de intrusiones, análisis forense y respuesta a incidentes
Arquitectura	Monolítica	Multi-hilo y multi-núcleo	Basada en distribuciones de Linux (Ubuntu, Debian)
Soporte de protocolos	TCP, UDP, ICMP, HTTP, DNS, SMTP, FTP, SSH, SSL	TCP, UDP, ICMP, HTTP, DNS, SMTP, FTP, SSH, SSL, SMB, DHCP, NFS, SIP, H.323	TCP, UDP, ICMP, HTTP, DNS, SMTP, FTP, SSH, SSL, SMB, DHCP, NFS, SIP, H.323
Velocidad de procesamiento	Menor que Suricata	Mayor que Snort	Depende del hardware utilizado
Integración con otras herramientas	Barnyard2, PulledPork	Barnyard2, PulledPork	Elastic Stack, Wazuh, OSSEC, Suricata
Facilidad de uso	Interfaz de línea de comandos (CLI) y GUI básica	CLI y GUI avanzada	GUI avanzada

Fuente: Elaboración propia

3. Protección de dispositivos

En esta sección, se detallarán medidas enfocadas en equipos o computadores que sirven de interacción entre la tecnología y los usuarios:

- **Actualizaciones y parches:** en general los Ransomware y otros tipos de malware, se aprovechan de las vulnerabilidades que presentan aplicaciones o software que no estén actualizados, el programar actualizaciones automáticas minimiza algunas maneras en que los equipos sean explotados de manera exitosa, de hecho, se considera una de las medidas más básicas, pero de las más importantes.

- **Aplicaciones de Privilegios mínimos:** para mejorar la seguridad en el manejo de dispositivos finales por parte de los usuarios, es importante aplicar métodos que le permitan acceder de manera limitada a la instalación o ejecución de tareas dentro de su cuenta, por lo cual, se crearán privilegios limitados para tareas comunes. Para este

propósito la implementación de un servidor de dominio permite controlar de mejor manera todos los accesos de usuarios, permite así definir lo que necesitan ejecutar y depende de sus actividades y perfiles.

- **Contraseñas:** la utilización de contraseñas robustas permite que para un atacante sea más difícil vulnerar la confidencialidad de los sistemas, por lo tanto, al contar con servidor de dominio, se configuran políticas que obliguen al usuario a colocar contraseñas con un número mínimo de letras, o caracteres que mejoren la seguridad, al identificarse varios intentos fallidos de acceso, se produzca un bloqueo de la cuenta.

- **Navegación segura:** evitar sitios web sean considerados dudosos es una tarea fundamental para evitar ataques de Malware, puesto que algunos esconden *exploits kits* que analizan vulnerabilidades de los navegadores y logran instalar el software malicioso, por ello es importante actualizar constantemente los navegadores; así mismo, se implementa algún software que permita navegar a través de una red privada virtual (VPN), permite así que el tráfico de red viaje de manera cifrada y evita que los atacantes la revisen.

- **VPN:** el uso de una red privada virtual ofrece ventajas importantes debido a que permiten establecer conexiones encriptadas y seguras cuando un usuario navega en internet, mantiene su identidad de manera anónima. Adicionalmente permite al usuario mantenerse a salvo de las cookies de publicidad o sitios que requieren rastrear la ubicación del usuario; a nivel de una organización le permite evitar el robo de información privada.

Herramientas sugeridas:

- Open VPN
- LogMeIn Hamachi
- Surfshark VPN

Tabla 10. Comparación de herramientas VPN

Características	OpenVPN	LogMeIn Hamachi	Surfshark
Licencia	Software libre	Servicio de suscripción	Servicio de suscripción
Protocolos admitidos	TCP, UDP, L2TP, PPTP	UDP, TCP	UDP, TCP, IKEv2, OpenVPN
Seguridad	Cifrado AES-256, autenticación SHA-512, certificados X.509	Cifrado AES-256, autenticación HMAC, certificados SSL	Cifrado AES-256-GCM, autenticación HMAC, certificados SSL
Interfaz de usuario	Cliente GUI, línea de comandos	Cliente GUI	Cliente GUI
Registro de actividad	No registra actividad	Registra la actividad del usuario	No registra actividad
Plataformas admitidas	Windows, Mac OS, Linux, Android, iOS	Windows, Mac OS, Linux	Windows, Mac OS, Linux, Android, iOS

Fuente: Elaboración propia

4. Sistemas EDR

Por la naturaleza de su mecanismo, este tipo de sistemas son capaces de detectar vulnerabilidades de día cero e incluso algunas clases de malware, puesto que utilizan métodos como la detección de comportamiento basada en la segregación de la amenaza en la nube, el aprendizaje automático y la ejecución de archivos para tratar de identificar malware e intentos de explotación.

Un sistema EDR (*Endpoint Detection Response),* se complementa con las acciones de un Antivirus tradicional, puesto que utilizan la inteligencia artificial y el *Big Data* para mejorar de manera autónoma la detección de amenazas para su posterior eliminación de manera automática.

Este tipo de herramientas superan en gran nivel a un antivirus normal, puesto que ofrecen mayores herramientas que permiten identificar, detectar y prevenir cualquier tipo de amenaza externa que vulnere la seguridad de la red, sus principales características son:

- Machine Learning
- Sandboxing

- Indicadores de compromiso
- Herramientas de recuperación
- Detección archivos sospechosos
- Aislamiento de archivos sospechosos en la nube

Herramientas sugeridas:

- VMware Carbon Black
- CrowdStrike
- SentinelOne

Tabla 11. Comparación de herramientas EDR

Características	VMware Carbon Black	Crowd Strike	SentinelOne
Protección contra Pishing	No	Si	No
Detección y Prevención de amenazas	Incluye la identificación de comportamientos maliciosos y prevención de ataques de día cero	Utiliza una técnica basada en la inteligencia artificial y el aprendizaje automático para detectar amenazas conocidas y desconocidas, previene ataques de día cero	Utiliza inteligencia artificial y aprendizaje automático para detectar malware y ataques de día cero
Tipo de detección	Agente/Cloud	Cloud	Agente/Cloud
Facilidad de uso	Compleja	Fácil	Fácil
Investigación y respuesta a incidentes	Capacidades de investigación y respuesta a incidentes, incluye recolección de datos de endpoint y creación de informes personalizados	Incluye dentro de sus capacidades la visualización de la cadena de ataque y la identificación de amenazas persistentes avanzadas (APT).	Ofrece una consola de administración unificada, visualización de la cadena de ataque, identifica amenazas persistentes avanzadas (APT), permite automatizar respuestas a incidentes

Fuente: Elaboración propia

5. Implementación de Servidores de Dominio

La implementación de servidores de dominio es fundamental para administrar los recursos informáticos, pues organizan y protegen a los usuarios mediante diferentes políticas de administración, esto basado en los niveles de jerarquía, que se brinda a los usuarios para de esa manera resguardar la información. Dentro de estas políticas, se destacan aquellas Políticas de Seguridad *(GPO)* que son utilizadas para administrar objetos de equipos y usuarios, esto va a depender del nivel de restricciones, por ejemplo, se usa una lista de bloqueo que permita definir las aplicaciones que podrán ser ejecutadas en rutas habituales de ataques de malware como la carpeta “AppData”.

Estas políticas son desarrolladas de manera particular de acuerdo a las necesidades de la organización, o a su vez, se usan políticas que bloquean diferentes tipos de ataque, adicional a este nivel de seguridad, se usa software diseñado para estos propósitos, como las herramientas antimalware que en sus componentes agregan la posibilidad de restringir la ejecución de diferentes variantes de Malware.

Las directivas o programas que son utilizadas para la restricción de software son considerados medios sugeridos para evitar que algunos programas de software sean ejecutados en los equipos de un dominio o una red, para evitar así infectar a todos los equipos de una organización:

Herramientas sugeridas:

- CryptoPrevent Anti-Malware
- Windows App Locker
- Malware Bytes
- Implementación de un dominio con directivas de seguridad

Tabla 12. Comparación de herramientas Antimalware

Características	CryptoPrevent	WindowsApp Locker	Malwarebytes
Tipo de Herramienta	Herramienta de prevención de malware	Control de acceso de aplicaciones	Herramienta de eliminación de malware
Funciones principales	Protege contra la ejecución de *ransomware* y otros tipos de malware	Controla el acceso a las aplicaciones de Windows	Escanea y elimina el malware existente
Modo de funcionamiento	Funciona como una aplicación en segundo plano que monitorea la actividad del sistema	Funciona como una herramienta de gestión de políticas de seguridad de Windows	Funciona como una aplicación de escaneo y eliminación de malware
Enfoque de Seguridad	Preventivo	Preventivo	Reactivo
Licencia	Disponible en una versión gratuita y de pago	Disponible en Windows Enterprise y Ultimate Editions	Disponible en una versión gratuita y de pago
Características avanzadas	Protección de carpetas específicas, protección contra amenazas de scripting y protección de la cuenta de usuario	Políticas de restricción de aplicaciones por nombre, editor, hash y ubicación de archivo	Protección en tiempo real, escaneo programado, eliminación de rootkits, bloqueo de sitios web maliciosos y protección contra *ransomware*
Facilidad de uso	Fácil de configurar y usar	Requiere mayor conocimiento en políticas de seguridad de Windows	Fácil de usar y configurar

Fuente: Elaboración propia

6. Infraestructura de escritorios virtuales (VDI)

Ante la aparición y el auge de las nuevas modalidades de teletrabajo en diferentes organizaciones, este tipo de infraestructura permite asignar un escritorio de manera virtual a los usuarios, con similares funcionalidades que un equipo físico. Todos estos escritorios virtuales son almacenados en la nube bajo un servidor central que permite administrar sus actualizaciones de manera rápida y sin tener que acudir de manera física, pero una de sus ventajas más significativas es que agrega medidas de ciberseguridad, si el escritorio es víctima de un ataque dirigido, la información está debidamente respaldada en la nube.

Dentro de la infraestructura de escritorios virtuales, una característica importante es que, si alguno de los equipos ha sido víctima un ataque de malware, una vez que el usuario finalice su sesión, el sistema es restaurado a su estado anterior y elimina la infección por completo. Adicional a ello ofrecen ventajas en cuanto a seguridad, disponibilidad, flexibilidad y la posibilidad de garantizar continuidad en el negocio.

Herramientas sugeridas:

- Amazon Workspaces
- Microsoft Azure
- VMware Horizon Cloud

Tabla 13. Comparación de herramientas de virtualización de escritorios

Características	Amazon Workspaces	Microsoft Azure	VMware Horizon Cloud
Compatibilidad	Windows y Linux	Windows	Windows y Linux
Protocolos de acceso	PCoIP y Amazon Workspaces Streaming Protocol (WSP)	Remote Desktop Protocol (RDP) y Virtual Desktop Protocol (VDP)	PCoIP y Blast Extreme
Integración con Active Directory	Sí	Sí	Sí
Almacenamiento	Amazon Elastic File System (EFS) y Amazon S3	Azure File Storage y Azure Blob Storage	Virtual SAN (vSAN) y Network-attached storage (NAS)
Herramientas de monitoreo y gestión	Amazon CloudWatch y AWS Management Console	Azure Monitor y Azure Portal	VMware vRealize Operations y Horizon Console
Seguridad	AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud (VPC) y AWS Key Management Service (KMS)	Azure Active Directory (AD), Azure Virtual Network (VNet) y Azure Key Vault	VMware NSX y AppDefense

Fuente: Elaboración propia

- Capturas Instantáneas de Máquinas Virtuales: La virtualización de servidores actualmente es una práctica muy común, puesto que permite una administración adecuada de recursos tanto de hardware como de software, pero para el tema específico de ataques de *ransomware*, es importante generar respaldos de las instantáneas de las máquinas virtuales, permiten restaurar el estado de la máquina en tiempo real, lo que proporciona una opción eficiente de guardar estados de equipos como su configuración e información en diferentes puntos de tiempo específicos.

7. Aislamiento de Aplicaciones en cliente final (Sandbox):

El Sandbox es una tecnología que permite ejecutar aplicaciones informáticas dentro de un ambiente controlado, el cual, se encuentra aislado del sistema operativo principal y que tiene los archivos necesarios para que estas funcionen pero de una manera vigilada y controlada; en el caso de que dicho programa esté contagiado con algún malware, el Sandbox no le permite contagiar al resto del equipo y adicionalmente es analizado su funcionamiento y tácticas de ataque para aprender de ellas y mejorar la eficiencia en la seguridad de la información. Bajo Sandbox, se utilizan navegadores web y sus respectivos complementos, de manera, que se evite que ciertas formas de *ransomware* afecten su sistema.

La importancia de analizar este tipo de tecnología, es porque presenta varias ventajas sin importar el tipo de organización, permite ejecutar procesos sospechosos dentro de un ambiente aislado y controlado, con la posibilidad de limitar el acceso a diferentes recursos importantes como la memoria, contacto con otras aplicaciones, entre otros. En el caso de producirse una infección por malware, esta tecnología permite confinar el software malicioso y analizarla a detalle para así conseguir datos útiles que permitan detectar ataques con mayor antelación.

Herramientas sugeridas:

- Cuckoo Sandbox
- Any Run Sandbox

Tabla 14. Comparación de herramientas Sandbox

Características	Cuckoo Sandbox	Any Run Sandbox
Tipos de análisis	Análisis de malware y amenazas de red	Análisis de malware y amenazas de red
Soporte de sistemas	Linux, Windows, MacOS, Android	Windows
Funcionalidades	Se ejecuta en una máquina local y tiene la capacidad de analizar archivos, URLs y memoria en múltiples plataformas, incluye Windows, Linux, Android y MacOS	Any Run Sandbox, por otro lado, es una herramienta en línea que se enfoca en el análisis de archivos y URLs en las plataformas Windows y Android
Arquitectura	Se ejecuta en una máquina virtual	Se ejecuta en la nube
Integraciones	Integración con VirusTotal, Yara, Suricata, etc.	Integración con VirusTotal, Yara, MITRE ATT&CK, etc.
Interfaz de usuario	Compleja	Sencilla
Análisis de Memoria	Sí	No
Precio	Open-source y gratuita	Varias opciones de suscripción disponibles

Fuente: Elaboración propia

8. Servidores NAS

Actualmente algunas organizaciones utilizan unidades de almacenamiento compartidas, alojadas en algún tipo de dispositivo NAS (*Network Access Server*), el cual es afectado por Ransomware. A continuación, se enumeran mecanismos de protección adicionales como:

- **Seguridad:** para la administración del NAS es fundamental utilizar contraseñas seguras y usar doble factor de autenticación, lo que agrega una capa extra de seguridad.

- **Actualizaciones:** mantener actualizado el Firmware del dispositivo es fundamental para evitar que esté expuesto a vulnerabilidades que permitan algún tipo de ataque.

- **Permisos de archivo:** otorga a los usuarios los privilegios mínimos en las respectivas unidades compartidas a las cuales requieren acceder.

9. Inventario de Datos

Las organizaciones actualmente manejan una gran cantidad de información, eso implica que la importancia de la misma depende del área e impacto que esta aporta si es que esté debidamente categorizada, esto permite su recuperación y reparación en caso de ser necesario. A pesar de que actualmente los servicios de respaldo de información en la nube son comunes, es importante tener respaldos locales de información de áreas críticas, pero aún más indispensable, es determinar aquellas áreas que realmente necesitan tener un respaldo, a continuación, se detallan algunos pasos importantes a tener en cuenta:

- **Identificación de los activos de datos:** el primer paso es identificar todos los activos de datos que posee la organización. Esto incluye bases de datos, archivos en papel, sistemas de almacenamiento en la nube, servidores, dispositivos móviles y cualquier otro medio de almacenamiento de datos. Realiza un inventario exhaustivo de todos los activos.

- **Clasificación de los datos:** una vez identificados los activos de datos, es importante clasificarlos según su importancia y confidencialidad, categorizar los datos en función de su nivel de sensibilidad, como datos personales, datos financieros, secretos comerciales o información confidencial. Esto ayuda a priorizar las medidas de protección necesarias.

- **Determinación de las fuentes de datos:** identificar las fuentes de datos de la organización, estas incluyen sistemas internos, bases de datos externas, aplicaciones de terceros y otros proveedores de servicios.

- **Documentación detallada:** es necesario tener una documentación detallada que describa cada activo de datos, esta incluye información como la ubicación física o lógica del activo, la descripción de los datos que contiene, el propósito del almacenamiento de datos y cualquier otra información relevante.

- **Implementación de medidas de seguridad:** es necesario implementar las medidas de seguridad adecuadas para proteger los activos de datos, cifrado de datos, con la implementación de controles de acceso, monitoreo de actividad sospechosa, realización de copias de seguridad regulares y otras prácticas recomendadas de seguridad de la información.

- **Mantenimiento y actualización continua:** el inventario de datos no es un proceso único, sino un proceso continuo, es importante mantener y actualizar regularmente el inventario de datos a medida, esto garantiza que la información sea precisa y esté al día. Cada organización tiene requisitos y circunstancias particulares, por lo que es importante adaptar estos pasos a las necesidades específicas de la organización.

10. Copias de Seguridad

Las copias de seguridad son garantizadas a través de planes que permitan recuperar los datos en caso de un ataque de Ransomware, esto permite una recuperación efectiva:

- **Plan de Recuperación:** el plan permite acceso rápido a las copias de recuperación y el tiempo que requiere para restaurarlas, esto es definido en el inventario de datos, se requieren políticas y procedimientos claramente documentados que establezcan, cuándo es generada la copia de seguridad, donde se copiarán o restaurarán los datos y quién es responsable de la copia de seguridad y el proceso de recuperación, para esto es necesario que las personas responsables de dicho proceso sean capacitadas.

- **Copias de Seguridad fuera de conexión:** si bien es cierto las copias de seguridad, se replican de manera continua, pero esto no aplica cuando hay que reaccionar a un ataque de *ransomware*, puesto que serían versiones cifradas, por tal motivo para restaurar estas copias de seguridad, se extraerían de un sistema sin conexión, no estarán cifrados ni alterados. Es por ello, que se realizarán múltiples copias instantáneas de manera histórica, la frecuencia en las que con ejecutadas dependen de la importancia que la organización requiere para cumplir sus objetivos.

- Garantía de copias de seguridad y recuperación: los planes de copias de seguridad y su recuperación ante algún tipo de ataque, suelen ser un escenario que pocos anticipan, por tal motivo, se probarán con éxito de acuerdo con los procedimientos establecidos en la organización, eso permite garantizar que están protegidos de ataques de *ransomware*, usuarios internos mal intencionados o filtración de esos datos.

A continuación, algunos métodos para probar las copias de seguridad de la información:

- **Pruebas regulares de restauración:** una manera efectiva de validar las copias es restaurarlas de manera periódica con diferentes grupos de datos.

- **Verificación de la Integridad de datos:** antes de realizar una copia los datos son verificados para que no tengan errores o estén corruptos, para ello, se usa el comando *checksum* o software de verificación de archivos.

- **Utilizar múltiples medios de almacenamiento:** es importante guardar los respaldos en diferentes medios de almacenamiento, esto garantiza que en el caso de que algún medio falle, se acceda a la información en otro diferente.

- **Utilizar redundancia:** para poder garantizar la disponibilidad e integridad de la información, es importante utilizar la redundancia en las copias de seguridad, esto

implica guardar múltiples copias de seguridad en diferentes medios de almacenamiento, sistemas RAID e incluso diferentes ubicaciones geográficas dependen de la importancia de la información.

El planificar las copias de seguridad es solo la mitad del proceso, puesto que, sin un Plan de Recuperación ejecutado y probado regularmente, se convierte en un problema grave cuando sea un ataque real, el cual demande restaurar la información para la correcta operación de la organización. Es para ello importante considerar que, dentro de un Plan de Contingencia y la continuidad de un negocio, se contemple como un proceso adicional de la empresa el tema de seguridad y recuperación.

11. Administración integral de la Tecnología

Dentro de una organización, la gestión de las operaciones es fundamental, sin importar cual es el giro de negocio o tipo de industria, para poder cumplir con la demanda que oferta a sus clientes, la tecnología es indispensable puesto que aporta el desarrollo de nuevas formas de innovar en eficiencia y mejora de sus procesos internos, así como incrementar la productividad.

La infraestructura de tecnología está conformada por dispositivos de red, servidores o aplicaciones, y en todo este entorno cualquier descuido en la seguridad podría causar efectos que comprometerían las operaciones de la organización, por ello la gestión adecuada de los elementos de infraestructura no es suficiente, se da un paso más allá en correlacionar los datos de las operaciones de tecnología.

Es importante elegir una herramienta que ofrezca las funcionalidades adecuadas para la gestión de TI y la seguridad de la empresa, que sea escalable y fácil de usar, y para realizar una gestión adecuada de la Infraestructura de seguridad es necesario integrar datos de las operaciones y relacionarlos, esto permite a los altos mandos mejorar la toma de decisiones en una organización, se basa en herramientas que contenga características como:

- Monitoreos del rendimiento de una red
- Monitoreos de rendimiento del servidor o servidores principales
- Monitorear el rendimiento de las aplicaciones
- Realizar análisis de tráfico de red
- Administrar las direcciones IP y los puertos de dispositivos de red
- Gestión de incidentes de TI
- Gestión de inventarios
- Controles o permisos de acceso
- Copias de seguridad y recuperación en la nube
- Alertas en tiempo real

Herramientas sugeridas:

- Manage Engine
- NinjaOne

Tabla 15. Comparación de herramientas de Administración de Tecnología

Características	Manage Engine	NinjaOne
Funcionalidades	Ofrece una amplia variedad de herramientas para la gestión de TI, incluye soluciones de monitoreo, gestión de redes, seguridad, helpdesk y gestión de activos.	Se enfoca principalmente en la monitorización y la gestión de redes, ofrece herramientas avanzadas de monitoreo de red y de análisis de tráfico.
Interfaz de usuario	La interfaz de usuario es intuitiva y fácil de usar, con paneles de control personalizables y gráficos en tiempo real.	La interfaz de usuario es moderna y limpia, con una navegación fluida y rápida.
Integraciones	Ofrece integraciones con una amplia variedad de herramientas de terceros, incluye soluciones de seguridad, monitoreo y gestión de nube.	Cuenta con integraciones limitadas, pero ofrece soporte para SNMP, Syslog y NetFlow.
Seguridad	Ofrece soluciones de seguridad para la gestión de contraseñas, auditoría de seguridad y prevención de amenazas.	Incluye la detección de intrusiones y la prevención de amenazas.
Escalabilidad	Es altamente escalable, se adapta a las necesidades de las empresas de todos los tamaños.	También es escalable, pero su enfoque principal es la monitorización y la gestión de redes para empresas medianas y grandes.
Soporte técnico	Ofrece soporte técnico en varios idiomas, incluye español, y proporciona asistencia por teléfono, correo electrónico y chat en vivo.	Ofrece soporte técnico por teléfono y correo electrónico, pero no proporciona soporte en vivo.

Fuente: Elaboración propia

12. Pruebas de Virus EICAR (*European Institute for Computer Antivirus Research*)

Este tipo de prueba fue desarrollado por el Instituto Europeo para la Investigación de los Antivirus Informáticos, su objetivo es el de verificar la efectividad de respuesta de los programas Antivirus, para ello solo es necesario descargar el archivo de tipo DOS del sitio oficial de EICAR (https://www.eicar.org/download-anti-malware-testfile/), el cuál actúa como si fuera un virus real, el objetivo es validar el funcionamiento de detección en tiempo real de las soluciones antivirus.

Esta prueba de virus consiste en un archivo de texto que contiene una cadena de caracteres específica que simula el comportamiento de un virus informático. Este archivo no es dañino y no representa una amenaza real para el sistema, pero permite a los ingenieros de ciberseguridad evaluar la capacidad de detección de los programas antivirus y garantizar que este funcione correctamente.

La importancia de aplicar la prueba de virus EICAR radica en los siguientes puntos:

- **Verificación del funcionamiento del antivirus:** Al ejecutar la prueba de virus EICAR, se confirma si el programa antivirus está configurado correctamente y es capaz de detectar y bloquear amenazas. Esto es esencial para garantizar la protección del sistema y los datos frente a ataques reales.

- **Evaluación de la efectividad de los sistemas de seguridad:** esta prueba permite evaluar la efectividad de los sistemas de seguridad implementados en una red o infraestructura. Al realizar pruebas periódicas con esta prueba, se identifican las posibles brechas en la protección y tomar medidas correctivas para fortalecer la seguridad.

- **Cumplimiento de estándares y regulaciones:** En muchos casos, las organizaciones cumplirán con estándares y regulaciones específicas relacionadas con la seguridad de la información. La realización de pruebas de virus, incluye la prueba EICAR, es un requisito para cumplir con estas normativas y demostrar, que se toman medidas adecuadas para proteger los sistemas.

- **Formación y concientización de los usuarios:** La prueba de virus EICAR, se utiliza como una herramienta de formación y concientización para los usuarios. Al enviar correos electrónicos de prueba con el archivo EICAR adjunto o simular escenarios de infección, se educa a los usuarios sobre la identificación y prevención de amenazas, fomentar prácticas seguras y reducir el riesgo de infecciones reales.

TECNICAS DE REACCIÓN:

1. Concientización de usuarios

Los usuarios son una parte fundamental de la seguridad de cualquier organización, y por ende son la primera línea de defensa, como el punto débil en la cadena de seguridad. La mayoría de los incidentes de seguridad son causados por errores humanos, como dar *click* en enlaces sospechosos o descargar archivos maliciosos, por lo tanto, es fundamental que los usuarios de la organización comprendan los riesgos de seguridad y las mejores prácticas para reducirlos.

La concientización en seguridad es un componente integral de cualquier programa de ciberseguridad, pues permite a los usuarios identificar y prevenir amenazas antes de que sean un riesgo mayor. Las capacitaciones irán enfocadas en instruir a los usuarios cómo manejar correos electrónicos de *pishing* y ataques de Ingeniería Social, también, manejar contraseñas seguras y cambiarlas regularmente.

Otro aspecto a considerar es el educar a los usuarios sobre las políticas de seguridad y los procedimientos de la organización, como la forma de acceder a los sistemas de información, cómo manejar sus datos personales y cómo informar acerca de incidentes de seguridad.

En resumen, la concientización periódica es esencial para garantizar la seguridad, puesto que, al educar a los usuarios con las mejores prácticas, se reducen de manera significativa la posibilidad de ataques y por ende permita proteger la información crítica de la organización.

2. Gestión de Vulnerabilidades

En la actualidad las organizaciones dependen de los sistemas informáticos y varios servicios de tecnología para poder cumplir con sus objetivos de negocio, por lo tanto,

es indispensable contar con un plan integral de Gestión de Vulnerabilidades IT, que consiste en una serie de procesos y herramientas de seguridad que permiten identificar, analizar y solventar de manera continua las posibles vulnerabilidades y ciber amenazas, dentro de estos procesos están:

- **Escaneo de Vulnerabilidades:** se utilizan herramientas automáticas, por ejemplo, Nessus permite identificar vulnerabilidades en los sistemas y aplicaciones. Este proceso es realizado de manera regular, al menos una vez al mes para corregir las vulnerabilidades y corregirlas antes que sean explotadas.

- **Evaluación de Vulnerabilidades:** una vez identificadas las vulnerabilidades es necesario evaluar el impacto de cada una, esto quiere decir, que se evalúa el riesgo de que la vulnerabilidad sea explotada y las consecuencias que tendría la organización.

- **Gestión de Vulnerabilidades:** la gestión implica priorizar las vulnerabilidades y elaborar un plan de acción que permita corregirlas, se toma en cuenta que no todas serán corregidas de inmediato, pero si las que mayor impacto generen a la organización. Esta gestión es continua y es revisada de manera regular para asegurar que se toman las medidas pertinentes para corregir las vulnerabilidades ya identificadas.

- **Pentesting:** es un término conocido como *Hacking* Ético, es una parte fundamental de la Gestión Integral de Vulnerabilidades, pero difiere en el hecho de que no es un proceso automático que escanea todas las vulnerabilidades, si no que consiste en un profesional que explota una vulnerabilidad encontrada y establece si es realmente explotable al poner en peligro la confidencialidad de la información.

La gestión de vulnerabilidades incluye el constante monitoreo de la red dentro de la organización, por tal motivo el tiempo recomendado para ejecutar estas acciones es de al menos una vez al mes para el escaneo y evaluación de vulnerabilidades, mientras

que el *pentesting,* se realizaría al menos una vez al año. Hay que tomar en cuenta que los tiempos varían en función del tamaño y complejidad de la organización, así como la identificación de sistemas y activos que son necesarios proteger.

3. Puesta en marcha del Plan de respuesta a Incidentes

Las organizaciones en la actualidad estarán preparadas de manera constante ante un posible incidente, por lo tanto, este es elaborado en base a los objetivos de la organización, en la presente guía, se ha mostrado como puede definirse un plan integral para responder a un incidente y los responsables de tomar acciones durante las diferentes fases de detección, contención, erradicación y recuperación. Así mismo, se considera que los ataques informáticos cada día son más sofisticados y exigen un mayor esfuerzo a los equipos de seguridad informática de las organizaciones, por tal motivo existen los equipos de respuesta a incidentes de seguridad – CSIRT *(Computer Security Incidents Response Team),* cuyo objetivo principal es mitigar y minimizar los daños que causen un incidente, logra que el impacto sea mínimo y que la organización logre retomar con normalidad las principales actividades en el menor tiempo posible y sin causar mayor impacto.

4. Pentesting

Cuando existe un ataque, el objetivo es minimizar los daños y hacerlo lo más rápido posible, para ello es necesario verificar regularmente el plan de respuesta a incidentes y así conocer cómo los miembros de una organización responden ante una situación simulada, por lo tanto, el *Pentesting* es una técnica utilizada para evaluar la seguridad de los sistemas y activos de información. A continuación, se sugieren algunos pasos a seguir para realizarlo de manera efectiva:

- **Definir los objetivos del *pentesting:*** esto implica definir los sistemas y activos que serán evaluados y los escenarios de ataque que se simula.

- **Recopilar información:** conocer todo lo perteneciente a los activos y sistemas que se evalúan, por ejemplo, la infraestructura de red, sistemas operativos de equipos, aplicaciones, servicios que son usados, entre otras.

- **Identificar posibles vulnerabilidades:** en esta parte del proceso, se hace un análisis de vulnerabilidades para evaluar cuales son explotadas por un atacante, tema que fue analizado en la “Gestión de Vulnerabilidades.”

- **Planificar y ejecutar *Pentesting:*** cuando las vulnerabilidades fueron identificadas, se hace una planificación y ejecución del p*entesting*, esto implica simular un ataque para comprobar si las vulnerabilidades encontradas son explotadas.

- **Documentar los resultados:** la documentación de resultados permite tener una evidencia clara de los resultados obtenidos en el *pentesting,* incluye las vulnerabilidades y las consecuencias de su explotación, así mismo, se deja constancia de las medidas necesarias para corregirlas.

- **Informe y recomendaciones:** se emite un informe completo de todo el proceso, el cuál es presentado a la dirección de la organización para analizar las medidas a tomar para no solo resolver las vulnerabilidades encontradas, si no buscar mecanismos que permitan mejorar la seguridad de los sistemas evaluados.

Finalmente es importante tomar en cuenta que este tipo de procesos serán realizados por profesionales de seguridad, que se encuentren altamente capacitados y a su vez cuenten con la experiencia necesaria para garantizar que el proceso no afecte o cause daños a los sistemas y activos evaluados:

Herramientas sugeridas:

- Kali Linux
- Nessus

Tabla 16. Comparación de herramientas de Escaneo de Vulnerabilidades

Características	Kali Linux	Nessus
Propósito	Distribución de Linux especializada en pruebas de penetración	Escáner de vulnerabilidades y evaluación de seguridad
Funciones principales	Pruebas de penetración, auditoría de seguridad, análisis forense	Escaneo de vulnerabilidades, análisis de redes y sistemas
Arquitectura	Basado en Debian	Basado en cliente-servidor
Instalación	ISO instalable o máquina virtual preconfigurada	Cliente de software, que se conecta a un servidor
Interfaces	Interfaz de línea de comandos (CLI) y una interfaz gráfica de usuario (GUI)	Interfaz gráfica de usuario (GUI)
Herramientas incluidas	Más de 600 herramientas de pruebas de penetración y seguridad	Base de datos con miles de plugins y pruebas de seguridad
Personalización	Altamente personalizable y flexible, permite agregar y quitar herramientas según las necesidades	Configurable y permite ajustar el escaneo y las políticas de seguridad
Actualizaciones	Actualizaciones regulares de paquetes y nuevas versiones de Kali Linux	Actualizaciones de plugins y nuevas versiones de Nessus
Uso profesional	Ampliamente utilizado por profesionales de la seguridad y pentesters	Ampliamente utilizado por profesionales de la seguridad y empresas de todo el mundo
Precio	Gratuito y de código abierto	De pago con opciones de licencia basadas en suscripción

Fuente: Elaboración propia

5. Recuperación de Datos

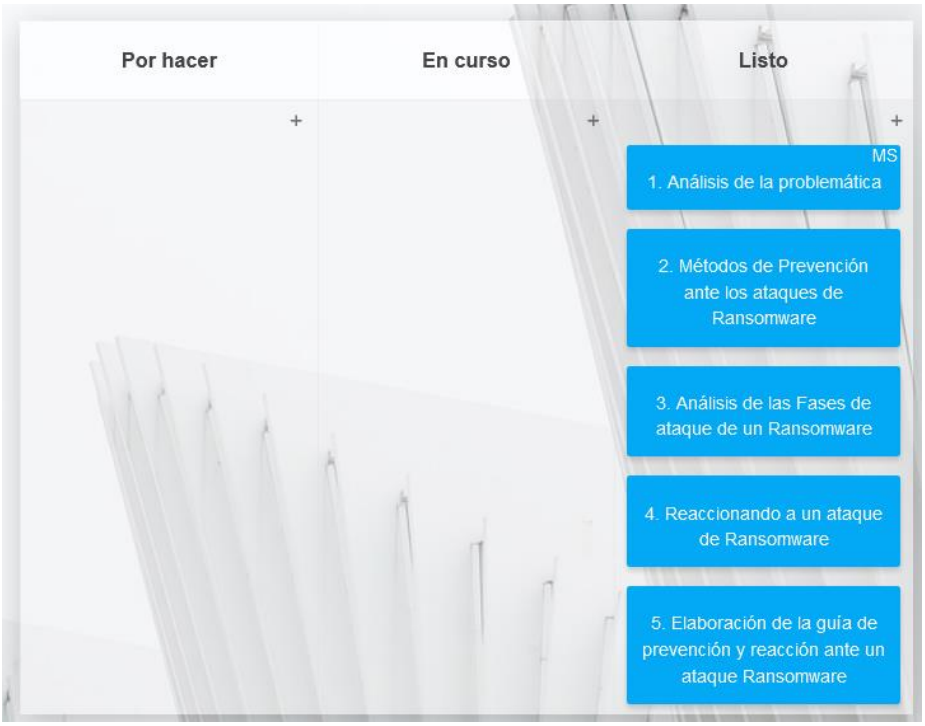
Ante una situación en la cual el ataque ha sido exitoso en una organización, la tarea más importante es la recuperación de datos a través de las copias de seguridad que no han sido afectadas, sin embargo, en el caso de encontrarse que la información está cifrada, es de gran utilidad ingresar al sitio web de ***No More Ransom***, dada la importancia de no pagar por los rescates de información, este sitio es un aporte fundamental en la lucha contra el *Ransomware*, es una iniciativa de varias instituciones (*National High Tech Crime Unit* de la policía de Países Bajos, *European Cybercrime Centre de Europol*, Kaspersky y McAfee), quienes a través de sus aportes y esfuerzos

contribuyen con educar a usuarios sobre este tipo de ataques y que contra medidas utiliza, pero esencialmente, se encargan de poner a disposición de los usuarios las herramientas de descifrado de algunos tipos de Ransomware conocidos.

Sitio web oficial: https://www.nomoreransom.org/es/index.html

Finalizada esta etapa, pasa al tarjetero de Kanban como finalizada.

Figura 14. Tablero Kanban: Elaboración de la guía - LISTO



Fuente: Elaboración propia

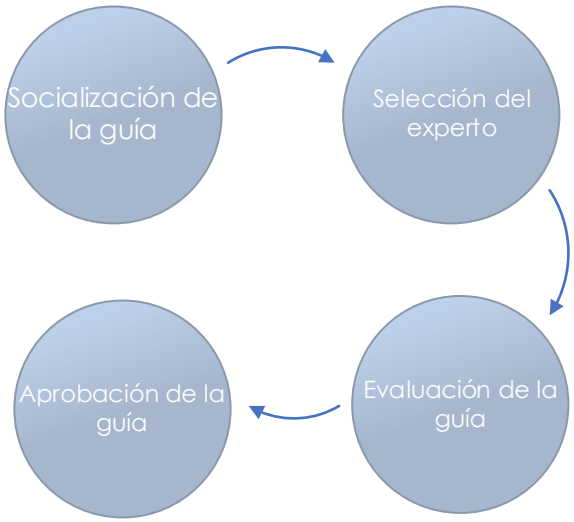
CAPÍTULO III. ANÁLISIS DE RESULTADOS

3.1 Validación de expertos

El propósito de elaborar la presenta guía, fue el evaluar si es que la misma es aplicada de manera general en una organización, por lo tanto, el desarrollo consiste en explicar una serie de herramientas y técnicas que permiten mitigar de mejor manera los ataques de *Ranswomware*, esto sin especificar una arquitectura, software o tipo de organización específica, puesto que sirve como un modelo general y de ayuda a mejorar la seguridad de la información.

Para la evaluación de la guía, se ha considerado contemplar cuatro etapas de la siguiente manera:

Figura 15. Proceso de validación de la guía



Fuente: Elaboración propia

Fase 1: Socialización de la guía:

La Cooperativa de Ahorro y Credito San Francisco Ltda. es considerada una de las instituciones financieras más importantes del país, cimentada en principios cooperativos, se encarga de ofrecer varios servicios financieros desde su nacimiento en el año 1963, fecha en la que inicia sus operaciones con un total de 286 socios, para el año 2010 logra posicionarse en el top 10 de las cooperativas más grandes del segmento 1, el cual comprende aquellas entidades cuyos activos superan los 80 millones de dólares en activos según lo estipula la SFPS (Segmentación de las Entidades del Sector Financiero Popular y Solidario); para el año 2010 logra posicionarse como la segunda empresa más rentable del país, para lograr así su importancia dentro del sector Financiero.

De tal manera que, se ha decidido socializar la guía al oficial de seguridad de la cooperativa, puesto que basado en su experiencia evalúa su utilidad y aplicabilidad, al tomar en cuenta que de manera constante implementa las medidas necesarias para asegurar la seguridad de la información.

Fase 2: Selección del experto:

El Ing. Cristian Vinicio Tabares Burbano, se desempeña como oficial de seguridad de la cooperativa, ha sido seleccionado como profesional afín al área de investigación, dado que trabaja constantemente en algunas funciones generales como:

- Análisis y gestión de riesgos de seguridad
- Análisis y gestión de Incidentes
- Políticas generales de tecnología
- Selección y aprobación de Software de acuerdo a un análisis y cumplimiento de criterios
- Autorizar los cambios que son realizados en el Firewall

- Permisos en la administración de bases de datos
- Permisos de salida e ingreso de información

Fase 3: Evaluación de la guía

Para la evaluación de la guía, se cuenta con un checklist que es calificado por el experto, el mismo que permite conocer su cumplimiento:

Figura 16. Checklist validado por experto de seguridad

GUÍA	
TÉCNICAS DE PREVENCIÓN	**CUMPLIMIENTO**
1. Protección del Perímetro	5
2. Defensas y monitoreo en la red	4
3. Protección de Dispositivos	5
4. Sistemas EDR	5
5. Restricciones de uso de Software	5
6. Infraestructura de escritorios virtuales (VDI)	5
7. Aislamiento de aplicaciones en cliente final (Sandbox)	4
8. Servidores NAS	5
9. Inventario de Datos	5
10. Copias de Seguridad	5
11. Administración integral de la Tecnología	5
TÉCNICAS DE REACCIÓN	
1. Concientización de usuarios	5
2. Manejo de Vulnerabilidades	5
3. Puesta en marcha del Plan de Respuesta a Incidentes	5
4. Incidentes Simulados	5
5. Recuperación de Datos	5
APÉNDICE A: HERRAMIENTAS SUGERIDAS DE PREVENCIÓN	
1. Protección del Perímetro	5
2. Defensas y monitoreo en la red	5
3. Protección de Dispositivos	5
4. Sistemas EDR	5
5. Restricciones de uso de Software	5
6. Infraestructura de escritorios virtuales (VDI)	5
7. Aislamiento de aplicaciones en cliente final (Sandbox)	5
8. Administración integral de la Tecnología	5
9. Pruebas de virus EICAR	5
10. Sitio web (No more ransom)	5

Escala de evaluación:	
5	SE CUMPLE PLENAMENTE
4	SE CUMPLE EN ALTO GRADO
3	SE CUMPLE PARCIALMENTE
2	SE CUMPLE EN UN NIVEL BAJO
1	NO SE CUMPLE

Fuente: Elaboración propia

Fase 4: Aprobación de la guía:

La guía fue aprobada por el Ing. Cristian Vinicio Tabares Burbano como Oficial de Seguridad de la Información a través de un oficio, que se encuentra en el Anexo 1.

3.2 Resultados de validación:

Las recomendaciones realizadas por el experto que ha evaluado la guía, se enfocan principalmente en dos apartados, Defensas y Monitoreo en la Red y Aislamiento de Clientes finales en Sandbox, debido a que considera son temas que son explicados a mayor detalle, las cuales son consideradas como observaciones válidas, sin embargo, debido a toda la información que abarcan, podrían ser estudiados en futuros proyectos de investigación.

El presente proyecto es considerado para cualquier organización como un recurso invaluable en la lucha contra el creciente riesgo de ciberataques, pues proporciona directrices claras y precisas con el objetivo de fortalecer las medidas de seguridad, educar al personal sobre las amenazas existentes y promover una cultura de ciberseguridad proactiva, además, al ofrecer estrategias de seguridad efectivas, la guía permite a la organización minimizar los impactos negativos de un ataque de *Ransomware,* salvaguardar de mejor manera la información y la continuidad de los procesos.

CONCLUSIONES:

- La elaboración de la presente guía incluye varias medidas de prevención y reacción ante un ataque de Ransomware, pero lo más relevante se encuentra en la implementación de soluciones de seguridad como firewalls, la creación de un robusto sistema de respaldos, mantener sistemas actualizados, establecer políticas de seguridad y educar a los usuarios sobre cómo identificar ataques de *pishing*, reduce así la probabilidad de éxito del atacante y fortalece la postura de Ciberseguridad de una organización.

- Para la elaboración del presente proyecto de Investigación y Desarrollo, se ha realizado un estudio de la literatura actual, y a pesar de que existen varias técnicas y herramientas de prevención de Ransomware, estas permiten mejorar la seguridad informática en una organización, pero no garantizan que puedan mitigarse en su totalidad las vulnerabilidades, puesto que ninguna solución es permanente.

- El *Ransomware* es una amenaza constante a nivel mundial, por lo tanto, se concluye que la importancia de la presente guía está enfocada en las técnicas de prevención y diagnóstico anticipado, este tipo de directivas y controles permiten el aislado correcto del respaldo de la información, lo cual impulsa a que la continuidad del negocio, no se vea afectada y los servicios afectados estén disponibles en el menor tiempo posible.

- Se desarrolló un proceso de validación de la guía, el cual contempla cuatro etapas para evaluar su aplicabilidad; dado que cada punto incluido en la presente guía resulta ser útil para cualquier tipo de organización sin importar la tecnología o infraestructura que maneje, busca que se desarrollen planes proactivos en la gestión de la seguridad.

- En la actualidad la formación en Ciberseguridad es un pilar fundamental en la elaboración de estrategias de defensa contra los diferentes ataques de *Malware* y los de tipo *Ransomware* son los más comunes*;* es así que la solución se basa en la prevención, y con este principio la seguridad es considerada como un punto estratégico en el crecimiento organizacional.

RECOMENDACIONES

- Se recomienda que las organizaciones sean conscientes de la amenaza que significa un ataque de *Ransomware,* y tomen en cuenta las prácticas desarrolladas en la presente guía, especialmente en integrar medidas de seguridad perimetral, como el uso de una herramienta *Firewall* que es de software o hardware, conjuntamente con un IDS (*Intrusion Detecion System*) o IPS (*Intrusion Prevention System*).

- Ante el vertiginoso asenso tecnológico que atraviesa la sociedad, el uso de la tecnología móvil y servicios basados en la nube cada vez es más común; por tal motivo, se recomienda estudiar los posibles ataques futuros dirigidos a móviles y dispositivos IoT (*Internet of things*), esto supone nuevos ataques de tipo RoT (*Ransomware of things*) y requiere de nuevas técnicas y herramientas que permitan mitigarlos.

- La seguridad en una organización es primordial, por lo que es recomendable realizar auditorías a los sistemas para poner a prueba su efectividad; se realiza un test de penetración, auditorías de red, seguridad perimetral, web, e incluso si es que existió un ataque previo, una auditoría forense para obtener datos relevantes que permitan evitar un evento similar.

- En el caso de haber sido víctima de un ataque de *Ransomware,* el primer paso a seguir es no pagar por el rescate de la información, dado que esto no garantiza su recuperación, por lo tanto, apoyarse en los equipos de respuesta ante incidentes informáticos (CSIRT) es un buen camino, estos reciben constantemente información de incidentes de seguridad y aportan con bases de conocimiento que permitan actuar inmediatamente.

BIBLIOGRAFÍA

Arantón, L. (2008). Sobre virus y antivirus. *Derma-Red*, 38-41.

Armas , L. (2003). Análisis comparativo de los principales sistemas antivirus. *ACIMED*.

Baidal, D., Triviño, A., Cáceres, A., Mera, R., & Oviedo, B. (6 de Julio de 2021). Análisis y técnicas de prevención ante ataques ransomware. *Revista Tecnológica Ciencia y Educación Edwards Deming*, 18-108. doi:10.37957/ed.v5i1.72

Baluja, W., & Anías, C. (2016). Amenazas y defensas de seguridad en las redes de próxima generación. *Ingeniería y Competitividad*, 7-16.

Brewer, R. (16 de Septiembre de 2016). Ransomware attacks: detection, prevention and cure. *Network Security*. doi:10.1016/S1353-4858(16)30086-1

Celiktas, B. (Junio de 2018). Ransomware, Detection and Prevention Techniques, Cyber Security, Malware Analysis. ResearchGate.

Correa, J., Pérez , H., & Velarde , A. (2016). Virus informáticos. *Conciencia Tecnológica*.

Gil , V., & Gil , J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 193-197.

Gonzalez, D., & Hayajneh, T. (2017). Detection and prevention of crypto-ransomware. *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)* (págs. 472-478). New York City: IEEE. doi:10.1109/UEMCON.2017.8249052

Kanbanize. (2021). *Qué es Kanban: Definición, Características y Ventajas*. Obtenido de Kanban Software for Agile Project Management: https://kanbanize.com/es/recursos-de-kanban/primeros-pasos/que-es-kanban

Lara, E. (2019). *Diseño de un modelo de seguridad de la información, basado en OSSTMMV3, NIST SP 800-30 E ISO 27001, para centros de educación: Caso de estudio Universidad Regional Autónoma de los Andes, extensión Tulcán.* Quito: Universidad Internacional SEK.

Machín, G. (2016). La Ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*, 47-68.

Maestre, J. (2018). *Reconocimiento de anomalías para la detección de instrucciones en.* Madrid .

Mairh, A., Barik, D., Verma, K., & Debasish, J. (2011). Honeypot in Network Security: A Survey. *Proceedings of the 2011 International Conference on Communication,*

Computing & Security - ICCCS '11. Rourkela, Odisha, India. doi:10.1145/1947940.1948065

Mata, I., & Guevara , O. (2010). Virus informáticos, todo un caso, pero no perdido. *CienciaUAT*, 56-61.

Moreno , J., Rodríguez, C., & Leguias, I. (2019). Revisión sobre propagación de ransomware en sistemas operativos Windows. *Revista de I+D Tecnológico*, 1-12.

Ortiz, D. (29 de 07 de 2021). *El Comercio*. Obtenido de Ecuador está entre los países con más ciberataques en América Latina: https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html

Ortiz, D. (22 de 04 de 2022). *El Comercio*. Obtenido de El Comercio: https://www.elcomercio.com/actualidad/blackcat-ataque-hackers-municipio-quito.html

Osorio, A. (2019). *Esquema metodológico apoyado en una herramienta (software) para la detección y prevención de CryptoRansomware en una estación de trabajo.* Medellín: ITM.

Parra , L., & Yánez, E. (Octubre de 2017). ANÁLISIS DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA, UTILIZANDO HERRAMIENTAS. 14. Guayaquil, Ecuador: Universidad de Guayaquil.

Quiroz , S., & Macías , D. (2018). Seguridad en informática: consideraciones. *Ciencias Informáticas*, 676-688.

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. Obtenido de https://digitalcommons.kennesaw.edu/facpubs/4276

Salhuana Albitres, M. (2020). APLICACIÓN DE LA METODOLOGÍA KANBAN EN LA CONSTRUCCIÓN DE UN PROTOTIPO DE SISTEMA WEB PARA GESTIONAR LAS RESERVACIONES DE PAQUETES TURISTICOS EN LA EMPRESA WALK TO PERU. Villa, El Salvador.

Vega, G., Ávila, J., Vega, A., Camacho, N., Berrecil, A., & E. Leo, G. (Mayo de 2014). 523PARADIGMAS EN LA INVESTIGACIÓN. ENFOQUE CUANTITATIVO Y CUALITATIVO. *European Scientific, X*.

Villegas , A. (2018). *Aplicacion de los principios de la Ingeniería del Malware al contexto del Pentesting.* Madrid: Universidad Autonoma de Madrid.

ANEXOS

Anexo 1: Oficio de aprobación de la guía

SAN FRANCISCO LTDA.
COOPERATIVA DE AHORRO Y CRÉDITO

Ambato, 22 de junio del 2022

Señores,

Pontificia Universidad Católica del Ecuador – Sede Ambato

Departamento de Postgrados

De nuestra consideración,

El Oficial de Seguridad de la información de la Cooperativa de Ahorro y Crédito San Francisco Cía. Ltda. el Ing. Cristian Vinicio Tabares Burbano, informa que una vez realizada la validación del proyecto desarrollado por el Ing. Ángel Mauricio Salinas Zambrano con el tema **"GUÍA DE BUENAS PRÁCTICAS PARA PREVENIR Y REACCIONAR ANTE UN ATAQUE DE RANSOMWARE"**, ha determinado que:

Considerando el aumento en los ataques de tipo Ransomware dirigidos a diferentes entidades que poseen información valiosa y confidencial, la guía presentada es de gran utilidad y aplicable en cualquier organización ya que permite determinar los puntos vulnerables para protegerse, monitorear y reaccionar frente a un ataque de esta clase.

Atentamente,

Ing. Cristian Vinicio Tabares Burbano
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

SAN FRANCISCO LTDA. · COOPERATIVA DE AHORRO Y CRÉDITO ·

Ing. Diego Torres
JEFE DEL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN