OFICINA DE POSGRADOS

Tema:

ANÁLISIS FORENSE INFORMÁTICO DE UN SERVIDOR DE ARCHIVOS INSTITUCIONAL

Proyecto de investigación previo a la obtención del título de

Magister en Ciberseguridad

Línea de Investigación:

Seguridad de la información

Autor:

Ing. Jaime Daniel Analuisa Muso

Director:

Ing. Edgar Fernando Solís Acosta, Mg.

Ambato – Ecuador

Marzo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

ANÁLISIS FORENSE INFORMÁTICO DE UN SERVIDOR DE ARCHIVOS INSTITUCIONAL

Línea de Investigación:

Seguridad de la información

Autor:

Ing. Jaime Daniel Analuisa Muso

Galo Mauricio López Sevilla, Ing. Mg. f._____

CALIFICADOR

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

CALIFICADOR

Edgar Fernando Solís Acosta, Ing. Mg. f._____

CALIFICADOR

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

COORDINADOR DE LA OFICINA DE POSGRADOS

Pontificia Universidad Católica del Ecuador
OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Marzo 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo, **JAIME DANIEL ANALUISA MUSO**, con CC. **180432168-3**, autor del trabajo de graduación intitulado: **"ANÁLISIS FORENSE INFORMÁTICO DE UN SERVIDOR DE ARCHIVOS INSTITUCIONAL"**, previa a la obtención del título profesional de Magister en Ciberseguridad, de 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 Universidad.

Ambato, marzo 2022

Firmado electrónicamente por:
JAIME DANIEL ANALUISA MUSO

JAIME DANIEL ANALUISA MUSO

CC. 1804321683

AGRADECIMIENTO

Después de haber culminado esta etapa tan importante con éxito, no me queda más que agradecer a todas y cada una de las personas que de una u otra forma me apoyaron para alcanzar este objetivo de vida planteado, mis principales apoyos y soportes: mis padres, mi tío, mis hermanos y sobrinos.

Así, también, un agradecimiento rotundo por estar siempre ahí a mis amigos, compañeros de estudios, mis docentes, mi tutor y a toda mi familia por haberme apoyado en todo este proceso de formación.

Y, finalmente, un agradecimiento a Dios por darme vida fortaleza y sabiduría para siempre salir adelante ante toda adversidad.

Daniel Analuisa Muso

Maestrante

DEDICATORIA

Capacitarse atrae las oportunidades, por eso, va una dedicatoria muy especial a Dios, por darme la oportunidad de seguir con vida, cumplir este objetivo y día a día crecer como ser humano.

A mi madre que siempre ha confiado en mí, este logro es de los y para los dos gracias por todo.

Y claro está, finalmente, me dedico a mí mismo por todo el esfuerzo y trabajo que me conllevo lograr y completar este peldaño más de vida.

Daniel Analuisa Muso

Maestrante

RESUMEN

El presente proyecto de investigación permite establecer el tipo de ataque que vulneró al servidor de archivos, se aplica un procedimiento de análisis forense informático que permite conservar la integridad y confidencialidad de los datos obtenidos, así, como mantener la cadena de custodia de la evidencia. Es importante, realizar el análisis forense informático al servidor de archivos toda vez que los hallazgos encontrados permiten establecer políticas de seguridad para precautelar la integridad y confidencialidad de los datos que almacena este equipo, así, como implementar acciones que permitan reducir en gran medida futuros ataques. Así, también, se proponen recomendaciones para la aplicación de políticas de seguridad de la información, basado en estándares que permiten asegurar sus datos de tal manera que con la aplicación de estas medidas la institución comprenda de mejor manera sus riesgos de ciberseguridad, administren estos para lograr reducir sus riesgos y protejan tanto su entorno de red como sus datos.

Palabras claves: análisis forense, autopsy, *ransomware*, dharma

ABSTRACT

This research project establishes the type of attack that violated the file server, applying a computer forensic analysis procedure that allows to preserve the integrity and confidentiality of the data obtained, as well as to maintain the chain of custody of the evidence. It is important to perform the computer forensic analysis to the file server since the findings will allow establishing security policies to protect the integrity and confidentiality of the data stored in this equipment, as well as to implement actions to greatly reduce future attacks. Recommendations are also proposed for the implementation of information security policies, based on standards that allow to secure their data in such a way that with the application of these measures the institution better understand their cybersecurity risks, manage them to reduce their risks and protect both their network environment and their data.

Keywords: forensic analysis, autopsy, ransomware, dharma

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El análisis forense hoy en día, se ha convertido en un proceso de vital importancia para investigadores informáticos, es así, que las investigaciones desarrolladas en este campo de estudio son muy dividas y dispersas, cada auditor forense tiene una técnica propia adecuada en los diferentes dispositivos que analiza y escanea, el equipo o persona que realiza esta labor pretenden identificar y preservar la evidencia digital como primer paso para, así, analizar e inspeccionar datos en la búsqueda de evidencia que permita esclarecer o hallar indicios relacionados al caso de estudio.

Actualmente el uso de dispositivos electrónicos sean estos computadores, teléfonos celulares, tables, dispositivos de Internet de las Cosas (IoT, por sus siglas en inglés) entre otros, en la mayoría de actividades, que se realiza tanto en oficina como en el hogar permite al usuario final estar interconectados con personas de todo el mundo a través de internet, es este un punto de vulnerabilidad muy grande en la privacidad de la información, que se transmite, al no tomar medidas de precaución necesarias para proteger la integridad y confidencialidad de lo, que se genera y almacena en los dispositivos.

En Ecuador, actualmente, de acuerdo con una publicación de Ecuavisa del 2 de septiembre de 2021, se han registrado más de 1200 investigaciones por delitos informáticos (Ecuavisa, 2021), actualmente estos casos están tipificados dentro del marco normativo del Código Integral Penal (COIP) de acuerdo con el tipo de delito cometido, es aquí donde el análisis forense desempeña un papel importante a la hora de esclarecer casos en donde la evidencia a analizar es un equipo informático. Sin embargo, el análisis forense no solo busca esclarecer hechos delictivos, también, tiene otro propósito como recuperar información para ser analizada y tomar decisiones que permitan asegurar el activo.

En la actualidad, como es de conocimiento público varias instituciones sufren ataques informáticos a sus activos lo que deja perdidas notables, es así, que de acuerdo a información emitida por diario El Comercio, se da a conocer que los ataques informáticos a las pequeñas y medianas empresas (PYMES) van en crecimiento(Ortiz, 2021), para este grupo de empresas el proteger la información

de sus clientes les supone un alto valor de inversión, sin embargo, esto pone en peligro a las mismas en caso de sufrir un ciberataque lo que conllevaría a las instituciones varios problemas a más de la perdida de información, así como, también, temas legales; situación que acarrearía una gran problemática que causaría incluso que estas cierren sus empresas.

En la presente investigación, se analiza la siguiente problemática: un servidor de archivos víctima de un ciberataque, dado que la institución provee de varios servicios tanto a su personal interno como a sus clientes, pone este activo en un riesgo constante de sufrir algún ataque informático y aumenta la vulnerabilidad de la información almacenada al momento, que se da este suceso, es así, como este caso de estudio tiene como finalidad buscar información para conocer cuál fue la brecha de seguridad que aprovecharon los atacantes para comprometer al activo.

El análisis forense informático realizado al servidor de archivos conlleva ejecutar varias fases de estudio que permite preservar, analizar y recuperar información de ser el caso y así determinar, si, ha sido o es víctima de un ciberataque, por otra parte, medir el impacto provocado en la integridad y confidencialidad de la información que este equipo almacena en caso de existir una vulneración de seguridad informática; con el desarrollo de la presente investigación, se plantea el siguiente objetivo general: Proponer recomendaciones de seguridad basadas en un análisis forense al servidor de archivos de la institución, para precautelar la información almacenada en el servidor que forma parte de los activos en la institución, y que al momento de producirse un ciberataque, se minimice el impacto.

A esto, se suman los siguientes objetivos específicos:

1. Identificar la base teórica que permite implementar procedimientos de análisis forense.
2. Determinar una metodología adecuada acorde a los procesos legales vigentes para implementar el análisis forense.
3. Desarrollar pruebas sobre la metodología de análisis forense planteada.
4. Generar informes sobre el análisis forense realizado al servidor de archivos de la institución.

Además, para el tema en estudio, se realiza una investigación bibliográfica para determinar, si, existe un tipo de metodología establecida donde, se conoce el proceso para ejecutar el análisis forense a un servidor de archivos, una vez revisada la literatura relacionada al tema en estudio, la metodología utilizada, se divide en fases de acuerdo con lo establecido en el apartado 2.2 del libro Gestión de Incidentes de Seguridad Informática, que da a conocer la metodología del análisis forense informático, misma que va más allá de solo elaborar un informe final con las evidencias encontradas, también, establece actividades posteriores donde, se determinan medidas de mitigación al ataque investigado, todo esto basado en la gestión del riesgo como lo indica (Tejada, 2015), es así, que el análisis forense al servidor de archivos, se realiza de acuerdo a las siguientes fases y procedimientos:

Fases:

- Estudio preliminar
- Recopilación de evidencias
- Análisis de evidencias
- Informe

Procedimientos:

- Preparación
- Detección
- Análisis preliminar
- Contención, erradicación y recuperación
- Investigación
- Actividades posteriores

Los procedimientos y fases anteriormente indicados, realizan una búsqueda de casos que impliquen: alteración de información, espionaje, conflictos laborales, investigaciones de fraude, uso inadecuado de internet y correo electrónico en el lugar de trabajo, asuntos relacionados con falsificaciones, investigaciones de bancarrota, análisis de encriptación de datos entre otros. De acuerdo a lo indicado anteriormente, se tiene un antecedente que en el país, se han dado varios ciberataques de manera constante, es así, que surge la necesidad de realizar un análisis forense informático al servidor de archivos vulnerado perteneciente a la

institución, que por motivos de confidencialidad, no se revela el nombre de ésta, con la finalidad de recabar información que permita establecer cuál fue la brecha de seguridad que los atacantes aprovecharon para acceder al servidor y perpetrar un ataque al mismo.

En la presente investigación, se evidencian procesos donde, no se tomaron las medidas de seguridad informática respectivas y permitieron al atacante cometer una alteración de datos. Es así, como la institución parcha bugs de seguridad en caso de existir y minimizaría los ataques suscitados en contra de sus activos, por lo tanto, la institución obtiene un beneficio en lo relacionado a seguridad de la información, el análisis del ataque permite conocer a fondo la causa de este y aplicar medidas de seguridad informática para lograr afianzar su confiabilidad con sus clientes, además, de impedir que una interrupción de un servicio afecte a la continuidad del negocio.

Tal es el aporte del caso de estudio del equipo, que de acuerdo con los hallazgos encontrados, se utilizan para analizar y comparar ataques en equipos de similares condiciones en búsqueda de posibles brechas de seguridad que den paso a la ejecución de ciberataques parecidos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

En el presente capítulo, se analizan conceptos importantes que ayudan a comprender los procedimientos y pasos que conlleva realizar el análisis forense informático a un servidor de archivos.

1.1. Estado del arte

Dado que el análisis forense es una recopilación de información de un sistema operativo que permite al investigador buscar evidencias con las, que se establecen los posibles indicios de cuál fue la brecha de seguridad aprovechada por un atacante para vulnerar el equipo, es así, como habría dos escenarios a analizar, el primero, si, el equipo está en funcionamiento (encendido) y el segundo, si, está apagado.

Al investigar el primer escenario, se obtienen detalles más a fondo del ataque, que se produce en ese instante, es así, como en la investigación realizada por Dija et al (2017), se determina que uno de los puntos importantes a analizar es la navegación web en un ataque donde el equipo esté encendido, toda la información hallada es volátil y al momento de apagarlo, se pierde información de mucho valor para establecer la causa del ataque producido, sin embargo, el análisis en caliente causa alteración de la evidencia, para la obtención de datos en vivo, se requiere la ejecución de un programa en la máquina del sospechoso.

En otro caso de estudio, se analiza un ataque en vivo, donde Rusydi et al (2018), propone una solución de investigación para el análisis forense de datos en vivo, este caso da a conocer, que se extrae información de la memoria RAM donde, se almacenan sesiones de uso del computador, es importante, analizar los eventos, que se suscitan en el equipo analizado, en la actualidad el mayor medio de acceso para intercambiar información con todo el mundo es a través de internet con el uso de un navegador web.

El caso de estudio realizado por Suma et al (2017), permite conocer que debido al alto uso de internet este es uno de los medios que permite a un atacante comprometer un equipo, y dado que en la actualidad existe un crecimiento en los

delitos informáticos suscitados, relacionados con transacciones bancarias, redes sociales entre otros, aquí el análisis forense del navegador desempeña un papel importante a la hora de proporcionar información relevante en un delito cibernético investigado. Esto, se da porque los navegadores web crean un número de archivos en el sistema local en el momento de la navegación por Internet.

Los dispositivos móviles hoy en día, tienen una tendencia de crecimiento en su uso, sin embargo, al acceder a internet, se lo hace a través de un navegador web, entre los más utilizados están Google Chrome y Mozilla Firefox.

> La evidencia generada por los navegadores web, también, es importante, en muchas investigaciones penales. Una pregunta común de investigación es, si, un usuario designado realmente visitó un sitio web determinado en un momento especifico, respuestas a esta pregunta ayudarían a explicar la motivación (por ejemplo, visitar sitios web extremistas o descargar propaganda), probar o refutar la comunicación (por ejemplo, comunicarse con otros usuarios en foros o vía correo web), o para comprobar, sí, hay coartadas (por ejemplo, la actividad del usuario en el tiempo períodos de ausencia reclamada). Las principales fuentes de evidencia en los navegadores web son el historial del navegador, una característica común que permite avanzar / retroceder navegación a sitios web visitados, y la caché del navegador, un componente de software que almacena contenido web reciente por motivos de rendimiento (Gros, Dirauf, & Freiling, 2020).

Prabhu et al (2019) estudia un método de recuperación de los artefactos del navegador web para la realización de una investigación forense, se basa en la recuperación de la información eliminada con el uso del archivo index.dat, consiste en:

> Recuperar historiales, que se eliminaron a lo largo del período anterior, recuperar información del historial eliminada con archivos de registro. Las computadoras con sistema operativo Windows contienen una extensión de archivo que almacena información subjetiva, que se llama index.dat y es un archivo oculto en la computadora que contiene todos los sitios web que ha visitado y muestra cada URL.

En las investigaciones analizadas, se identifica que el uso de un navegador web para acceder a internet, independientemente del sistema operativo, genera un registro muy importante, que es analizado por el examinador forense en busca de evidencia para conocer a fondo la brecha de seguridad que aprovechó un atacante para comprometer un equipo de cómputo.

Ahora bien, al no existir trabajos similares al caso de estudio, se revisaron trabajos relacionados al área forense como los anteriormente detallados, en su mayoría hablan de recuperación de evidencias basados en los registros y rastros que deja un navegador web.

1.2. Servidor

“Un servidor (del inglés Server) es un ordenador que permite compartir sus periféricos con otros ordenadores” (Cabrera, 2014, p. 45). Estos son de varios tipos y entre ellos, se encuentran los siguientes:

- Servidor de archivos: almacena archivos compartidos de forma privada con los usuarios de una red.
- Servidor de impresión: comparte con usuarios de la red una o más impresoras conectadas.
- Servidor de aplicaciones: suministra a las aplicaciones de un sistema servicios a través de su infraestructura.
- Servidor de comunicaciones: interconecta redes locales o una red local con minicomputadoras o macrocomputadoras.
- Servidor de correo electrónico: brinda el servicio de correo electrónico en la red.
- Servidor Web: almacena y administra documentos HTML, su acceso, se hace a través de los navegadores web.
- Servidor FTP: almacena e intercambia archivos en la red que son accedidos por los usuarios.
- Servidor proxy: conmuta paquetes que permite enmascarar la dirección IP para ocultar datos de la red interna a internet.

Según el sistema operativo, así, como el tipo de red, que se utiliza y las necesidades de las instituciones, los distintos tipos de servidores, se encuentran en el mismo ordenador o distribuidos entre todos aquellos que forman parte de la red, los servidores de archivos, se establecen como dedicados o no dedicados, esto de acuerdo con su tipo de uso y donde su trabajo sea únicamente la gestión de red, además, se utiliza como estación de trabajo. El tipo de uso, que se dé al servidor, se basa en la cantidad de estaciones de trabajo presentes en la red, a mayor número de equipos, es recomendable usar un servidor dedicado, sin embargo, al usar un servidor no dedicado como estación de trabajo, existe el riesgo de presencia de problemas, todo el sistema que depende del equipo deja de funcionar y produce pérdidas irreparables.

1.2.1. Servidor de archivos

Es un servidor central mediante el que en una red de computadoras comparte sus recursos. Para la implementación de este servidor es necesario abarcar características tanto de software como hardware y de acuerdo con los permisos, que se asignen a los usuarios, estos accedan a carpetas y archivos compartidos sea para consulta, modificación, eliminación o carga («IBM Docs», 2021).

El servidor de archivos permite que varios usuarios accedan a archivos almacenados en este equipo, otros de sus usos es realizar funciones de servidor de descarga a través de la web logra, así, que los clientes y usuarios obtengan contenido como música, videos, imágenes, actualizaciones, programas o controladores.

También, permite realizar copias de seguridad, es decir, que trabaja en la creación y almacenamiento de estos respaldos, en base a los requerimientos del usuario conforme los archivos de sistema, que se guardan. El usar esta funcionalidad, es una opción económica que permite, a cada cliente mantener una copia de sus datos, en el caso que el servidor tenga acceso a internet, los datos almacenados están disponibles de forma remota, es decir, brindan servicio de almacenamiento online, sin embargo, en comparación de las soluciones en la nube, aquí existe un control total de todos los archivos y su seguridad.

Ventajas

- El ordenamiento de archivos, se realiza de manera sencilla.
- Estructura fácil de visualizar.
- Fácil intercambio de archivos.
- Control sobre versiones de archivos para evitar errores.
- Reduce la carga de datos que manejan los clientes.
- Acceso a remoto con el uso de WebDAV, SFTP o SCP.
- Control en la protección y seguridad de los datos.

1.2.2. Sistemas Operativos en servidores

Existen varios tipos de sistemas operativos para servidores, entre los más usados, se encuentran los siguientes:

- Microsoft Windows Server
- Servidores Linux/Unix
- Servidores en la nube

Estos sistemas permiten aprovechar al máximo las características de hardware y software que tienen los servidores (Tanenbaum, 2003).

Microsoft Windows Server

Fue el primer sistema operativo de Microsoft usado para trabajar en entornos de grupo, esta versión permite configurarse para permitir compartir recursos y responder a las solicitudes de los clientes en la red.

De acuerdo con Microsoft (2021) la versión más actual de su sistema operativo en la línea de servidores es Windows Server 2022, esta versión cuenta con características como: seguridad multicapa avanzada, funcionalidad híbrida con Azure, plataforma de aplicaciones flexible, entre otras.

Servidores Linux/Unix

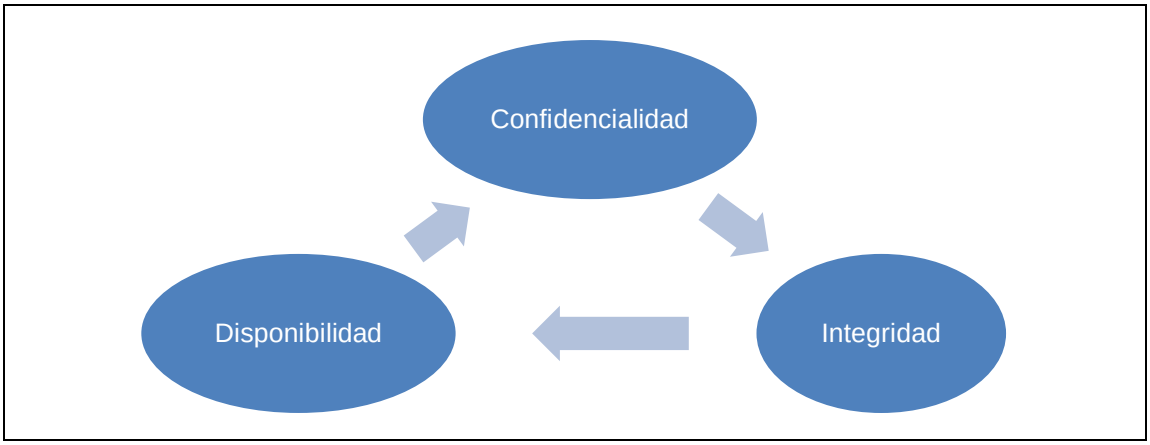
Un servidor Linux es un sistema operativo de código abierto de Linux, este ofrece a un bajo costo para las empresas la opción de brindar contenido, aplicaciones y servicios a sus clientes, al ser de código abierto existe una gran comunidad que permite obtener una constante actualización y mejora de los recursos que este sistema maneja.

Se encuentran varios sistemas basados en Linux, por ejemplo, uno de los más usados en servidores web, es CentOS, sin embargo, para atender peticiones a varios miles de usuarios, es necesario migrar a una solución que brinde estas características como, por ejemplo, Red Hat Enterprise (Banquet & Bobillier, 2015).

1.3. Ciberseguridad

La información digital generada hoy en día por las personas tiene un altísimo valor, sean estos, textos, datos, medidas, documentos, entre otros, lo que aporta valor a las instituciones, de acuerdo con Singh et al. (2022) hoy en día las empresas tienen como objetivo mantener sus sistemas seguros de manera continua y efectiva, es así, que basan la seguridad de la información en tres pilares que son Confidencialidad, Integridad y Disponibilidad, también, conocida como triada CID, como se observa en la Figura 1, este modelo basa su diseño en políticas de seguridad de información para las instituciones, si uno de estos pilares falla o presenta alguna debilidad automáticamente la o las instituciones quedan expuestas a un ataque, además, en su estudio revela cinco temas centrales de la investigación en ciberseguridad que son: (a) inteligencia artificial en ciberseguridad, (b) redes y seguridad de plataformas, (c) algoritmos y métodos, (d) optimización y modelado, y gestión de la ciberseguridad.

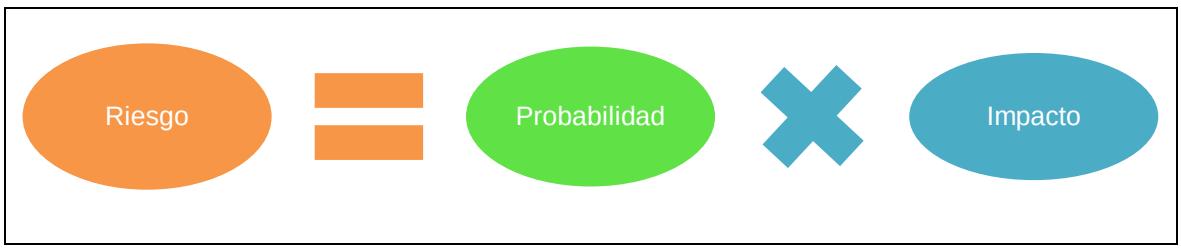
Figura 1. Triada CID



Fuente: elaboración propia

Por lo tanto, en seguridad de la información las instituciones toman en cuenta factores como riesgos, amenazas y vulnerabilidades, estos afectan de forma directa a sus recursos informáticos; aquí existen recursos tangibles, en este caso, es toda la infraestructura física e intangibles, es está toda la información que disponen las instituciones, es decir, documentos de texto, bases de datos y similares. En la actualidad el responsable de trabajar en el área relacionada con la seguridad de la información de las instituciones, se encarga de evaluar los riesgos que tiene un sistema, esto en basado en las amenazas y vulnerabilidades de los recursos que manejan, es así, como al tener que cuantificar el riesgo, se basa en un análisis cuantitativo, en la Figura 2, se observa la fórmula que mide el riesgo, el método de cálculo, consiste en multiplicar los factores probabilidad e impacto.

Figura 2. Cálculo del riesgo



Fuente: adaptado de Tejada (2015)

Factores que permiten calcular el riesgo son las amenazas que tiene un sistema, sin embargo, existen diferentes tipos de estas como las naturales, errores humanos y voluntarias; en los errores humanos, por ejemplo, se da el caso donde una persona elimina información de un servidor accidentalmente debido a un desconocimiento de la tarea que realiza, es por esto por lo, que se considera como una amenaza, sin embargo, los voluntarios, es uno como en el caso de estudio donde un ataque perpetrado a un sistema o equipo informático produce una afectación.

Mukhopadhyay y Prajwal (2021) indica que hoy en día debido a la pandemia del COVID 19 las huellas digitales, que se dejan en línea cada vez van en aumento, es así, que para los piratas informativos el phishing a través de correos electrónicos, se ha convertido en el principal método de ataque para atrapar a víctimas y engañarlos con falsos programas maliciosos integrados para ejecutar un ciberataque, el método de ataque que usan es engañar a sus víctimas fácilmente con el uso de vulnerabilidades únicas, dinámicas y varias diferentes a un virus estándar, es así, que el software de detección de malware que las empresas de TI proporcionan a sus empleados y a los usuarios de Internet en general no detectan estos ataques;

1.3.1. Ransomware

Ransom palabra del idioma inglés que a su traducción indica rescate y *ware* mercancía, es así, que traducido al idioma español este indica secuestro de datos; es un tipo de programa malicioso que infecta un equipo, de acuerdo con Kaspersky Lab empresa de ciberseguridad indica que “el *ransomware* es una clase de malware que representa un riesgo para ti y para tu dispositivo” (Kaspersky, 2021).

Hoy en día la mayoría de ataques informáticos, se basan en la infección por *ransomware,* sin embrago, este tipo de sucesos no es nuevo, de acuerdo con Malwarebytes (2021) empresa especializada en la fabricación de software anti-malware “el primer ransomware, conocido como PC Cyborg o AIDS, fue creado a finales de los 80. PC Cyborg cifraba todos los archivos del directorio C: después de reiniciar 90 veces, y después exigía al usuario renovar su licencia mediante el envío de 189 dólares por correo postal a PC Cyborg Corp”.

Ekta y Bansal (2021) menciona que el *ransomware* es el ataque cibernético más peligroso del mundo, impide que los usuarios accedan a sus dispositivos, se bloquea la pantalla del dispositivo del usuario y/o cifran los archivos. Este malware es dañino que causa un efecto negativo en los equipos infectados, pérdida y restricción al acceso de información, encriptación de datos, uno de los objetivos que tiene un ataque de *ransomware* es el solicitar un rescate a cambio de devolver la información sustraída o de retornar el acceso al equipo infectado, también, un simple ataque que muestra un sistema aparentemente seguro que fue vulnerado.

Lee et al. (2021) da a conocer 10 ataques suscitados en los últimos 5 años, que hacen uso de varias técnicas para comprometer la confidencialidad integridad y disponibilidad de los datos, así, como de los equipos víctimas de ataque, también, se evidencia que la capacidad de los atacantes para ofuscar su malware es muy avanzado de tal manera que hoy en día, se desarrolla malware sin archivos para eludir las técnicas de detección existentes.

Tipos de *ransomware*

Malwarebytes (2021) indica que existen tres tipos de *ransomware*, cada uno valorado de acuerdo a la gravedad que causa su ataque es, así, que estos van desde algo molestos hasta los que causan un nivel de crisis alto como ejemplo crisis de los misiles de rusia; entres los principales tipos están los siguientes:

Scareware

Ransomware no muy peligroso, sin embargo, este tiene como propósito engañar a través de varias clases de software que llevan a visitar sitios infestados de malware para intimidar a los usuarios de forma que paguen un monto por el rescate de sus datos y/o equipo atacado o a su compren un software que elimine la infección en, si, es un ataque al engaño.

Bloqueadores de pantalla

Este ataque bloquea la pantalla del equipo, asusta a la víctima y la acusa de almacenar información relacionada a actividades ilegales en sus dispositivos

electrónicos, este ataque muestra en pantalla un mensaje, suplantando a la policía o similares.

Un aspecto importante para tomar en cuenta en este tipo de ataque, es que ninguna autoridad legal actúa de esta manera y mucho menos solicita una recompensa a cambio de devolveré el acceso al equipo, sin embrago este ataque causa perdida de información valiosa como fotografías en dispositivos móviles.

***Ransomware* de cifrado**

Hoy en día el ataque que más daño causa es tal el grado de afectación que tiene, es el peor de todos, secuestra archivos a los que les aplica un grado de cifrado, para posterior exigir un pago a cambio de devolver el acceso, en este ataque es casi imposible recuperar la información afectada, de momento existe muy pocas herramientas de software que permiten descifrar datos, claro está aquí indicar que esto depende del tipo de *ransomware*, se recomienda nunca pagar por el rescate, además, el pago no garantiza que la información sea devuelta, es por esta razón que este ataque es considerado como el que produce un altísimo grado de afectación en un sistema.

1.3.2. Análisis Forense informático

El análisis forense informático (AFI) usa técnicas científicas y análisis especializado en las infraestructuras tecnológicas, de ser el caso, que se produzca una vulneración permite detectar amenazas, que se analizan en busca de causas que dieron lugar a un ataque.

Las técnicas que usa el AFI permiten identificar, preservar, analizar y elaborar un detalle de los datos investigados, es importante, indicar que este proceso extrae información sin alterar su estado original, es así, como esto es aceptado en un proceso legal; toda vez, que se detecta una amenaza y se materialice, se realiza un análisis forense donde, se averigua detalles como: causante, origen, método de ataque y debilidades de un sistema que permitieron su vulneración.

1.3.3. Responsabilidades de un forense informático

Para la realización del AFI existe una persona responsable de ejecutar este proceso, quien se encarga de hacer frente al ataque informático, es decir, investiga, recaba y analiza toda la evidencia digital posible para esclarecer la causa que dio lugar al ataque, se genera un informe válido en caso de tener un proceso judicial de por medio.

1.3.4. Herramientas para el análisis forense informático

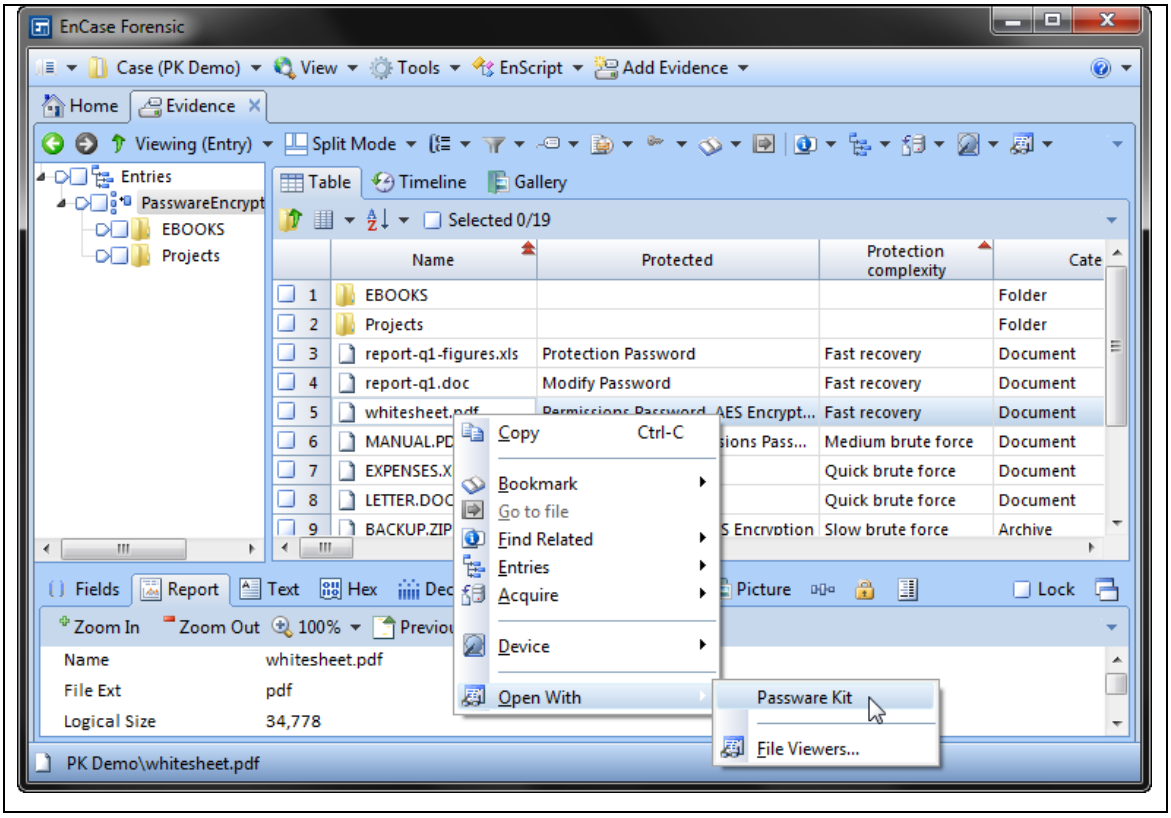
Hoy en día, existe un sinnúmero de herramientas en diferentes categorías como software libre de distribución, *open source*, así, como software comercial, aquí, es importante, indicar que los atacantes usan técnicas y herramientas muy sigilosas, así, como métodos que dificultan el análisis del ataque. López Delgado (2007) en su libro análisis forense digital indica herramientas de utilidad para realizar el AFI, los atacantes cada día mejoran sus técnicas para vulnerar un equipo, por eso, es fundamental, conocer herramientas que permiten extraer analizar y procesar evidencia digital que mejoren sus entornos de manera periódica, a continuación, se citan algunas:

Encase

Herramienta que de acuerdo con información detallada en su web indica: “Las dos características principales que hacen de EnCase una herramienta software única son la variedad de sistemas operativos y sistemas de archivos que admite” (ONDATA, 2021).

Al existir varios sistemas operativos como Windows, Linux, Solaris, AIX y OSX, EnCase ofrece analizar con profundidad todos los componentes de estos, también, interpreta otros sistemas de archivos para los, cuales, actualmente no existe un programa desarrollado, en la Figura 3 , se observa la interfaz con que trabaja.

Figura 3. Interfaz Encase



Fuente: Tomado a partir de ONDATA (2021)

OsForensics

Herramienta que permite extraer evidencia forense en equipos de cómputo de forma rápida, hace uso de búsquedas con indexación de archivos, identifica archivos sospechosos, compara firmas de las unidades, analiza correos electrónicos, memoria entre otros.

Trabaja con varios formatos de archivos como: WPD, SWF, DJVU, JPG, GIF, PNG, TIFF, MP3, DWF, DOCX, PPTX, XLSX, MHT, ZIP, PST, MBOX, MSG, DBX, ZIP, ZIPX, RAR, ISO, TAR, 7z, DOC, DOCX, PDF, PPT, XLS, RTF, realiza una búsqueda por nombre de archivo, tamaño, fecha de creación o modificación y trabaja en un entorno similar a un sistema operativo Windows.

En la Figura 4, se observa la interfaz con que trabaja, además, dentro de sus características muestra una línea de tiempo, para visualizar las actividades que realizó el equipo analizado.

Figura 4. Interfaz OSForensics

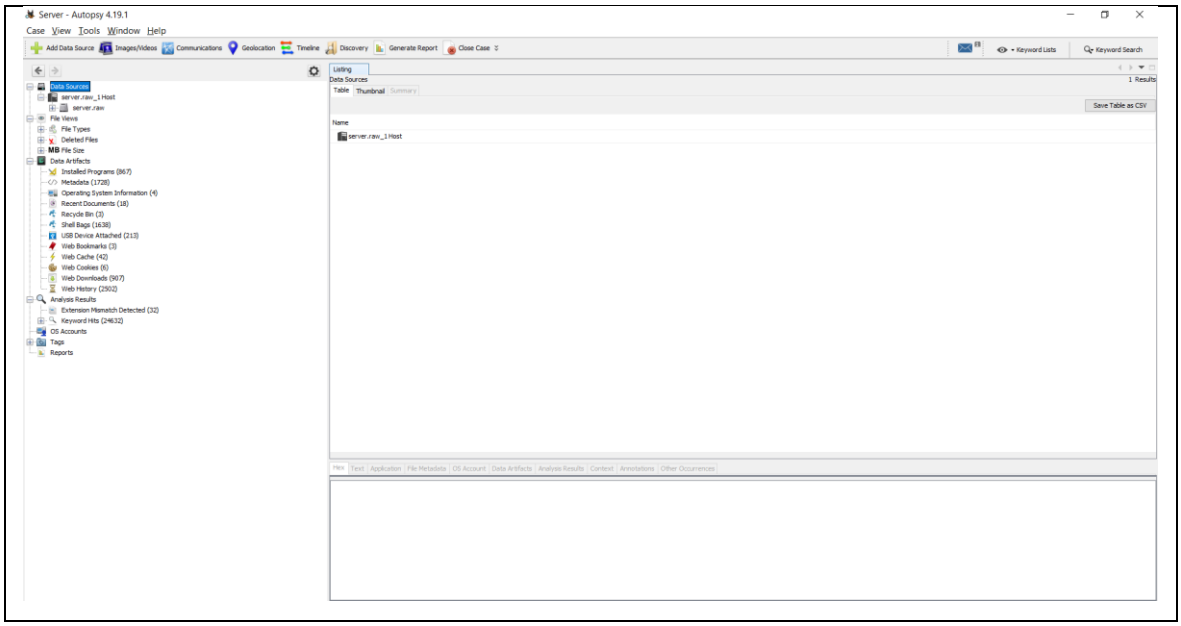
Fuente: tomado a partir de OSForensic (2021)

Autopsy

Autopsy (2021) indica que “es la principal plataforma forense digital de código abierto de extremo a extremo. Creado por Basis Technology con las características principales que espera de las herramientas forenses comerciales, es una solución de investigación de disco duro rápida, completa y eficiente que evoluciona con sus necesidades”.

Al ser de código abierto, en el presente proyecto de investigación se trabaja con esta herramienta, dispone de varios módulos para realizar una búsqueda de información en la imagen forense del servidor de archivos, además, esta plataforma es fácil de usar y tiene capacidad para analizar todo tipo de medios digitales y dispositivos móviles, en la Figura 5, se observa la interfaz de trabajo.

Figura 5. Interfaz Autopsy



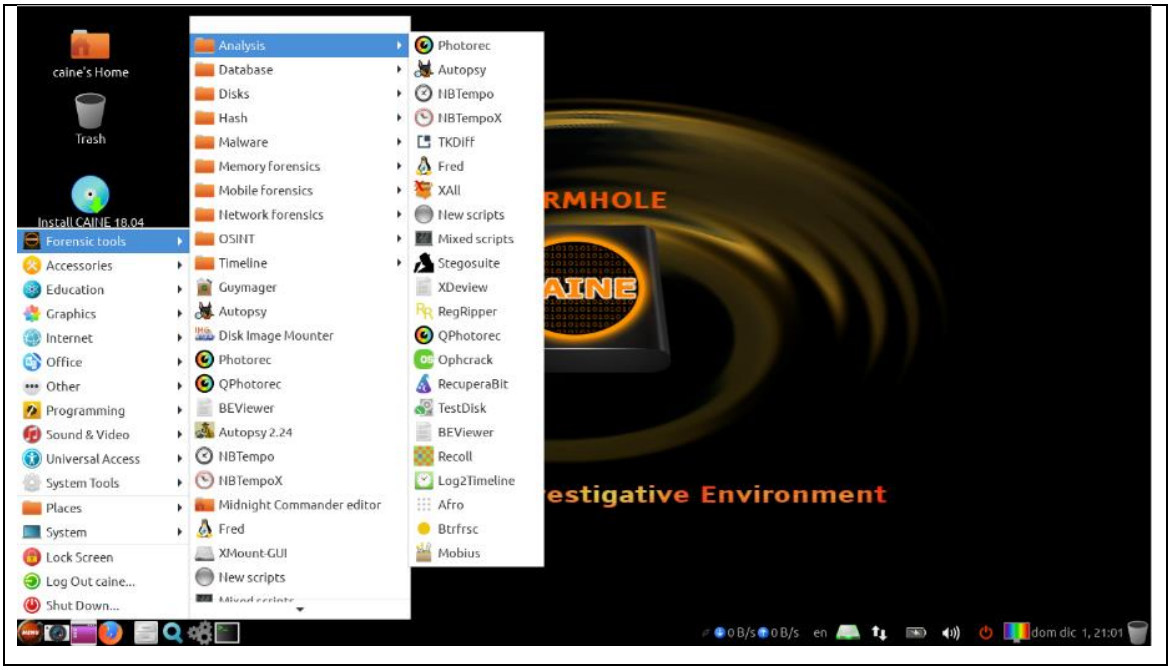
Fuente: elaboración propia

Caine

Nanni (2021) indica que “CAINE (*Computer Aided Investigative Environment*) es una distribución en vivo de GNU / Linux italiana creada como un proyecto de Digital Forensics”.

Este sistema ofrece un entorno de trabajo personalizado para el área forense, íntegra herramientas de software para el AFI con una interfaz gráfica amigable, tiene como objetivo garantizar una interoperabilidad que apoye al investigador forense en las 4 fases de la investigación, en la Figura 6, se observa la interfaz de trabajo.

Figura 6. Interfaz de Caine



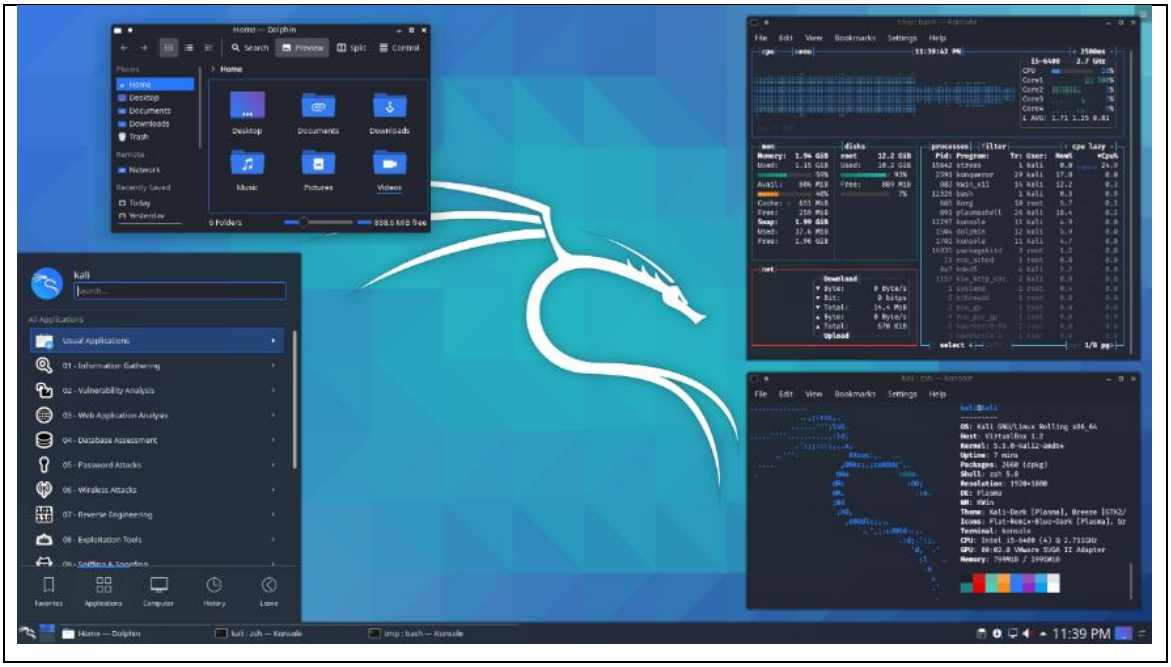
Fuente: tomada a partir de Nanni (2021)

Kali Linux

“Es una distribución de Linux de código abierto basada en Debian orientada a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa” (Kali Linux, 2021).

Kali Linux, no es un sistema operativo ni una herramienta, más bien es catalogada como una plataforma que íntegra varias herramientas y utilidades para recopilar información, también, permite elaborar informes, evaluar la seguridad de los sistemas operativos, en la Figura 7, se observa la interfaz de trabajo.

Figura 7. Interfaz de Kali Linux



Fuente: tomada a partir de Kali Linux (2021)

1.4. Normativa forense en el entorno jurídico

En Ecuador, existe normativa expresa para tipificación y juzgamiento de delitos, está es el Código Integral Penal (COIP) que en su art.1 indica

> Finalidad. – Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas (Asamblea Nacional del Ecuador, 2021).

Dentro del COIP la sección que permite juzgar un ciberdelito, se basa en la aplicación de la Sección Tercera, que abarca lo relacionado a delitos contra la seguridad de los activos de los sistemas de información y comunicación.

> Art. 229.- Revelación ilegal de base de datos. – La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un

sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años (Asamblea Nacional del Ecuador, 2021, p. 68).

Art. 230.- Interceptación ilegal de datos. – Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (Asamblea Nacional del Ecuador, 2021, pp. 68-69).

Art. 231.- Transferencia electrónica de activo patrimonial. – La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será

sancionada con pena privativa de libertad de tres a cinco años (Asamblea Nacional del Ecuador, 2021, p. 69).

Art. 232.- Ataque a la integridad de sistemas informáticos. – La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción, se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (Asamblea Nacional del Ecuador, 2021, p. 69).

Art. 233.- Delitos contra la información pública reservada legalmente. – La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando, se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis

> meses, siempre que no se configure otra infracción de mayor gravedad (Asamblea Nacional del Ecuador, 2021, p. 69).
>
> Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Asamblea Nacional del Ecuador, 2021, p. 69).

En el presente caso de estudio, se aplica el Art. 232 porque se vulnera la integridad del activo con el ataque producido.

La Organización Internacional de Normalización (ISO) en su norma ISO/IEC 27037, establece directrices para la identificación, recopilación, adquisición y preservación de evidencia digital, sin embargo, esta norma no estudia la fase de análisis de la evidencia, al contrario, provee una guía que sirve para los siguientes dispositivos y/o funciones, que se utilizan:

- Medios de almacenamiento digital utilizados en computadoras estándar como discos duros, disquetes, discos ópticos y discos magnéticos, dispositivos de datos con funciones similares
- Teléfonos móviles, Asistentes Personales Digitales (PDA), Dispositivos Electrónicos Personales (PED), tarjetas de memoria
- Sistemas de navegación móvil
- Cámaras digitales y de video (incluido CCTV)
- Computadora estándar con conexiones de red
- Redes basadas en TCP/IP y otros protocolos digitales
- Dispositivos con funciones similares a las anteriores

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Metodología y enfoque de la investigación

En el análisis forense la recopilación, análisis e interpretación de datos es el pilar fundamental para que los resultados obtenidos producto de este trabajo sean válidos, para el presente proyecto, se selecciona el siguiente tipo de investigación:

1.4.1. Investigación cuantitativa

Dado que el escenario de estudio requiere de una investigación experimental, se analizan posibles vulneraciones de seguridad del servidor de archivos, por esta razón, es necesario recopilar datos confiables y precisos que permiten determinar en qué medida afecto el ataque producido al equipo.

1.4.2. Investigación bibliográfica

Se usa este método, para revisar toda la literatura relacionada al campo de estudio, en el país, se han suscitado varios ciberataques a diferentes instituciones, por esta razón, es importante, identificar a fondo el tipo y objetivo que tienen estos sucesos; esta búsqueda y análisis establece que la información, que se compromete en los equipos es muy valiosa, por esta razón es necesario establecer procesos y modelos para realizar un análisis forense y establecer datos que contribuyen para esclarecer estos delitos informáticos.

1.4.3. Investigación de campo

La presente investigación al contar con un servidor de archivos que probablemente fue víctima de un ciberataque, es necesario realizar una investigación de campo, así como, también, extraer una copia bit a bit sin alterar ningún dato y recabar información del lugar en donde el equipo estaba en funcionamiento para, así, analizar e identificar, si, existe una vulneración de seguridad.

1.4.4. Instrumentos

Al existir la necesidad de recolectar información del servidor de archivos a investigar en el presente proyecto, se realiza una entrevista al responsable de la administración de este instrumento, en está existen preguntas enfocadas al área de trabajo del equipo, tipo de servicios que provee, entorno de trabajo entre otros similares, estos datos posibilitan obtener la mayor cantidad de información para establecer un proceso de estudio a seguir en la investigación, es así, que en el Anexo 1. Formato entrevista, se encuentra el modelo de entrevista aplicado.

1.4.5. Procesamiento y análisis de la información

Toda vez, que se investiga un servidor de archivos y la entrevista está enfocada a recabar datos para establecer una línea de tiempo ante el posible hecho de que exista un ataque informático, se toman los datos obtenidos para establecer un indicador que cuantifica el grado de afectación que tiene y realizar un seguimiento de los cambios suscitados en el equipo.

De la entrevista aplicada, se identifica que el escenario a investigar es el siguiente: un servidor de archivos apagado; toda vez que a raíz de la pandemia este equipo, no se usó con frecuencia, sin embargo, permanecía encendido expuesto al internet, es así, como al usar el equipo en reiteradas ocasiones, se evidencia que sus archivos almacenados, están cifrados, se procede apagar el equipo para evitar una propagación de este ataque.

1.4.6. Herramientas

En el presente proyecto, se hace uso de herramientas especializadas en el análisis forense, como Autopsy que permite extraer una copia de las evidencias obtenidas y Caine que a través de sus utilidades permite realizar el proceso de extracción de una copia bit y a bit de la información almacenada, además, se hace uso de una investigación bibliográfica para conocer a fondo detalles del ataque encontrado en la evidencia.

1.5. Metodología de desarrollo

El análisis forense, se realiza a un servidor de archivos no dedicado, este equipo, en su momento fue usado para realizar otras actividades aparte de proveer servicios como el de facturación electrónica, dado que su uso, fue entorno a un giro de negocio, el mismo, dejó de usarse a causa de la pandemia del COVID 19, sin embargo, quedó encendido, en marzo de 2021 al acceder a este, presentó problemas en su funcionamiento y surge la necesidad de investigar el suceso para determinar y hallar detalles del posible ataque informático.

Para la realización del AFI existen varias metodologías, que se indican, a continuación:

- Metodología del Departamento de Justicia (DOJ) de los Estado Unidos.
- Metodología del Instituto SANS.
- Digital Forensics Research Workshop (DFRW).
- Kevin Mandia y Chris Prosise.
- Metodología propuesta por Tejada

Al no existir una metodología universal, se estudian varias metodologías en busca de la que mejor se adapte al presente proyecto de investigación, en la Tabla 1, se observa una comparativa entre las metodologías antes indicadas:

Tabla 1. Comparación metodologías análisis forense

Fases	DOJ	SANS	DFRW	KEVIN	TEJADA
Estudio preliminar	✓	✓	✓	✓	✓
Recopilación de evidencias	✓	✓	✓	✓	✓
Análisis de evidencias	✓	✓	✓	✓	✓
Informe	X	✓	✓	✓	✓
Procedimientos					
Preparación	X	X	X	X	✓
Detección	X	X	X	X	✓
Análisis preliminar	X	X	X	X	✓
Contención, erradicación y recuperación	X	X	X	X	✓
Actividades posteriores	X	X	X	X	✓

Fuente: elaboración propia

Conforme lo indicado en la tabla anterior, se valida que no todas las metodologías analizadas establecen procedimientos para el AFI, por lo tanto, en el presente proyecto la metodología a utilizar es la indicada en el apartado 2.2 por Tejada (2015), se selecciona esta metodología que permite realizar actividades posteriores como la elaboración de recomendaciones de seguridad en el presente caso de estudio, para evitar futuros ciberataques, además, este modelo, se adapta a cualquier equipo independientemente del sistema operativo que utilice y está basado en la gestión del riesgo.

1.5.1. Análisis forense informático

En la Tabla 2, se observa las fases y en la

Tabla 3 los procedimientos para realizar el AFI.

Tabla 2. Fases del AFI

Estudio preliminar
Recopilación de evidencias
Análisis de evidencias
Informe

Fuente: adaptado de Tejada (2015)

Tabla 3. Procedimientos del AFI

Preparación
Detección
Análisis preliminar
Contención, erradicación y recuperación
Investigación
Actividades posteriores

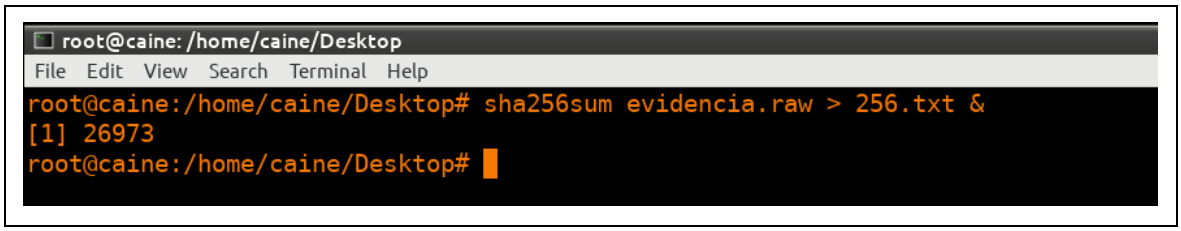
Fuente: adaptado de Tejada (2015)

Estudio preliminar y preparación

En esta etapa del AFI, se realiza un estudio de la escena para determinar la técnica a usar para la recopilación de la evidencia, de acuerdo con el escenario de estudio, se aplica una entrevista, se tiene dos escenarios posibles uno, si, el equipo está encendido y otro, si, se encuentra apagado, en cada caso, se determina los pasos a seguir para recopilar información. En el presente trabajo, se trabaja con el segundo escenario, es así, como, es importante, no encender el equipo para no alterar la evidencia, tal vez, se prende para capturar información de la memoria RAM, sin embargo, es importante, aquí recordar que al momento de realizar este proceso mencionado, toda la evidencia almacenada en la RAM es de tipo volátil, por lo tanto, se pierde al apagar el dispositivo.

Así, también, es muy importante establecer la cadena de custodia para asegurar todas las evidencias digitales, para esto, es recomendable usar herramientas que permiten realizar una copia bit a bit y que incluyan métodos que garanticen la integridad en los datos digitales adquiridos, se usa códigos de comprobación como SHA256, en la Figura 8, se observa el procedimiento realizado para la generación del hash sha256 para establecer la cadena de custodia de la evidencia.

Figura 8. Generación de la cadena de custodia



Fuente: elaboración propia

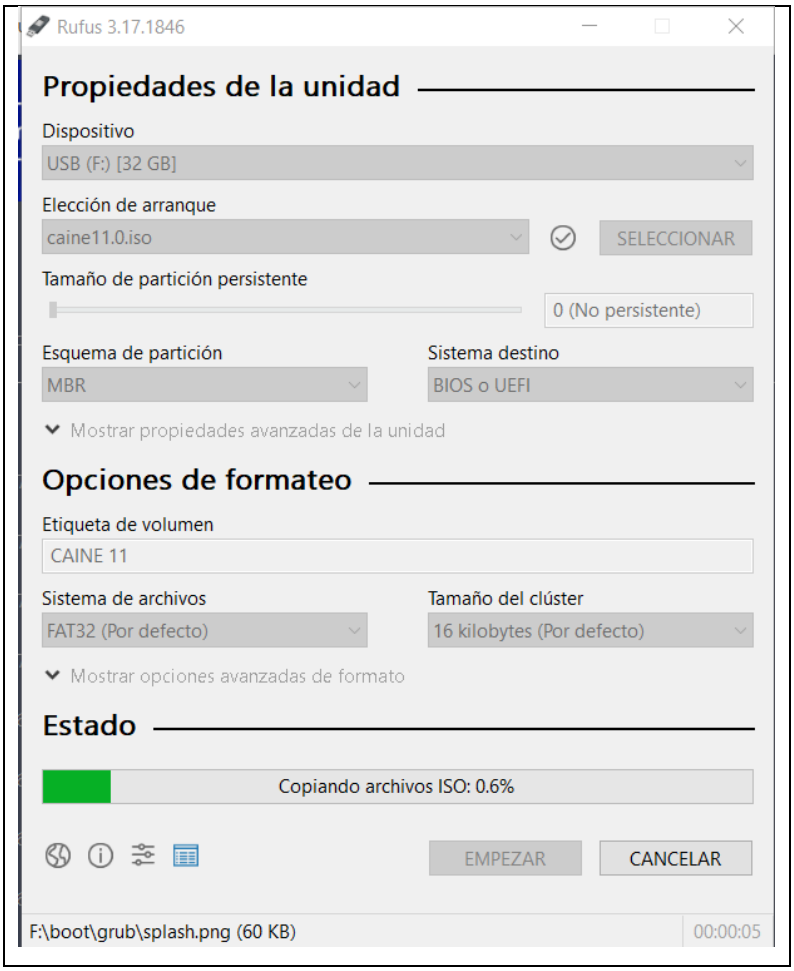
Recopilación de evidencias y detección

Etapa de mucha importancia, permite identificar que programas y/o servicios están atacados en caso de que el AFI, se realice en vivo, como anteriormente, se indicó, aquí se recaba toda la información posible, se captura el tráfico de red, se hace un volcado de memoria RAM, así como, también, se capturan procesos, que se ejecutan en el equipo atacado para establecer una línea de tiempo e identificar, cual, o, cuales, son los problemas que impiden el normal funcionamiento del

sistema, para el presente caso de estudio, se hace únicamente una copia bit a bit del disco duro del servidor como primer paso, para esto existen herramientas especializadas que permiten ejecutar este proceso; en la presente investigación, se realiza una copia con la distribución de CAINE a través de los pasos, a continuación, detallados:

1. Descarga de CAINE como herramienta para obtener la evidencia y Rufus para hacer *booteable* una memoria USB con el software CAINE, cada uno desde su respectiva web: https://www.caine-live.net/page5/page5.html y https://rufus.ie/downloads/
2. Ejecución de Rufus y validación de la configuración que permite instalar CAINE en una memoria USB, en la Figura 9, se observa los parámetros a establecer.

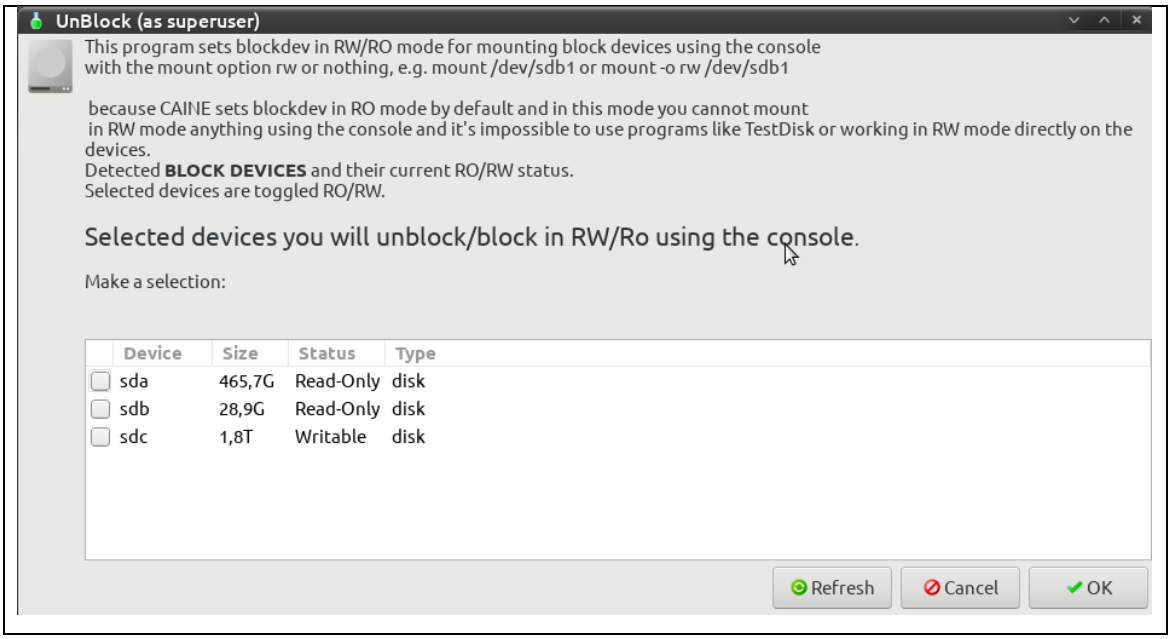
Figura 9. Instalación de Caine en memoria USB a través de Rufus



Fuente: elaboración propia

3. Conexión de memoria USB en el servidor de archivos
4. Encendido del servidor, muy importante aquí tener en cuenta, que se enciende el equipo y, se selecciona como sistema de arranque el que tiene la memoria USB instalado caso contrario la evidencia es alterada.
5. Una vez iniciado CAINE, se verifica que la protección contra escritura este activa en el disco duro del servidor de archivos, esto se realiza con el uso de la utilidad *UnBlock* como, se observa en la Figura 10.

Figura 10. Verificación de protección contra escritura



Fuente: elaboración propia

6. Apertura de un Terminal y acceso con privilegios de usuario *root*, como se observa en la Figura 11.

Figura 11. Consola y acceso como root

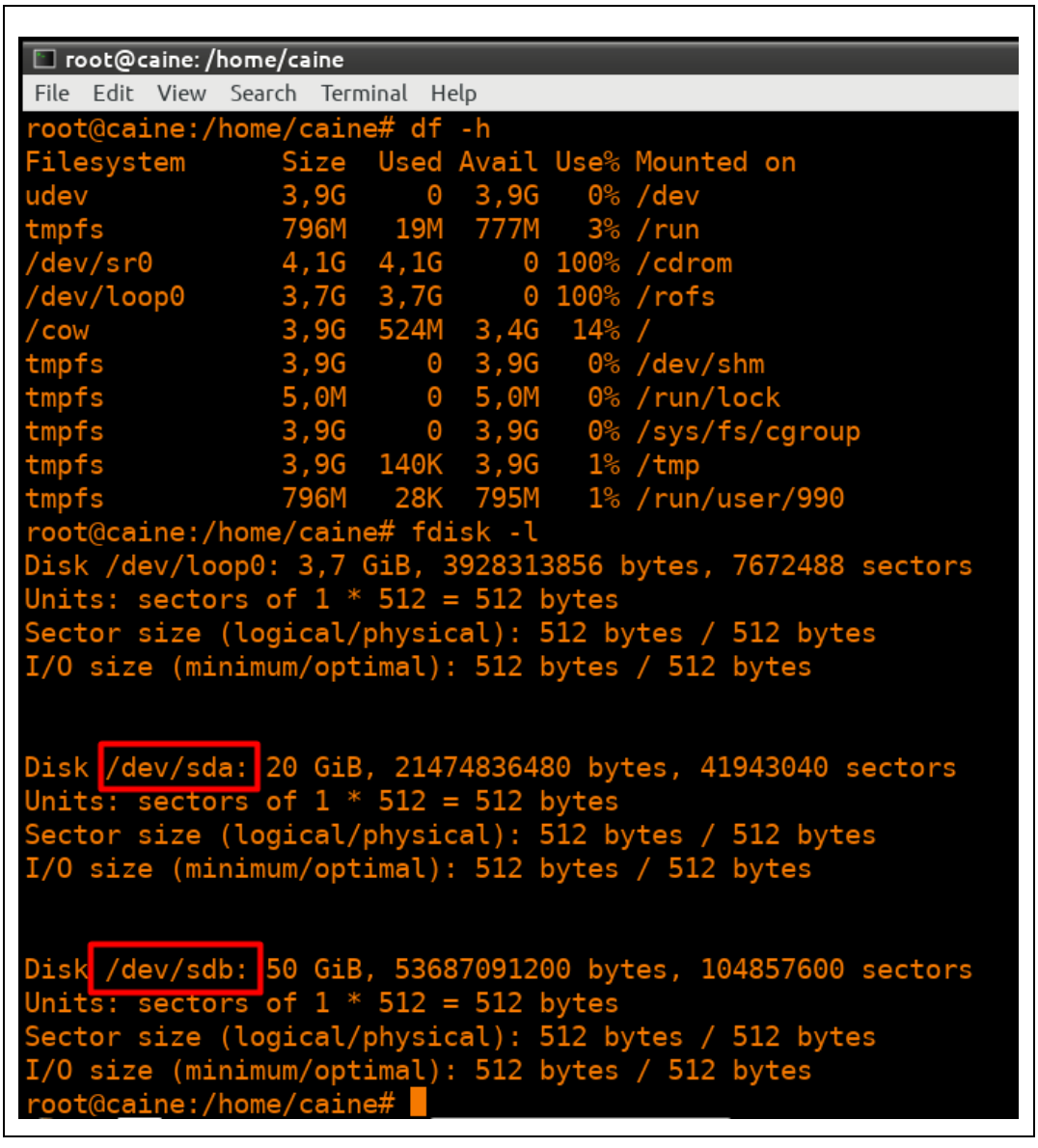
Fuente: elaboración propia

7. Se identifica el nombre y ruta del disco duro y/o partición a copiar, para realizar este proceso, se utiliza las siguientes sentencias de código:

- df -h
- fdisk -l

En la Figura 12, se observa la ejecución de los códigos indicados anteriormente.

Figura 12. Verificación del nombre y ruta de disco



Fuente: elaboración propia

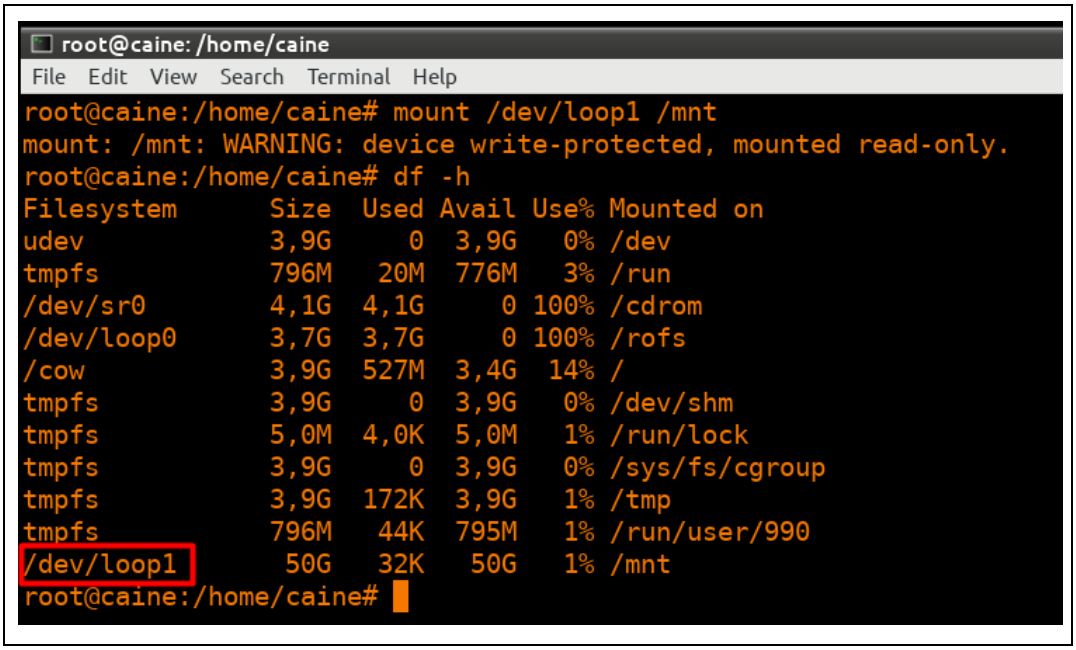
8. Uso de la herramienta dd (por sus siglas en ingles *Dataset Definition*), sencilla, útil, y fácil de usar; se utiliza sobre discos y/o particiones, su línea de código para realizar la copia es la siguiente:

dd if=origen of=destino &

9. Una vez identificado el disco a copiar, es importante, tener en cuenta que para la copia, se realiza en un disco externo con mínimo el doble de capacidad del disco origen, toda vez que el disco externo instalado tiene la ruta /dev/loop1, se monta el mismo con el siguiente código:

- mount /dev/loop1 /mnt

Figura 13. Montaje de disco externo en Caine



Fuente: elaboración propia

En la Figura 13, se valida que el disco está montado en la ruta /mnt, se accede a esa ruta con el código cd /mnt para realizar la copia al dispositivo externo.

10. Identificado el disco a copiar y una toda vez que el mismo está montado en la ruta indicada anteriormente, el código a ejecutar para la copia es el siguiente:

    dd if=/dev/sda of=evidencia.raw &

    Tener en cuenta que el disco, se graba tal cual con respecto a su origen, es decir, su tabla de particiones, espacio vacío, y sus similares, en caso de ocurrir errores en la copia bit a bit debido a sectores defectuosos en el disco, como alternativa, se utiliza la herramienta ddrescue; “GNU ddrescue es una herramienta de recuperación de datos. Copia datos de un archivo o dispositivo de bloque (disco duro, cdrom, etc.) a otro, tratando de rescatar primero las partes buenas en caso de errores de lectura” (GNU, 2021).

11. De darse el caso que al usar dd, se presente algún error en el proceso de copia, se usa la siguiente sintaxis para la copia:
    - ddrescue if=origen of=destino &
    - ddrescue if=/dev/sda of=evidencia.raw &
12. Una vez concluida la copia es de suma importancia establecer, si, la imagen forense creada es un duplicado exacto del dispositivo de almacenamiento original, para esto, se crea un valor de *Hash* que viene a ser una identificación única generada a través de un algoritmo criptográfico, el código para calcular este valor es el siguiente:
    - sha256sum evidencia.raw > 256evidencia.txt
    - sha256sum /dev/sda > 256disco.txt
13. Finalmente, se compara los *hashes* generados, en este caso son iguales, si, la copia, se realiza de manera exitosa y es idéntica al original, se válida con el siguiente código:
    - cat *.txt

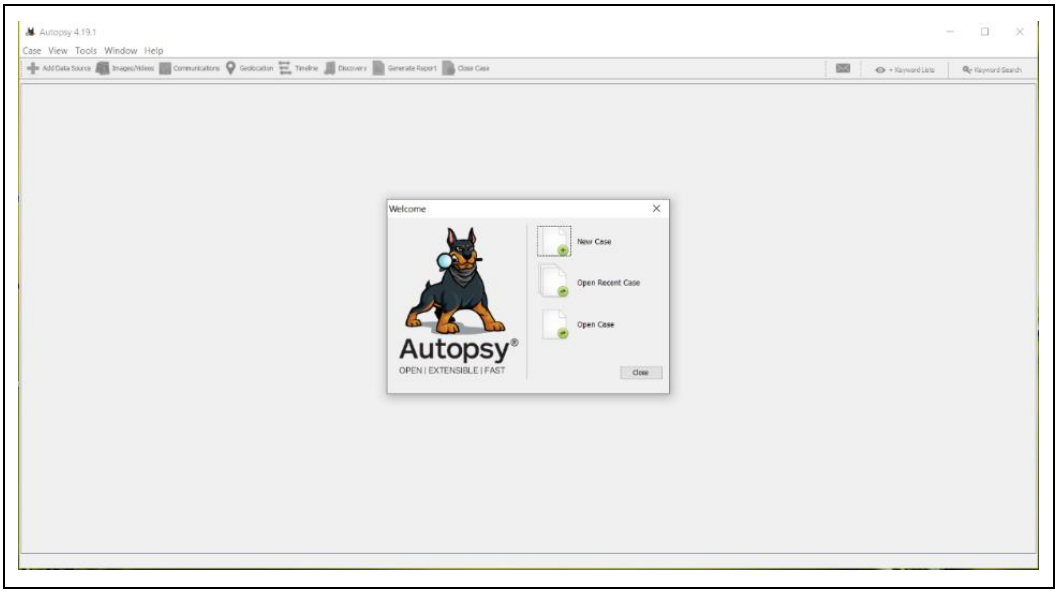
Análisis de evidencias – contención erradicación y recuperación

Una vez obtenida la evidencia, se monta en la herramienta Autopsy para su análisis a través de los siguientes pasos:

1. Descarga de Autopsy en el siguiente enlace: https://www.autopsy.com/download/

2. Instalación y ejecución, como, se observa en la Figura 14.

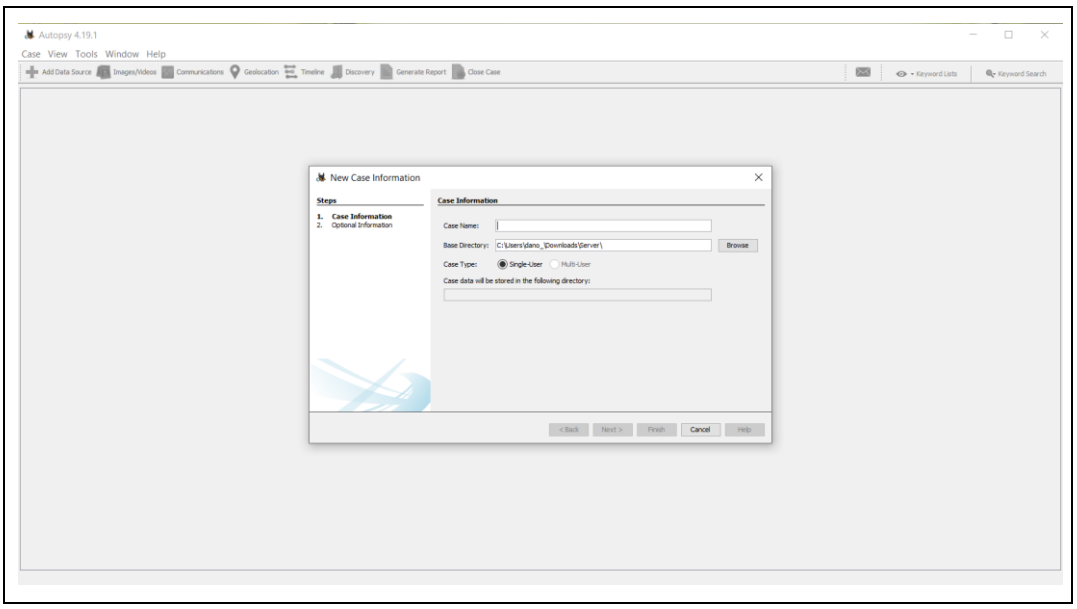
Figura 14. Ejecución Autopsy



Fuente: elaboración propia

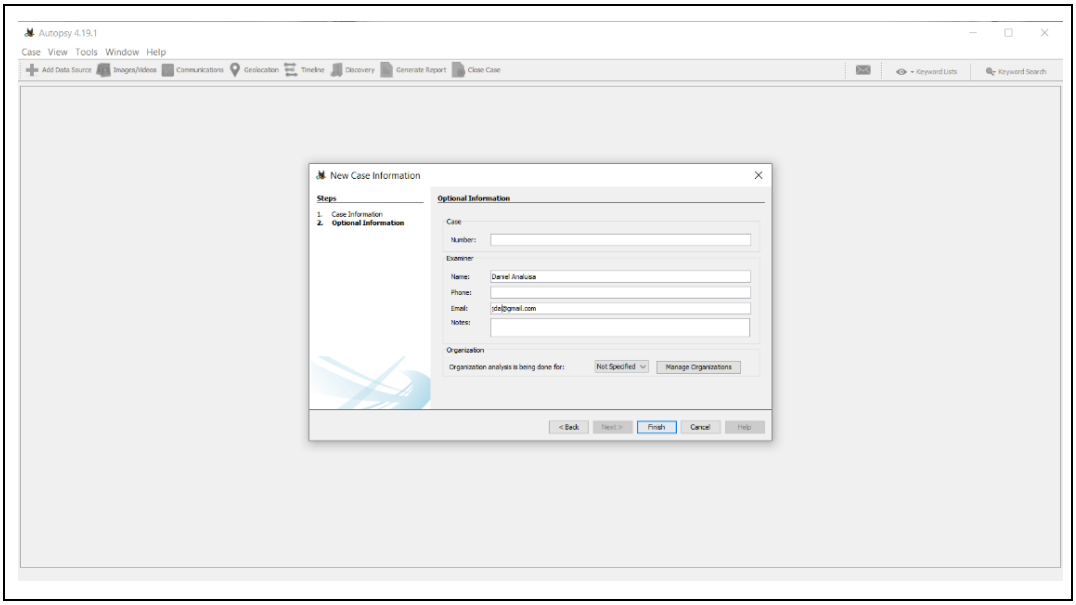
3. Creación de un caso, en este apartado, se detallan los datos relacionados con la investigación (número de caso, nombre del investigador entre otros) a realizar, como, se indica en la Figura 15 y Figura 16, además, se indica la ruta de almacenamiento de todos los archivos.

Figura 15. Creación de caso en Autopsy



Fuente: elaboración propia

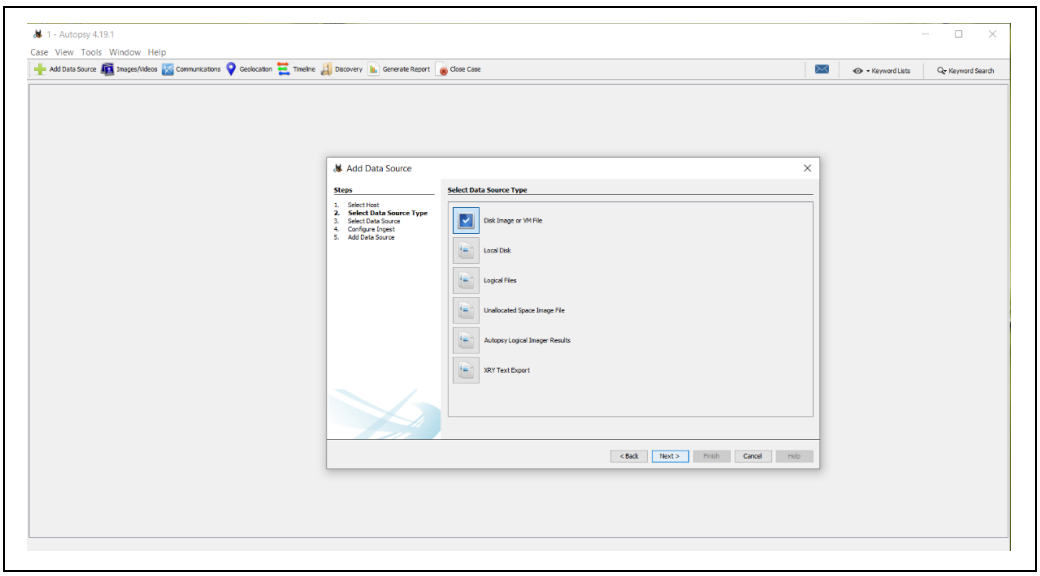
Figura 16. Parámetros creación de caso en Autopsy



Fuente: elaboración propia

4. Como siguiente paso, se selecciona la opción *Disk Image or VM File*, esta utilidad permite montar una copia de imagen, como se observa en la Figura 17, se busca el archivo copia en este caso tiene la extensión .raw; Autopsy soporta formatos de archivos AFF (*Advanced Forensic Format*), *Expert Witness*, y raw (en bruto).

Figura 17. Apertura de copia .raw

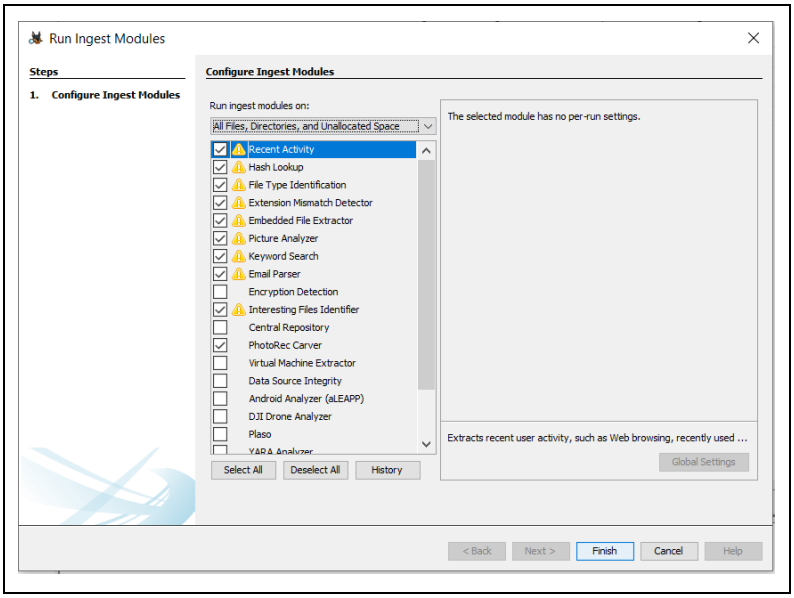


Fuente: elaboración propia

5. Se selecciona los diferentes módulos para determinar las diferentes opciones de búsqueda, esto de acuerdo con la necesidad de la investigación, como se observa en la Figura 18, entre las opciones, se tiene:

- Módulos de ingesta
- Módulo de actividad reciente
- Módulo de búsqueda de base de datos hash
- Módulo de identificación de tipo de archivo
- Módulo de extracción de archivos integrado
- Módulo analizador EXIF
- Módulo de búsqueda de palabras clave
- Módulo analizador de correo electrónico
- Módulo detector de modificación de extensión
- Módulo verificador E01
- Módulo analizador de Android
- Módulo de identificación de archivos interesantes
- Módulo PhotoRec Carver

Figura 18. Módulos de Autopsy para búsqueda de evidencias

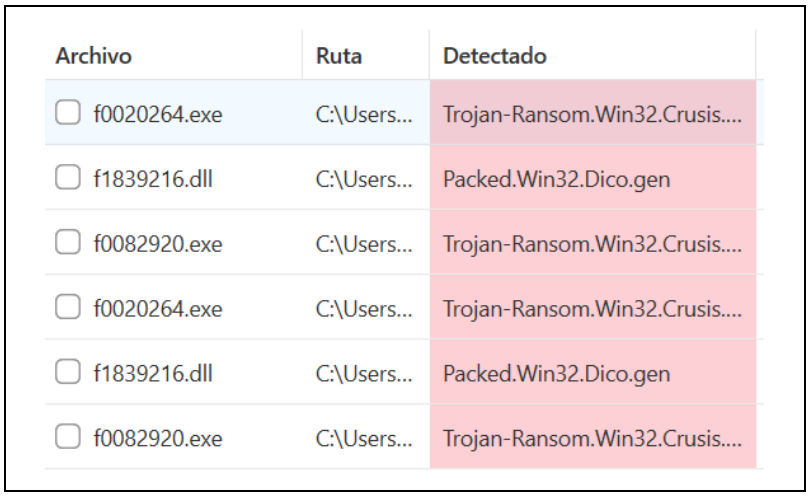


Fuente: elaboración propia

6. Una vez seleccionado los diferentes módulos para buscar información, estos procesos, se ejecutan en segundo plano y proporcionan resultados en tiempo real.
7. Como siguiente y último paso en esta etapa el investigador busca indicios para establecer causas y brechas de seguridad que aprovecho el atacante.

Como primer indicio del ataque hallado en la presente investigación, en la Figura 19**,** se observa que existe un programa con un nombre desconocido de tipo *ransomware*, y a través de una investigación bibliográfica, se determina el método de ataque que ejecuta.

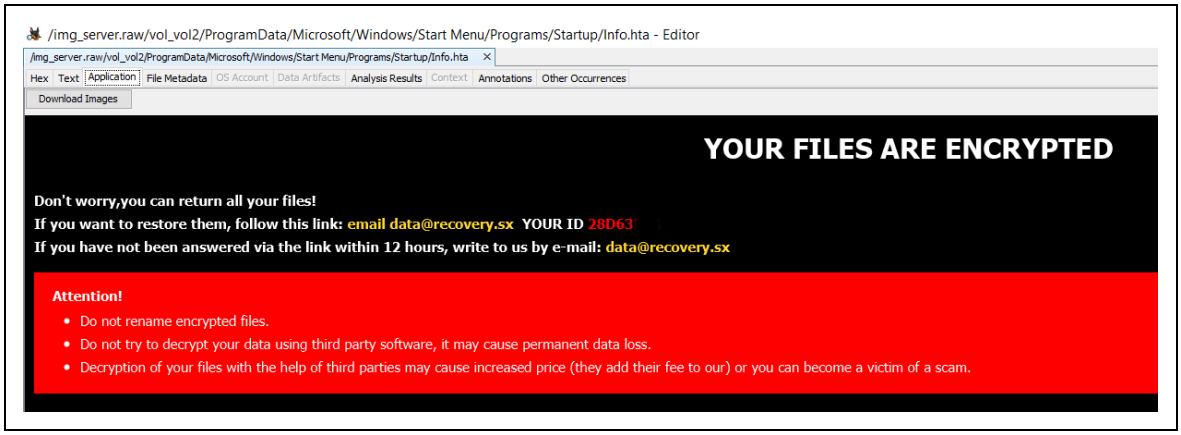
Figura 19. Programa malicioso



Fuente: elaboración propia

A continuación, es necesario contener, erradicar y recuperar la información alterada producto del ataque suscitado, una vez detectado el ataque y extraída toda la evidencia digital posible, el servidor de archivos quedó nuevamente aislado de la red de datos para evitar que el ataque, se propague a más equipos; en la Figura 20, se observa el mensaje que dejó este ataque, que solicita una recompensa a cambio de descifrar la información comprometida en el equipo.

Figura 20. Ataque a través del cifrado de archivos



Fuente: elaboración propia

Hoy en día la mayor cantidad de ataques, se producen por *ransomware* que encripta información y datos del equipo, se solicita una recompensa para liberarlos, se recomienda no pagar ningún rescate porque no garantiza el descifrado de la información, es por esto, que se sugiere mantener copias periódicas de los datos almacenados, esto agiliza el proceso de recuperación de un sistema en caso de producirse un ataque de este tipo.

Informe e investigación

En el Ecuador, al existir normativa que tipifica delitos cometidos a activos informáticos, esto permite hacer las denuncias respectivas en caso de que algún equipo sea o esté atacado permite, así, que personal especializado investigue estos casos; para la investigación es de suma importancia adjuntar toda la cantidad posible de evidencias, es así, como el AFI genera esta información.

Como etapa final del AFI, se elabora un informe que tiene todas las evidencias del caso, que posibilita conocer a detalle el delito informático investigado, en el Anexo 4. Formato informe Consejo de la Judicatura, se establece el formato de informe proporcionado por el Consejo de la Judicatura (Consejo de la Judicatura, 2020), que es documentado con detalles técnicos en el Capítulo 3 del presente trabajo, como parte de la exposición de los resultados obtenidos.

Actividades posteriores

Como actividades posteriores la institución trabaja en conjunto con su departamento de TI o a través de su CSIRT (Equipo de Respuesta ante Emergencias Informáticas) para establecer y aplicar medidas de seguridad informática de forma inmediata para solucionar los bugs que permiten a los atacantes vulnerar sus sistemas, en este caso de estudio en el epígrafe 3.2 del capítulo 3, se establecen recomendaciones de seguridad que son de utilidad para evitar futuros ataques de este tipo, sin embargo, hay que recalcar que no existe un sistema 100% seguro.

CAPÍTULO III. ANÁLISIS DE RESULTADOS

3.1. Informe de análisis forense

El desarrollo del siguiente apartado, se documenta de acuerdo con el Anexo 4. Formato informe Consejo de la Judicatura, sin embargo, al tratarse de un tema de investigación, se realizan ajustes y, se omiten detalles en los datos generales por situación educativa, esto con el objetivo de preservar la integridad en la información de la persona que realiza el AFI.

“INFORME PERICIAL”

3.1.1. Datos generales

No. De Proceso	001
Nombre y Apellido de la o el Perito	Jaime Daniel Analuisa Muso

3.1.2. Parte de antecedentes

En la presente investigación existe un servidor de archivos, que tiene su información almacenada encriptada, producto de un ataque informático, por lo tanto, se realiza un AFI para determinar cuál o cuáles son las causas que permitieron que este ataque suceda.

El servidor de archivos funcionaba de forma normal, sin embargo, a raíz del aislamiento por la pandemia del covid19 este dejó de ser usado, sin embargo, quedó encendido con conexión a internet y como su uso, se daba en torno a un giro de negocio este no era utilizado, en marzo de 2021, se accede al equipo para utilizar el sistema contable, cuando el usuario intenta acceder al sistema, valida que este presenta inconsistencias y notifica inmediatamente al área de soporte para su revisión, como resultado del análisis previo de los archivos que almacena el equipo, se verifica que tiene cifrada la información y paquetes informáticos a nivel de software; De acuerdo con los procedimientos respectivos en seguridad de la información, se procede a aislar de la red al equipo infectado para evitar que el atacante afecte a más equipos, se apaga y envía a servicio técnico para su revisión;

se desconoce la fecha exacta, toda vez que el equipo no tiene un monitoreo constante.

Previo al inicio de la investigación del ataque suscitado en el servidor de archivos, se firma un acuerdo de confidencialidad entre el investigador y la institución propietaria del servidor en base al formato establecido en el Anexo 3. Formato acuerdo de confidencialidad, con la finalidad de precautelar intereses de ambas partes y la información entregada, para que esta no sea divulgada y varios de los hallazgos acerca del ataque, se manejen de manera confidencial.

3.1.3. Parte de consideraciones técnicas o metodología a aplicarse

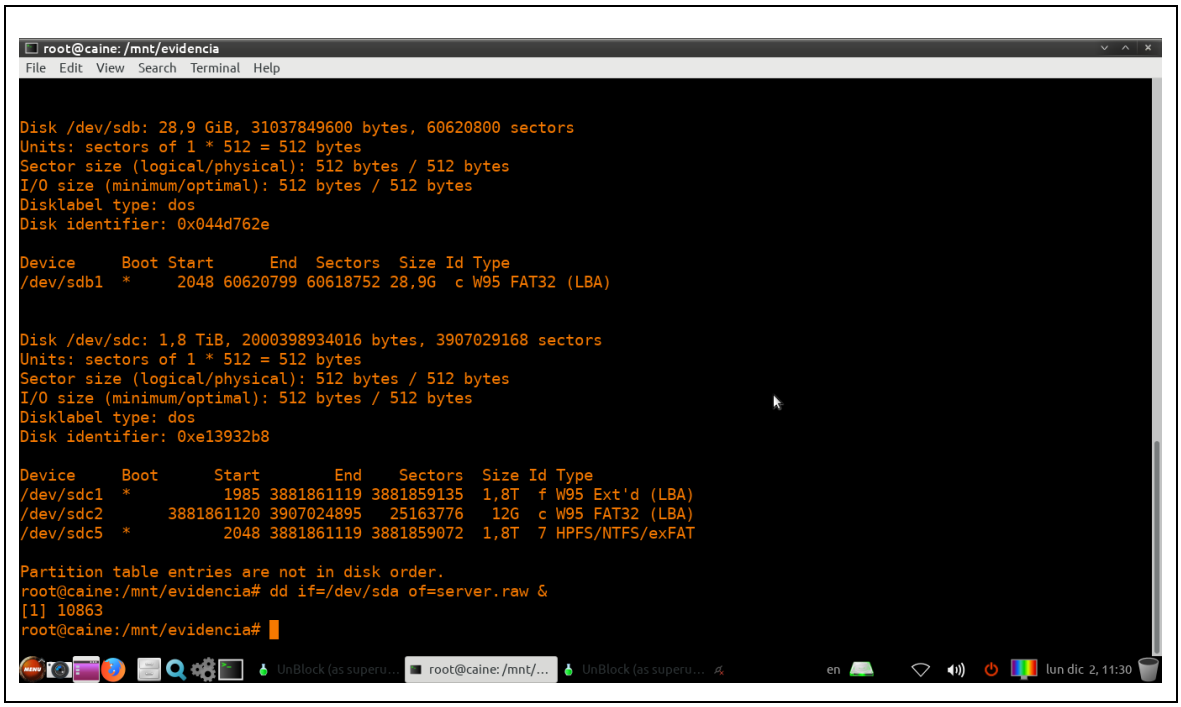
En la Figura 21, muestra el servidor de la marca HP, cuenta con un disco duro de 500Gb de capacidad en almacenamiento, información, que se obtiene del acta entrega recepción suscrita conforme el formato establecido en el Anexo 2. Formato acta entrega recepción, la metodología de investigación, que se aplica en el presente caso, se detalla en el epígrafe 2.2.1 y 2.2.2 del capítulo anterior.

Figura 21. Servidor HP

Fuente: elaboración propia

En este caso de estudio, se usa Autopsy como herramienta forense para analizar la información almacenada en el servidor de archivos y Caine como utilidad para realizar una copia bit a bit de la información almacenada, como, se observa en la Figura 22, ambas herramientas aseguran la confidencialidad e integridad de los datos, que se obtiene en esta investigación.

Figura 22. Copia bit a bit de los datos del servidor



Fuente: elaboración propia

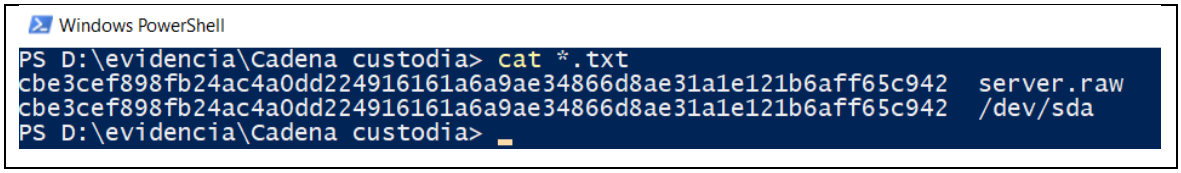
3.1.4. Parte de conclusiones

Las conclusiones correspondientes al análisis forense, se reflejan a la cuarta y quinta conclusión del presente proyecto en el epígrafe correspondiente.

3.1.5. Parte de inclusión de documentos de respaldo, anexos, o explicación de criterio técnico

Como primer paso en la investigación del caso, se valida la cadena de custodia como, se observa en la Figura 23; se concluye que la copia bit a bit entregada para el análisis coincide con la información original almacenada en el servidor de archivos.

Figura 23. Verificación cadena de custodia

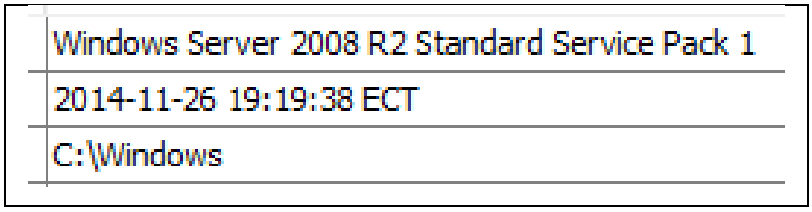


Fuente: elaboración propia

Una vez validada la información entregada y que esta no ha esta alterada, se procede a montar el archivo recibido que tiene un tamaño de 465 Gb, su copia, se realiza bit a bit y tiene formato raw.

La Figura 24, detalla el sistema operativo del servidor (Windows Server 2008 R2).

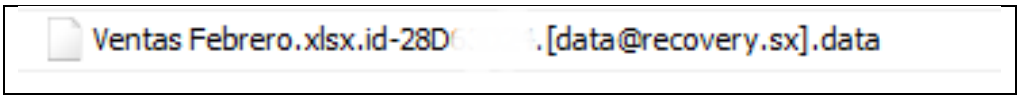
Figura 24. Versión sistema operativo del servidor



Fuente: elaboración propia

En la Figura 25, se valida que el tipo de encriptación de los archivos tiene una extensión .data.

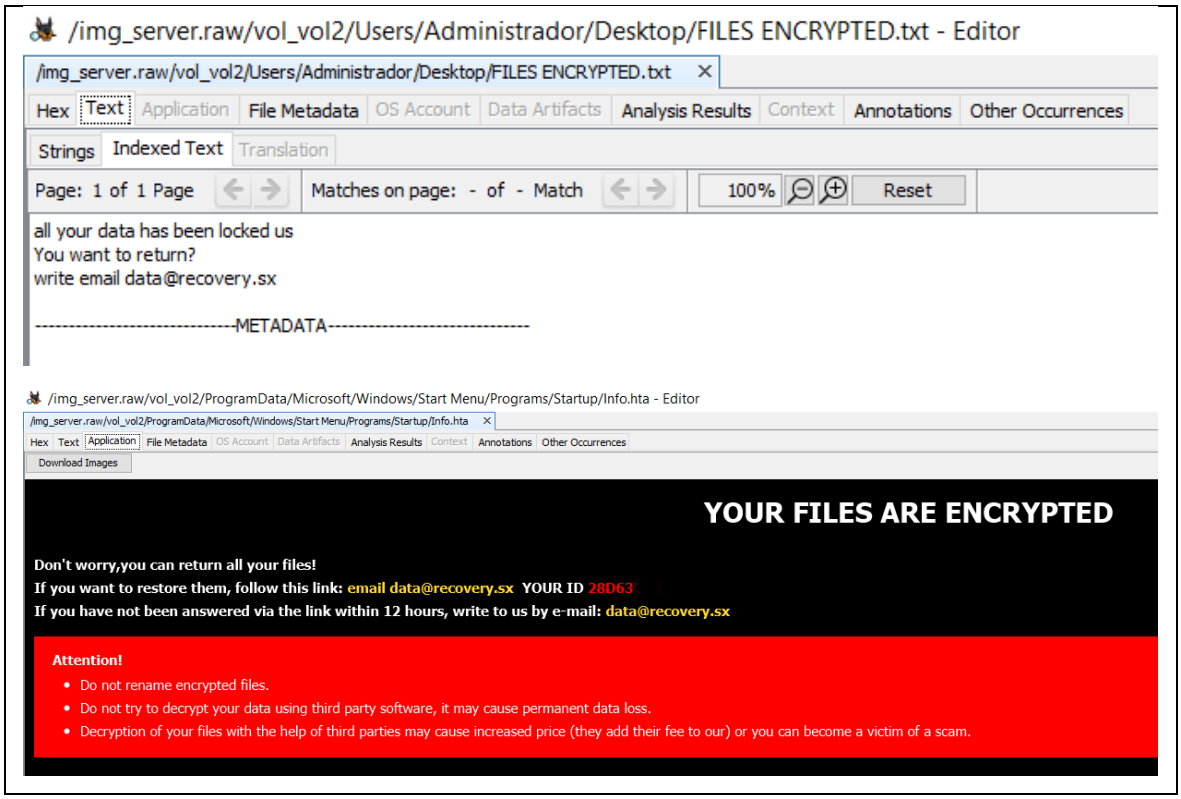
Figura 25. Extensión de archivos encriptados



Fuente: elaboración propia

De acuerdo con la extensión que tienen los archivos encriptados del servidor, Smith (2020) valida que este ataque, se atribuye a la familia Dharma *Ransomware*; en la Figura 26, se observa el mensaje que los atacantes dejan en el equipo.

Figura 26. Mensaje de los atacantes en el servidor



Fuente: elaboración propia

Conforme la fecha de creación de los archivos encriptados, se identifica que en el servidor previo al ataque, se realiza una modificación en la configuración de hora; en la Figura 27, se observa como fecha, 11 de julio de 2009.

Figura 27. Fecha de archivo modificado

COMPRAS MAYO.xlsx.id-28D6	.[data@recovery.sx].data	∇	1	2009-07-11 02:57:36 ECT

Fuente: elaboración propia

De acuerdo con la fecha y el correo encontrado en la encriptación de archivos, la Figura 28, detalla que existen archivos creados, que van desde el 06/07 al 11/07 de 2009.

Figura 28. Fecha de modificación de archivos

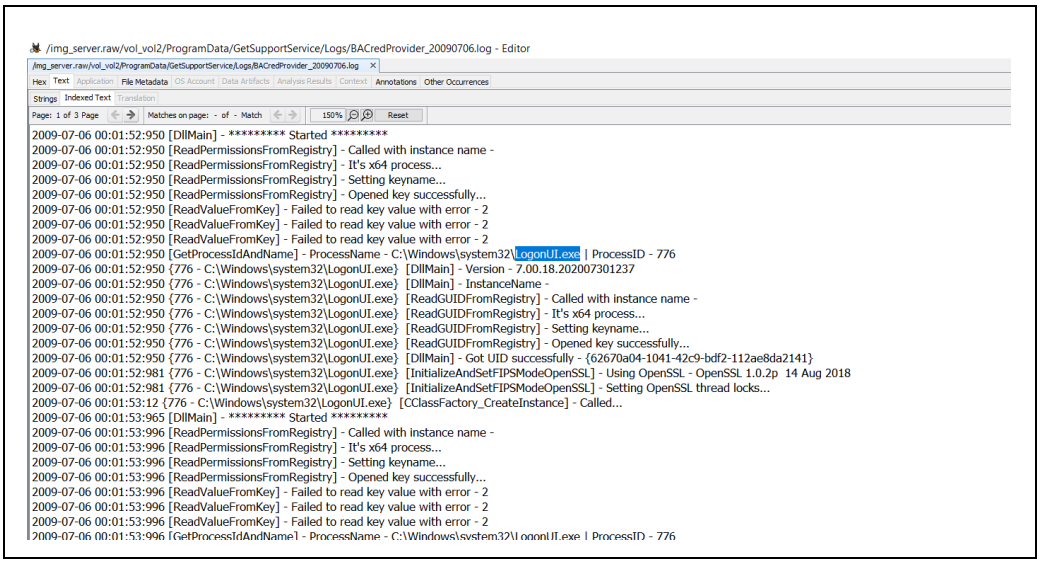
Keyword Preview		Modified Time	Access Time	File Path
sk.lnk.id-28d	[«data@recovery.sx«].data> c…	2009-07-06 00:19:50 ECT	2009-07-06 00:19:50 ECT	/img_server.raw/vol_vol2/Users/Administrador/NTUS
sk.lnk.id-28d	[«data@recovery.sx«].data> c…	2009-07-06 00:19:50 ECT	2014-11-26 19:19:47 ECT	/img_server.raw/vol_vol2/Users/Administrador/ntuse
0}.dat.id-28(	[«data@recovery.sx«].data-slac	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].dat	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].data-slac	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].dat	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].data-slac	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].dat	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].data-slac	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].dat	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].data-slac	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].dat	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD
0}.dat.id-28(	[«data@recovery.sx«].data-slac	2009-07-06 00:28:11 ECT	2009-07-06 00:28:11 ECT	/img_server.raw/vol_vol2/Users/Administrador/AppD

Keyword Preview		Modified Time	Access Time	File Path
o.xlsx.id-28d	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
o.xlsx.id-28d	.[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
op.ini.id-28d	[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
o.xlsx.id-28d	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
op.ini.id-28d	[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
o.xlsx.id-28d	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
to.pdf.id-28c	.[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
o.xlsx.id-28d	.[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Docur
rx.pdf.id-28c	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
br.xls.id-28d	.[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
to.pdf.id-28c	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
rx.pdf.id-28c	.[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
ar.xls.id-28d	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
br.xls.id-28d	.[«data@recovery.sx«].dat	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt
ar.xls.id-28d	.[«data@recovery.sx«].data-slac	2009-07-11 02:57:40 ECT	2009-07-11 02:57:40 ECT	/img_server.raw/vol_vol2/Users/Administrador/Deskt

Fuente: elaboración propia

Así, también, se evidencia que el 06/07 el archivo tiene como hora 00:19:50, es así, como en los registros del servidor, se encuentra que a las 00:01:52, se hace un llamado al proceso LogonUI.exe, como, se observa en la Figura 29; este proceso ayuda al computador para crear una interfaz que facilita iniciar sesión en el sistema.

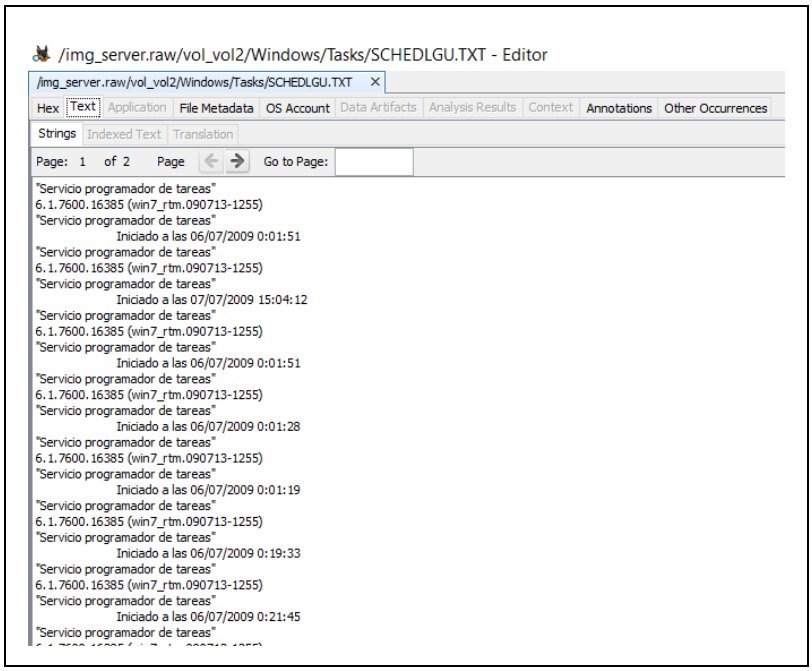
Figura 29. Proceso LogonUI.exe



Fuente: elaboración propia

Así, también, de acuerdo con la línea de tiempo y conforme la hora, la Figura 30 evidencia la ejecución del programador de tareas del servidor a las 0:01:51.

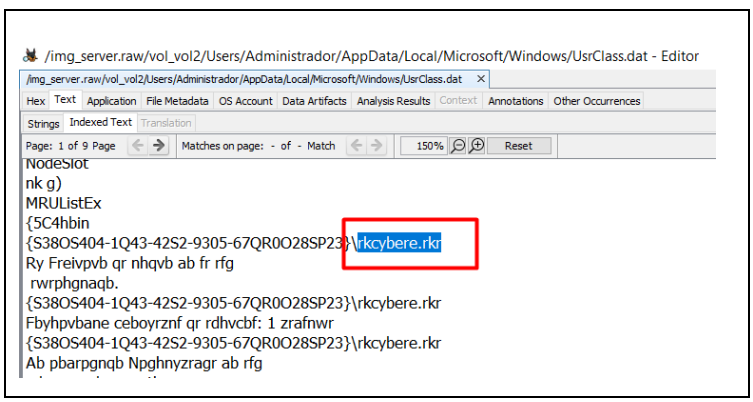
Figura 30. Inicio de programador de tareas



Fuente: elaboración propia

Usrclass.dat es un registro que guarda información e instrucciones para archivos ejecutables; la Figura 31 muestra que dentro de este registro existe texto ofuscado, esto con la finalidad de que datos capturados de navegación y archivos recientes sean menos notorios.

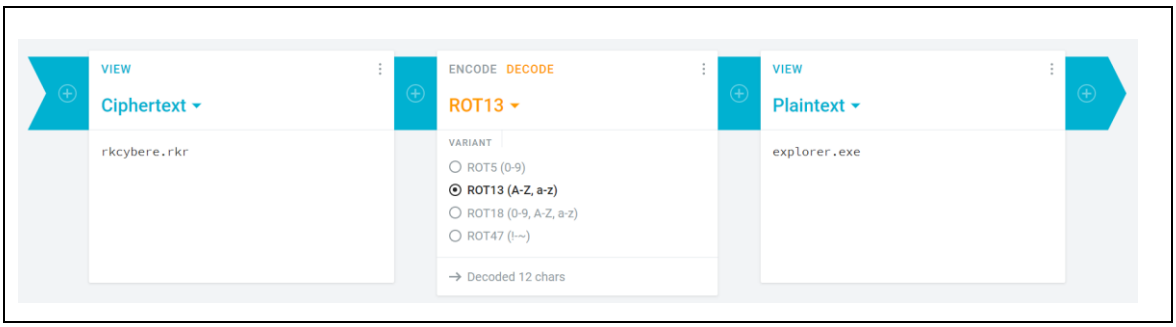
Figura 31. Texto ofuscado en registro UsrClass.dat



Fuente: elaboración propia

El texto ofuscado tiene un cifrado simple del tipo de cifrado César (Rot13,), donde su método de ofuscamiento consiste en reemplazar cada letra con la que está 13 lugares hacia adelante o hacia atrás a lo largo del alfabeto, la Figura 32 muestra el descifrado del texto con ayuda de la utilidad rot13-decoder (Cryptii, 2021).

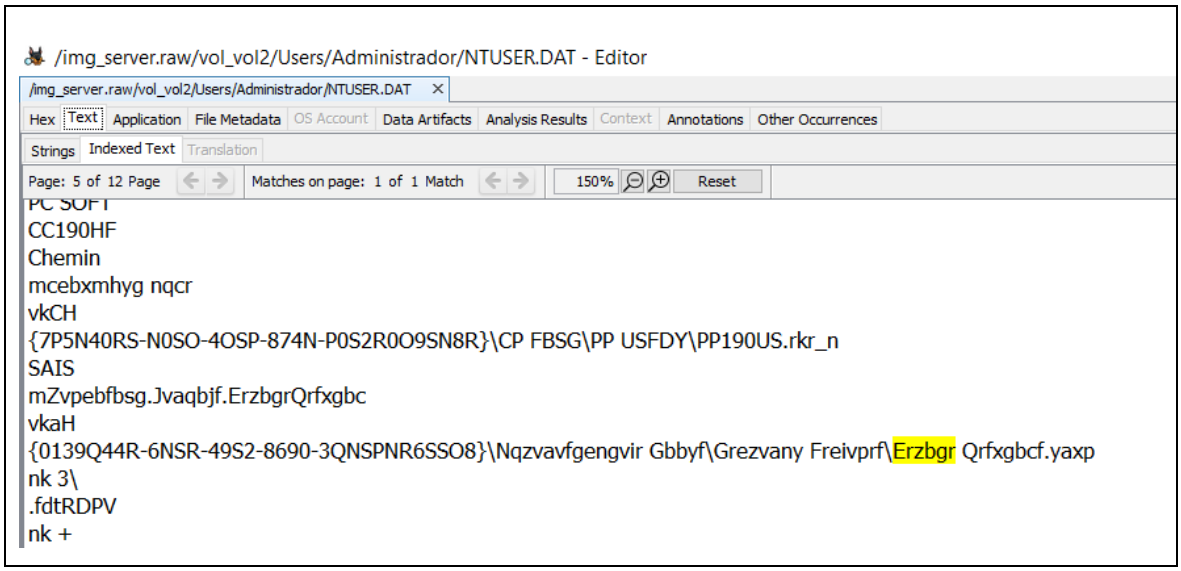
Figura 32. Descifrado Rot13

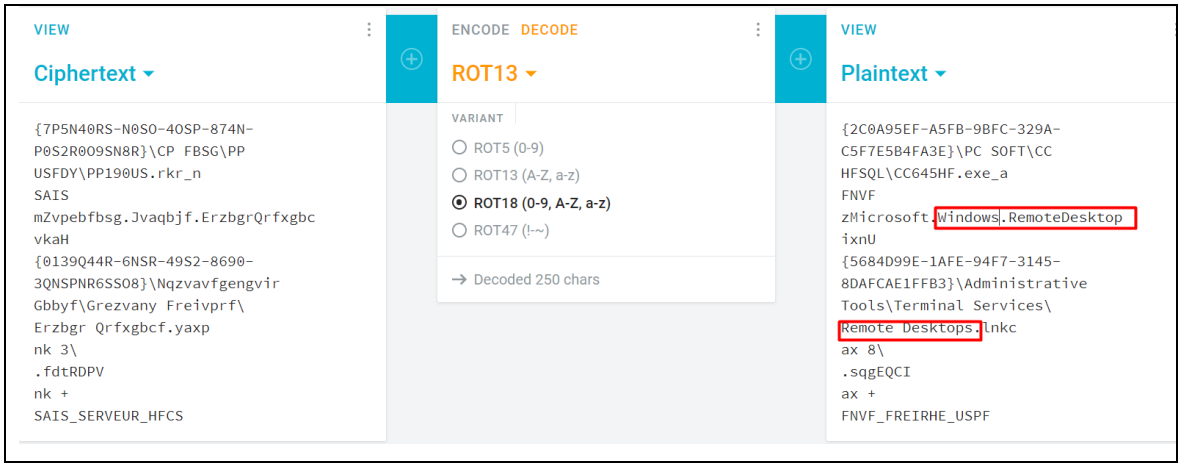


Fuente: elaboración propia

La Figura 33 indica que en el registro NTUSER.DAT, se hace un llamado al servicio de escritorio remoto.

Figura 33. Registro NTUSER.DAT llamado a escritorio remoto

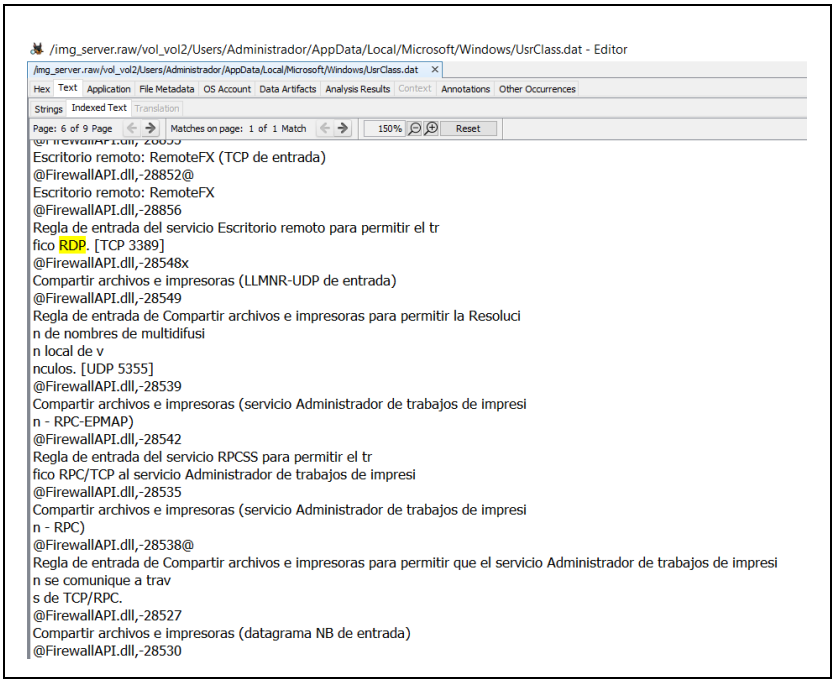




Fuente: elaboración propia

Conforme al análisis del registro UsrClass.dat, en la Figura 34, se evidencia la habilitación de varios puertos en el sistema operativo del servidor, se habilita el puerto 3389 que faculta hacer uso del protocolo RDP (por sus siglas en ingles *remote desktop protocol*) para conexiones remotas; de acuerdo con Smith (2020) uno de los métodos de ataque que hace uso este *ransomware* es explotar credenciales RDP débiles o robadas.

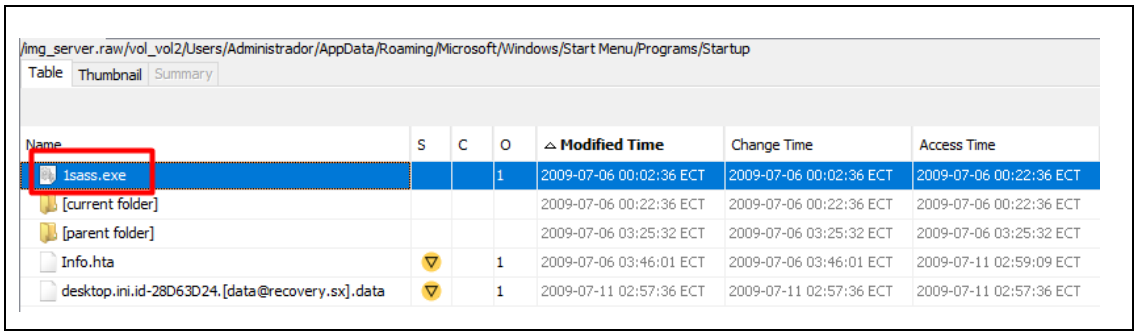
Figura 34. Registro de habilitación de puertos en el servidor



Fuente: elaboración propia

De acuerdo a la grabación de video realizada por (CheckMAL Inc., 2021, 0m8s), se valida que este tipo de ataque cifra los archivos con la ejecución de un archivo con extensión .exe, este tiene cualquier nombre; la Figura 35 evidencia la ruta donde, se aloja el archivo ejecutable que cifra toda la información almacenada en el servidor.

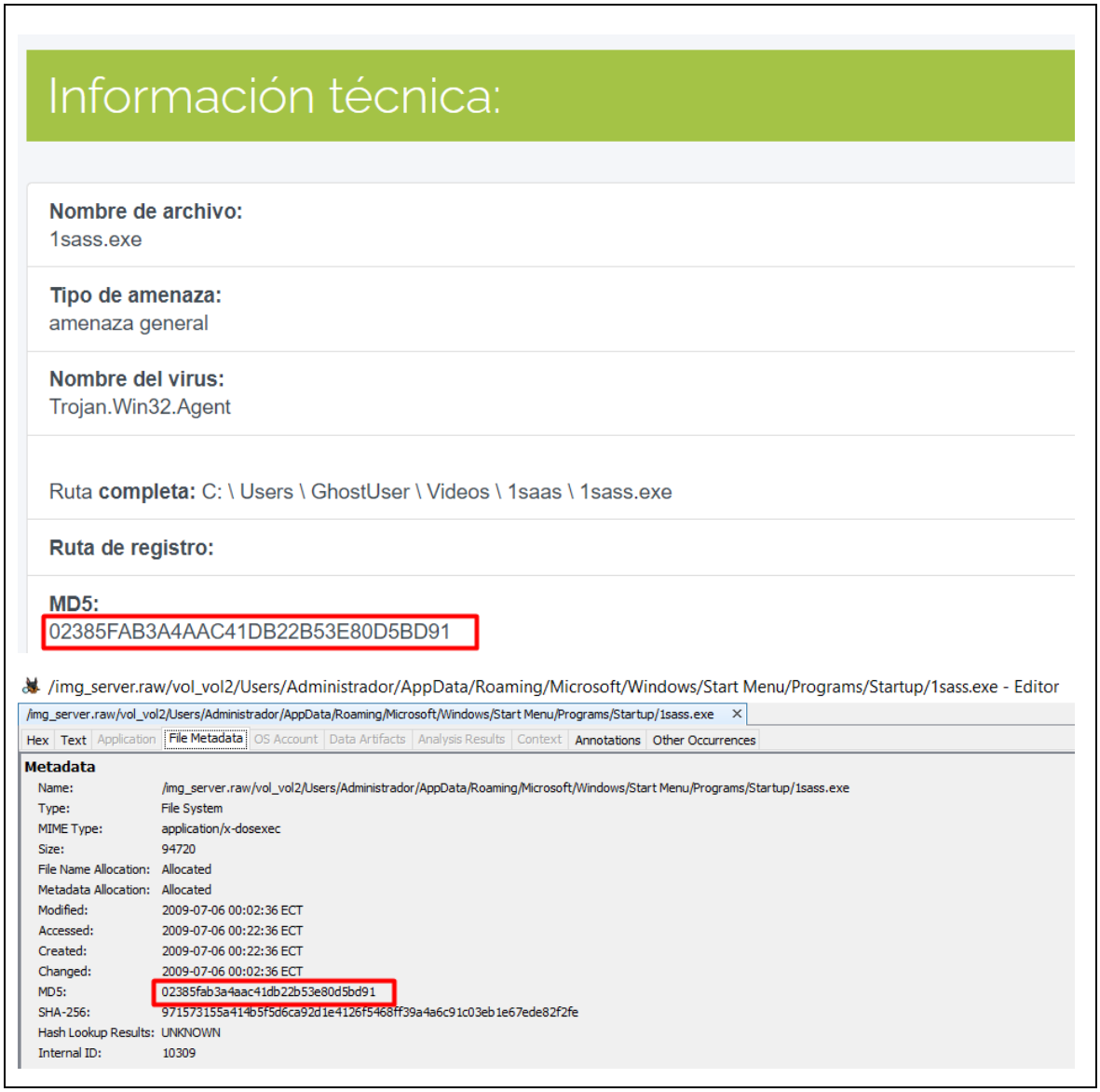
Figura 35. Ejecutable del *ransomware*



Fuente: elaboración propia

El archivo ejecutable con nombre 1sass.exe de acuerdo con ITSafety (2020), se detecta comoTrojan.Win32.Agent, al estar alojado en la carpeta de inicio del sistema operativo Windows del servidor, se ejecuta junto al sistema operativo al momento de encender el equipo; en la Figura 36, se observan detalles de este ejecutable entre estos el *hash* mismo que coincide con el alojado en el servidor.

Figura 36. Hash de archivo 1sass.exe



Fuente: elaboración propia

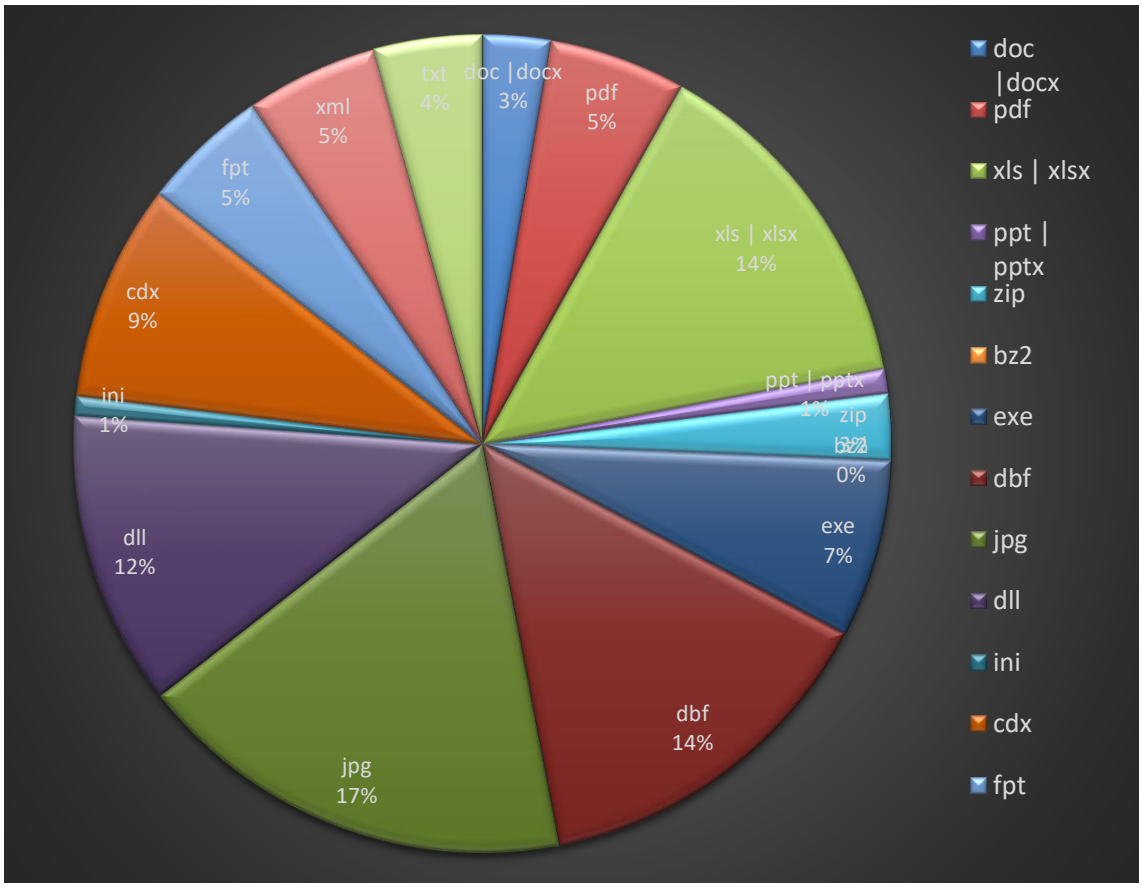
Conforme indica Security (2017) las extensiones de archivos que este *ransomware* ataca son las, que se observan en la Figura 37.

Figura 37. Extensiones de ficheros que ataca Dharma

Fuente: adaptado de Security (2017)

En la Figura 38, se observa la cantidad de ficheros encriptados en el servidor de archivos, donde los con extensión .jpg .dll y .dbf son los que más existen en los datos que almacena el servidor.

Figura 38. Porcentaje de ficheros encriptados



Fuente: elaboración propia

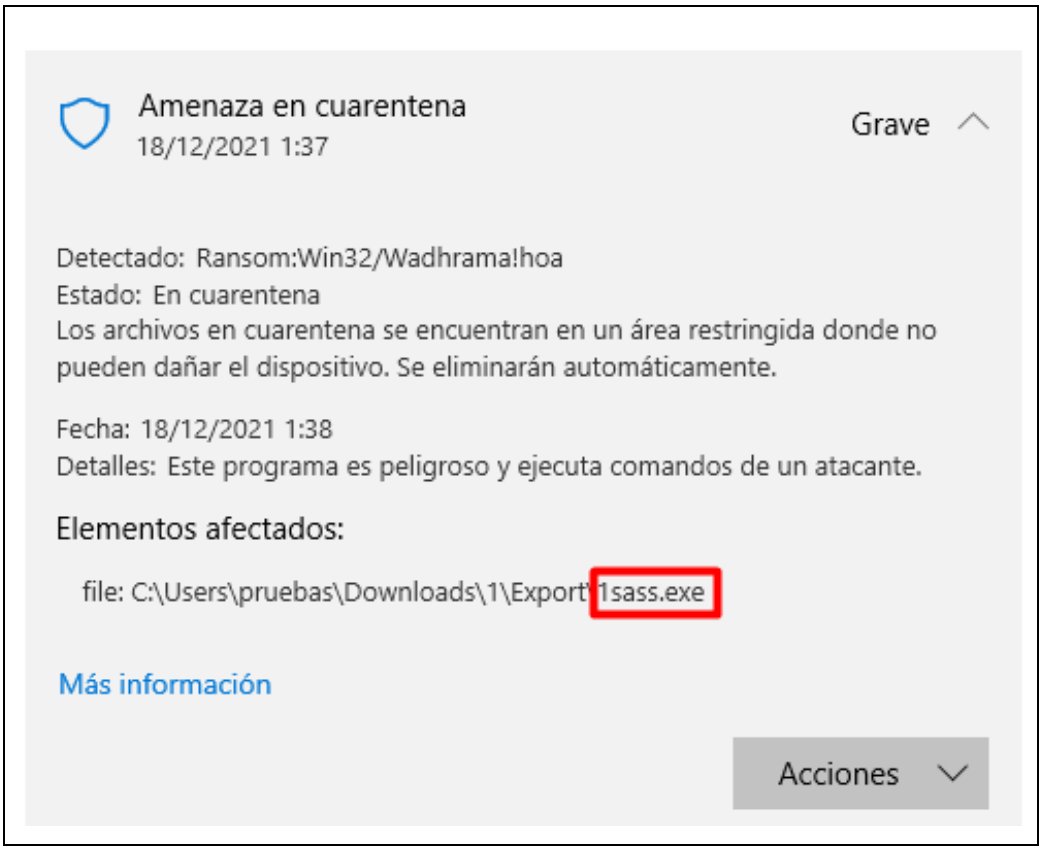
3.1.6. Otros requisitos

No se incluyen otros requisitos al caso en estudio, toda vez que en el presente caso de investigación, se guarda reserva en los datos del propietario del servidor de archivos.

3.1.7. Información adicional

Finalmente, se monta un escenario de prueba para ejecutar el archivo que contiene el *ransomware*, esto permite validar que efectivamente 1sass.exe es el que cifra los archivos del servidor, en la Figura 39, se evidencia que en primera instancia Windows defender detecta a este ejecutable como *ransomware*.

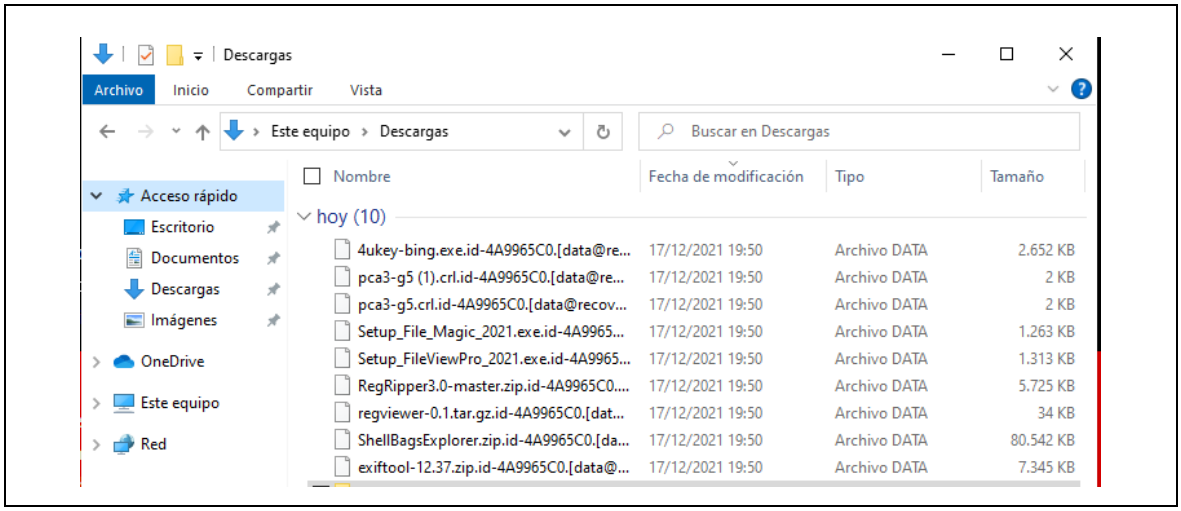
Figura 39. Ransomware en escenario de prueba



Fuente: elaboración propia

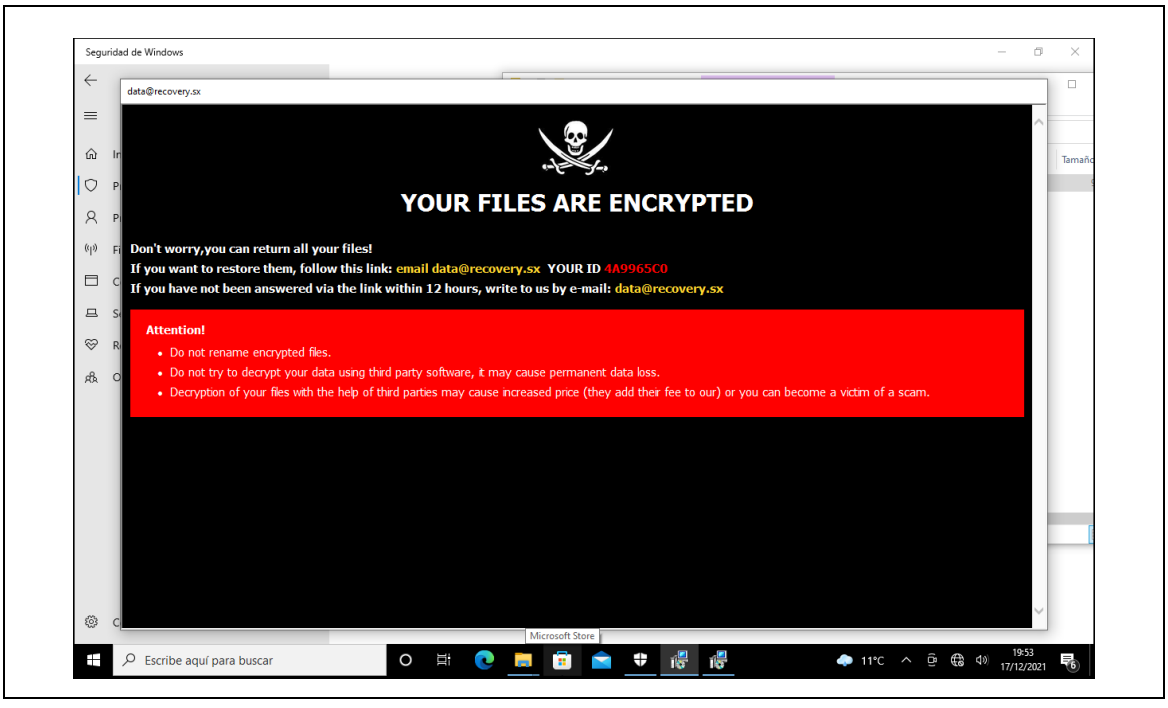
Previo a la ejecución de 1sass.exe es necesario deshabilitar las protecciones que tiene Windows defender, al ejecutar el archivo, en la Figura 40, se evidencia los archivos cifrados y en la Figura 41 su nota de rescate, se valida, así, que efectivamente este ejecutable cifra archivos.

Figura 40. Encriptación de archivos en escenario de prueba



Fuente: elaboración propia

Figura 41. Nota de rescate en escenario de prueba

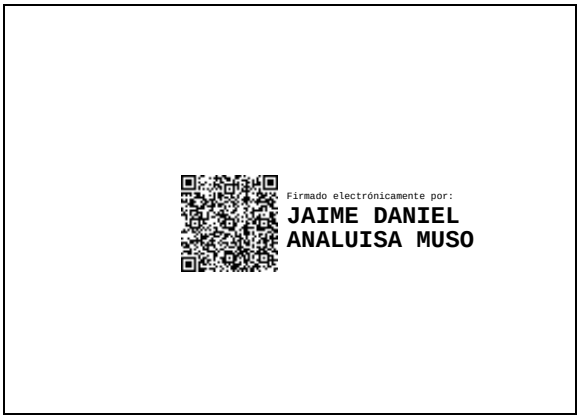


Fuente: elaboración propia

3.1.8. Declaración juramentada

Yo, Daniel Analuisa declaro que el presente informe pericial es realizado con toda la independencia del caso, con profesionalismo y conforme todas las técnicas establecidas en los manuales.

3.1.9. Firma y rúbrica



3.2. Propuesta de recomendaciones de seguridad

Conforme lo analizado en el caso de estudio es menester recomendar implementar en la institución la norma ISO 27005 para la gestión de riesgos en la seguridad de información, esta permite comprender el tratamiento de riesgos, la aceptación del riesgo, la comunicación y consulta, el monitoreo y revisión, es así, aplicable a toda organización; Su implementación, hace uso del modelo PHVA (Planificar, Hacer, Verificar, Actuar) y así establece una hoja de ruta para realizar un proceso de gestión con un enfoque de mejora continua de acuerdo con las necesidades y requerimientos de la institución.

Así, también, para reducir el riesgo vinculado a amenazas cibernéticas como la, que se encuentra en este estudio y en base a los controles que NIST establece en su *framework,* se emplea Kanban para determinar varios controles y realizar un seguimiento continuo de estos, entre los controles que permiten reducir ataques de *ransomware,* se tienen los indicados en la Tabla 4.

El implementar estos controles, reduce en gran medida la brecha de seguridad de la información, se logra, así, detectar futuras amenazas que ponen en riesgo equipos de la institución, además, se identifica que existe el control RS.AN-3, este

establece realizar análisis forense; como conclusión estos controles abarcan procesos de Identificación, Protección, Detección, Respuesta y Recuperación.

Así, también, si los controles marcados en negrita en la Tabla 4, hubiesen estado implementados en la institución el impacto producido por el ataque informático, se hubiera reducido en gran medida, inclusive si, se lo detectaba a tiempo, sin embargo, los métodos de ataque que usan los piratas informáticos cada vez son más sofisticados que pasan desapercibidos inclusive con herramientas y controles establecidos para detectarlos.

Tabla 4. Controles de seguridad basados en NIST

Control	Descripción
ID.AM-2 Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	Usa una solución de administración de activos de hardware y software para inventariar todo el software en la organización. Este proceso sería automático. Soluciones: Administración de activos de hardware y software
ID.AM-4 Los sistemas de información externos están catalogados.	a) Crea un catálogo de todos los flujos de datos desde y hacia los sistemas internos de cada área, y sistemas externos. Los flujos con sistemas externos serían, por ejemplo, conexiones directas a servidores de clientes o proveedores, o serían el acceso manual a plataformas de Software as a Service (SaaS). b) Utiliza un sistema de análisis de bitácoras para detectar todos los flujos de datos externos, y una solución de control de acceso a la nube (CASB) para detectar todas las aplicaciones SaaS, que se utilicen .
ID.GV-3 Se comprenden y, se gestionan los requisitos legales y regulatorios con respecto a la seguridad informática, incluidas las obligaciones de privacidad y libertades civiles.	Identifica todas las regulaciones gubernamentales relacionadas a la protección de datos, y asegúrate que sean atendidas por los controles implementados. Colabora con el área legal para mantenerte al tanto de estas regulaciones.
ID.RA-2 La inteligencia de amenazas informáticas, se recibe de foros y fuentes de intercambio de información.	Utiliza servicios gratuitos y de paga de ciber inteligencia para mantenerte al tanto de las ciber amenazas actuales, y ajusta los controles de acuerdo a las mismas. Soluciones: Ciber inteligencia
ID.RA-3 Se identifican y, se documentan las amenazas, tanto internas como externas.	Mantén una lista de posibles ciber amenazas relevantes a tu organización. Toma en cuenta

	que surgen nuevas ciber amenazas, por lo que, es importante, mantenerte al día sobre el tema. Esta es una lista parcial: - Botnets - Ataques de denegación de servicio - Exploits - Malware - Phishing - Ransomware - Sitios web maliciosos - Empleados maliciosos Soluciones: Ciber inteligencia
ID.RA-4 Se identifican los impactos y las probabilidades del negocio.	Para cada una de las ciber amenazas que hayas determinado en ID.RA-3, indica cuál sería el impacto si ocurre ese tipo de ataque, y cuál es la probabilidad de que ocurra.
ID.RA-5 Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	Determina cuál es el nivel de riesgo para cada activo en base a sus vulnerabilidades, impactos, y probabilidades de incidencia. Solución: Gerencia integrada de riesgos
ID.RA-6 Se identifican y priorizan las respuestas al riesgo.	En base a lo determinado en ID.RA-5, establece planes de contingencia para cada caso. Soluciones: Gerencia integrada de riesgos
ID.SC-1 Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	El objetivo de la gestión de riesgo en la cadena de suministro es asegurarnos que los proveedores no introduzcan riesgos cibernéticos a la organización, que afectan la confidencialidad, integridad, o disponibilidad de datos. Solución: Gerencia de riesgo de proveedores.
ID.SC-2 Los proveedores y socios externos de los sistemas de información, componentes y servicios, se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	Como primer paso, identifica a todos los proveedores y cómo la interacción con ellos presentar una amenaza a los sistemas de la organización. Solución: Gerencia de riesgo de proveedores.
PR.AC-1 Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	a) Identifica todos los sistemas de hardware, software, y bases de datos, y determina qué grupos de usuarios tienen acceso. En base a

	esto, establece procesos para dar, modificar, y remover permisos de acceso. b) Asegúrate que haya una lógica de negocio detrás de cada permiso de acceso. Haz la pregunta, ¿por qué esta categoría de usuario requiere acceso a este sistema? Asegúrate que el proceso tenga la capacidad de modificar los derechos de acceso si un usuario cambia de status (despedido, cambio de departamento, cambio de puesto, etc.) c) Asigna a un responsable de gerencia de acceso para cada sistema. d) Revisa que las cuentas de acceso temporales tengan una caducidad definida. e) Checa que el proceso tenga la capacidad de detectar cuentas de acceso inactivas. f) No permitas que haya cuentas compartidas; es una cuenta específica por persona, para auditar comportamiento. g) Asegúrate que el proceso tenga la capacidad de detectar comportamiento anómalo en las cuentas, y que este comportamiento sea investigado por el área de respuesta a incidentes. h) No permitas que los usuarios tengan permisos de administrador sobre sus computadoras personales. i) Asegúrate que los accesos a aplicaciones web sean a través de sistemas de *login* único. j) Asegúrate que las contraseñas utilicen algoritmos de encriptación fuertes (por ejemplo, no utilizar SHA-1). k) Asegúrate que no haya sistemas que serían accedidas por la contraseña de una sola persona; en caso de que esa persona falte, tiene por lo menos otra persona con capacidad de acceder el sistema. L) Asegúrate que no haya contraseñas de fábrica (*default passwords*) en los aparatos y paquetes de software. Solución: Administración de identidad y acceso, Software de higiene digital
PR.AC-2 Se gestiona y se protege el acceso físico a los activos.	a) Divide el espacio físico en categorías de seguridad, y asigna permisos de acceso a categorías de personal y visitantes.

	b) Asigna pases de acceso permanentes a empleados, y temporales a proveedores y visitantes. c) Implementa un control de acceso con tarjeta magnética a zonas restringidas, y agrega reconocimiento biométrico y de contraseña a zonas altamente restringidas. d) Mantén una bitácora computarizada de todos los accesos detectados. e) Coordina la generación y revocación de accesos con el área de recursos humanos. f) Pide identificación oficial para todos los accesos de visitantes. g) Asegúrate que visitantes siempre sean acompañados por personal de la organización al visitar zonas restringidas. h) Revisa que el sistema de control de acceso de las tarjetas magnéticas emita alertas al detectar comportamiento anómalo; por ejemplo, una tarjeta de visitante entre a una zona restringida sin que una tarjeta de personal de la organización entre al mismo tiempo, o el tiempo de permanencia en una zona restringida sobrepase un umbral determinado. i) Asegúrate que haya cámaras en todas las áreas, que cámaras apunten a equipos restringidos, que tengan la resolución para grabar caras claramente, y que todas las grabaciones, se guarden por lo menos durante 3 meses. j) Revisa que no haya puertos de ethernet abiertos en zonas públicas del edificio, como la sala de espera. k) Asegúrate que las conexiones de cables de ethernet de computadoras, teléfonos IP, impresoras, pantallas, etc., no serían desconectados. l) Revisa que haya alarmas de seguridad y procesos de respuesta a intrusiones. m) Revisa que los racks de servidores estén bajo llave, y que tengan alarma de apertura, con notificación instantánea al área de seguridad física.

PR.AC-3 Se gestiona el acceso remoto.	a) El acceso remoto ocurre si un usuario, se conecta a la red sin estar físicamente presente en la organización. b) Documenta los métodos de acceso remoto permitidos y sus requerimientos técnicos. c) Establece un procedimiento para pedir permiso para tener acceso remoto. d) Monitorea y registra todo acceso remoto. e) Implementa encriptación fuerte para los accesos remotos. f) Rutea todos los accesos remotos a puntos de acceso determinados. g) Asegúrate que los accesos remotos caduquen automáticamente después de cierto periodo. h) Implementa autenticación de doble factor en los accesos remotos. i) Asegúrate que todos los equipos que van a tener acceso remoto sean administrados por tu organización; no permitas accesos remotos desde equipos no administrados. j) Asegúrate que las restricciones de acceso remoto, también, se apliquen a plataformas móviles. k) Implementa un sistema de seguridad móvil, y no permitas que celulares que no sean administrados por el área de seguridad informática, se conecten a la red. Soluciones: Seguridad Móvil, Firewalls, Administración de identidad y acceso
PR.AC-4 Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	a) Asegúrate, que se documente por escrito por qué requiere acceso cada persona a cada sistema. b) Asegúrate que el acceso permitido al usuario sea el mínimo necesario para cumplir con la tarea, por la cual, requiere el acceso. c) Si es necesario, separa los sistemas de tal forma, que se le daría acceso a diferentes niveles de autorización. d) Revisa que la autorización de acceso a sistemas tenga una doble autorización, tanto por el gerente del área, como por alguien

	asignado como responsable en el área de seguridad informática. Solución: Administración de identidad y acceso
PR.AC-5 Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	a) Segmenta la red por nivel de riesgo, se usa categorías como acceso al público, acceso a empleados, acceso restringido, acceso altamente restringido, y restricciones por departamentos. b) Implementa ruteadores, switches, y firewalls para restringir el flujo de datos entre las diferentes áreas de la red. c) Asegúrate que el área de acceso al público (por ejemplo, para dar acceso a visitantes), no tenga ningún tipo de conexión con la red. Contrata un servicio de Internet con WiFi exclusivo para visitantes. d) Si tu organización tiene aparatos expuestos al público tal como quioscos interactivos, aparatos de escaneo de productos pantallas, o puntos de venta que serían robados, asegúrate que estos aparatos estén en un segmento de red separado. e) Asegúrate que el área de acceso altamente restringido no tenga ningún tipo de acceso desde los demás segmentos de red; mantén una separación física (air gap). Si tienes que transferir grandes cantidades de datos entre el segmento de acceso altamente restringido y otros segmentos, utiliza diodos de datos (*data diodes*). f) Implementa microsegmentación. g) Asegura el sistema de DNS. Soluciones: Firewalls, Administración unificada de amenazas, Seguridad de DNS, Microsegmentación, Diodo de datos.
PR.AC-6 Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	Revisa que todas las cuentas de acceso a la red correspondan con personas verdaderas. Soluciones: Administración de identidad y acceso
PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las	a) Establece un límite de fallos de autenticación de acceso a las cuentas de los usuarios; después de cierta cantidad de fallos, el sistema emite una alerta de incidente, y bloquea la cuenta. b) Si un usuario hace *login* a un sistema, muestra lo siguiente:

	- Una notificación de que las acciones, se monitorean, y cuáles son las consecuencias legales de usar la información en forma no autorizada. - Cuál fue el último acceso a la cuenta. - Cuántos intentos fallidos ocurrieron antes de este acceso exitoso. - Cómo contactar al área de seguridad informática si detecta cualquier uso indebido de su cuenta. c) No permitas que la misma cuenta, se utilice al mismo tiempo en más de una sesión. d) Desconecta automáticamente la sesión después de cierto tiempo sin actividad. e) Identifica y administra cuentas que no hayan sido usadas más de 30 días. f) Implementa autenticación de doble factor para cuentas que tengan privilegios de administrador. g) Implementa autenticación de doble factor si un usuario requiere acceso a áreas restringidas. h) Establece una longitud mínima para las contraseñas. i) Asegúrate que las contraseñas caduquen cada 30 días. j) No utilices DHCP, solo IP estáticas. Mantén un *record* de qué IP está asignada a qué hardware. Soluciones: Administración de identidad y acceso, Administración de activos de hardware y software, Software de higiene digital.
PR.AT-1 Todos los usuarios están informados y capacitados.	a) Implementa cursos de capacitación en seguridad informática de acuerdo al nivel del personal (cursos técnicos para los analistas, y cursos gerenciales para gerentes y directores). Crea una matriz de habilidades en seguridad informática requerida para cada categoría de personal, y desarrolla un catálogo de cursos presenciales y en línea. b) Implementa cursos de concientización sobre procesos de seguridad informática para todos los empleados (por ejemplo, cómo no caer en ataques de phishing, y cómo reportar actividad

	sospechosa). Solución: Entrenamiento a usuarios
PR.AT-2 Los usuarios privilegiados comprenden sus roles y responsabilidades.	Crea un curso en línea para entrenar a usuarios con acceso privilegiado, se explican qué procedimientos siguen para mantener la seguridad de los sistemas, y cómo proceder en caso de problemas. No les des acceso a los sistemas hasta que hayan pasado un examen de certificación en línea. Soluciones: Entrenamiento a usuarios
PR.AT-3 Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	a) Crea un curso en línea para proveedores, clientes, y socios que requiera acceso a los sistemas de la organización. **b) No permitas el acceso hasta que no hayan pasado el examen de certificación en línea.** **Solución: Entrenamiento a usuarios**
PR.DS-1 Los datos en reposo están protegidos.	Encripta todos los datos confidenciales. Establece un periodo determinado para archivar fuera de línea todos los datos que ya, no se usen. Implementa un firewall de base de datos. Soluciones: Respaldo de Datos, Encriptación de datos, Firewall de base de datos
PR.DS-2 Los datos en tránsito están protegidos.	a) Encripta todos los datos en tránsito a través de la red. b) Encripta todo el correo electrónico. c) Utiliza protocolos de comunicación seguros (HTTPS, SSH, SFTP, etc.) d) Encripta todos los datos subidos a la nube. Solución: Uso de protocolos de comunicación seguros
PR.DS-5 Se implementan protecciones contra las filtraciones de datos.	a) Implementa una solución de prevención de pérdida de datos (DLP). b) Implementa un sistema de control de acceso a la nube (CASB). c) Analiza a qué servidores externos están conectados a los equipos de tu red. d) Analiza los flujos de datos ente equipos propios, y detecta flujos anómalos. e) Analiza el tráfico encriptado.

	f) Establece un proceso para firmar contratos de confidencialidad de datos con empleados y proveedores que tengan acceso a datos restringidos. g) Establece un procedimiento para identificar canales de comunicación encubiertos. h) Implementa un firewall de bases de datos. Soluciones: Sistemas de prevención de intrusión, Seguridad inalámbrica, Firewall de base de datos, Prevención de pérdida de datos, Control de acceso a la nube.
PR.DS-6 Se utilizan un mecanismo de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	Implementa un sistema de monitoreo de integridad de datos. Implementa un proceso para revisar todo cambio a archivos, paquetes de software, y bases de datos, que no hayan sido previamente autorizados. Implementa un proceso para detectar cambios en el firmware. No permitas, que se utilice software que no tenga una firma digital válida de la compañía que lo produjo. Revisa que el hash de un paquete de software sea el correcto de acuerdo a la compañía que lo produjo. Solución: Monitoreo de integridad de archivos.
PR.DS-8 Se utilizan un mecanismo de comprobación de la integridad para verificar la integridad del hardware.	Revisa la integridad del firmware de todos los equipos. Solución: Monitoreo de integridad de archivos.
PR.IP-3 Se encuentran establecidos procesos de control de cambio de la configuración.	a) Implementa un sistema de control de configuración para administrar la configuración estándar de cada sistema. b) Establece un proceso de autorización de cambios de configuración; el cambio es autorizado por el responsable del área, y por el responsable de seguridad informática. c) En el proceso de autorización, registra la causa, por la cual, se requiere el cambio, qué riesgos produciría el cambio, y qué controles, se tienen que implementar para mitigar el riesgo.

	d) Detecta en forma automática cambios no autorizados a los sistemas e implementa un proceso de respuesta a incidentes. e) Mantén una bitácora de todos los cambios realizados. Solución: Sistema de control de configuración
PR.IP-4 Se realizan, se mantienen y se prueban copias de seguridad de la información.	a) Establece un proceso de respaldo automático de datos hacia la nube. b) No guardes los respaldos en la misma nube donde residen los datos. Por ejemplo, si tu red virtual está en Amazon Web Services, asegúrate que tu proveedor de respaldo en la nube no esté, también, en Amazon Web Services. c) Para datos importantes, además, del respaldo automático de datos hacia la nube, haz un respaldo físico local, y mantén esos datos físicamente desconectados de la red. Usa un diodo de datos. d) El respaldo es incremental; guarda datos de hace un año, 6 meses, 1 mes, 1 día, 1 hora, etc., de acuerdo a la importancia y necesidad de acceso. e) Asegúrate que los datos estén encriptados. f) Realiza una prueba de restauración de datos, para asegurarte que el proceso funcione correctamente. Soluciones: Respaldo de Datos, Diodo de datos.
PR.IP-7 Se mejoran los procesos de protección.	a) Implementa un sistema de hacking ético automatizado para detectar fallas en la arquitectura de seguridad informática. b) Corrige inmediatamente las fallas detectadas. c) Prueba nuevas soluciones de seguridad informática utilice el sistema de hacking ético automatizado, y selecciona aquellas que den mejores resultados. d) Haz pruebas de phishing a tus usuarios, y entrena a aquellos que caigan. f) Haz pruebas de ingeniería social por teléfono y en persona. Soluciones: Hacking ético automatizado, Pruebas de phishing, Proceso manual.

PR.IP-12 Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	a) Ejecuta *scans* de vulnerabilidades diarios. b) Remedia las vulnerabilidades críticas inmediatamente. c) Remedia las vulnerabilidades altas en el transcurso de la semana. d) Remedia las demás vulnerabilidades en el transcurso del mes. e) Antes de instalar un parche, pruébalo en un solo equipo y analiza sus efectos. f) Si, no se aplica un parche por alguna razón operativa, implementa controles compensatorios (por ejemplo, aislé el software en cuestión, o incremente la atención a incidentes para este equipo y segmento de red). g) Si, se descubra una vulnerabilidad crítica o alta, investiga si no ha sido explotada ya. h) Configura los equipos de PCS y laptops para que los sistemas operativos y aplicaciones, se actualicen automáticamente. i) Usa una solución de control de acceso a la nube (CASB) para analizar el riesgo estructural de las aplicaciones de la nube, que se utilizan. Si el riesgo es significativo en aplicaciones críticas, sustitúyelas. j) Analiza y reporta las tendencias de descubrimiento de vulnerabilidades, y el tiempo entre descubrimiento y remediación. k) Identifica software que, no se utiliza y remuévelo antes de que haga vulnerable. l) Realiza escaneo de las aplicaciones web. m) Si tu organización desarrolla código, implementa un proceso de análisis de código. Soluciones: Administración de vulnerabilidades, Análisis de código, Escaneo de aplicaciones web, Control de acceso a la nube.
PR.MA-1 El mantenimiento y la reparación de los activos de la organización, se realizan y están registrados con herramientas aprobadas y controladas.	a) Agenda el mantenimiento preventivo de equipos de cómputo de acuerdo a las recomendaciones del fabricante. b) Crea una lista de revisión de mantenimiento para cada tipo de equipo, tanto de su hardware como de su sistema operativo.

	c) Documenta toda reparación al equipo. d) Establece un procedimiento formal para reparar equipo, el cual, es autorizado por el responsable del área y alguien de seguridad informática. e) Si un equipo va a salir de las instalaciones para reparación, borra todos los datos. f) Al terminar la reparación de un equipo, corre un escaneo de malware inmediatamente, y déjalo aislado de la red, pero, con salida a Internet, y monitorea si intenta conectarse servidores externos no autorizados. g) Antes de conectar equipo de diagnóstico y reparación a un equipo que requiera mantenimiento, corre un *scan* de malware en el equipo de diagnóstico. h) Una vez que el equipo de diagnóstico y reparación haya sido utilizado, revisa que no contenga información extraída del equipo reparado. Soluciones: Borrado seguro de datos, Proceso manual.
PR.MA-2 El mantenimiento remoto de los activos de la organización, se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	**a) Si a un equipo, se le va a hacer mantenimiento remoto, asegúrate que la conexión es segura (VPN, SSH).** b) Analiza todo el flujo de datos entre el equipo de diagnóstico y reparación y el equipo en mantenimiento, para detectar fugas de datos. Soluciones: Firewalls, Análisis de tráfico, Prevención de pérdida de datos.
PR.PT-4 Las redes de comunicaciones y control están protegidas.	a) Analiza todo el tráfico de red para detectar patrones anómalos, se usa un sistema de prevención de intrusión (IPS). b) Implementa un web proxy para toda conexión a Internet, y filtra contenido malicioso. c) Implementa un sistema de análisis de reglas de firewall para centralizar todas las políticas de entrada y salida. d) Analiza los flujos de tráfico entre equipos y paquetes de software para detectar flujos anómalos. e) Establece en los firewalls reglas de *deny all*, y luego permite flujos que tengan una

	justificación de negocios, autorizado por el responsable del área y el responsable de seguridad informática. f) Analiza hacia con qué servidores externos, se conectan los equipos y checa su status en un servicio de ciber inteligencia. g) Revisa que los puntos de acceso de WiFi tengan contraseñas fuertes. h) Revisa que la señal de WiFi no sea detectada fuera de las instalaciones. i) Detecta, si se activen puntos de acceso de WiFi no autorizados. j) Desactiva la función de WiFi en todos los equipos que no la requieran. k) Pon todo servidor accesible desde Internet en una zona desmilitarizada. l) Implementa un firewall de aplicaciones web. m) Implementa un sistema de seguridad de email. Soluciones: Firewalls, Análisis de reglas de firewall, Sistemas de prevención de intrusión, Proxies, Seguridad inalámbrica, Análisis de tráfico, Ciber inteligencia, Firewall de aplicaciones web, Seguridad de email.
DE.AE-2 Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	**a) Establece un procedimiento para revisar a detalle cada incidente. Crea un reporte por incidente que incluya un análisis de causa y efecto, se toma en cuenta los siguientes puntos:** - Analiza si el incidente tuvo un factor de falta de seguridad física. - Analiza si el incidente está relacionado a vulnerabilidades sin parchar. - Utiliza un sistema de ciber inteligencia para expander el análisis. b) Utiliza un sistema de caza de amenazas. c) Ajusta las políticas de seguridad informática para evitar que el incidente ocurra de nuevo. d) Pon a prueba el sistema de orquestación y automatización de incidentes, se crea

	incidentes de prueba para cada escenario y monitorea la respuesta. Ajusta los procesos si hay deficiencias en la respuesta. Soluciones: Ciber inteligencia, Orquestación y automatización de incidentes, Caza de amenazas, Proceso manual.
DE.AE-3 Los datos de los eventos, se recopilan y se correlacionan de múltiples fuentes y sensores.	Utiliza el sistema de administración e eventos para recopilar y correlacionar los datos. Solución: Administración de eventos.
DE.AE-4 Se determina el impacto de los eventos.	Analiza cada evento y determina el impacto real que tuvo si fue un ataque completado, o el impacto que pudo haber tenido si fue un evento, que se pudo detener. Incluye esta información en el reporte de incidentes descrito en DE.AE-2.a.
DE.CM-1 Se monitorea la red para detectar posibles eventos de seguridad informática.	a) Revisa que el sistema de administración de eventos (SIEM) y sistema de orquestación y automatización de incidentes (SOAR) funcionen adecuadamente. b) Establece un proceso para detectar indicadores de intrusión (IOCs) y programa *playbooks* en el SOAR para atenderlos. Investiga continuamente nuevos tipos de IOCs reportados por fuentes fidedignas. c) Implementa y prueba un sistema de prevención de denegación de servicio (DDOS). d) Utiliza un sistema de análisis de tráfico para detectar ataques de denegación de servicio que salen de tu organización para atacar a otros. Soluciones: Administración de eventos, Análisis de tráfico, Protección de denegación de servicio, Orquestación y automatización de incidentes.
DE.CM-4 Se detecta el código malicioso.	a) Implementa antimalware en todos los servidores de la red y de la nube. b) Si tienes aparatos IoT, implementa una solución de seguridad para IoT. c) Implementa un sistema de control de acceso a aplicaciones para bloquear la ejecución de software no autorizado. Soluciones: Antimalware, Seguridad IOT/SCADA, Control de acceso a aplicaciones.
DE.CM-7 Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	Utiliza un sistema de análisis de tráfico y de comportamiento de usuarios para monitorear conexiones, dispositivos, y software no autorizados.

	Soluciones: Análisis de tráfico, Análisis de comportamiento de usuarios.
DE.CM-8 Se realizan escaneos de vulnerabilidades.	a) Implementa un sistema de análisis de vulnerabilidades y escaneo de aplicaciones web, y realiza *scans* diario. b) Remedia las vulnerabilidades altas la misma semana en que fueron detectadas. c) Remedia las vulnerabilidades medias durante el mes. d) Remedia las vulnerabilidades bajas durante el trimestre. Soluciones: Administración de vulnerabilidades, Escaneo de aplicaciones web.
DE.DP-1 Los roles y misión de detección están bien definidos para asegurar la responsabilidad.	Establece responsables para cada indicador de intrusión y para cada métrica de desempeño.
RS.AN-2 Se comprende el impacto del incidente.	Genera un reporte de lecciones aprendidas de cada incidente ocurrido durante el periodo, y ajusta procesos si es necesario.
RS.AN-3 Se realizan análisis forenses.	Realiza un análisis forense de los incidentes graves, y ajusta controles y procesos. Solución: Software de análisis forense
RS.AN-5 Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	A) Asegúrate que los resultados presentados por el sistema de hacking ético automatizado, se implementen y automaticen con un sistema de higiene digital. b) Asegúrate que las notificaciones del servicio de ciber inteligencia, se tomen en cuenta para modificar controles. Soluciones: Software de higiene digital, Ciber inteligencia, Hacking ético automatizado.
RS.MI-2 Los incidentes son mitigados.	Revisa los incidentes del periodo que, no se hayan contenido, que generaron pérdidas de confidencialidad, integridad, o disponibilidad, y analiza cómo fueron mitigados, cómo, se restauró la confidencialidad, integridad o disponibilidad, y en qué tiempo. Ajusta los procesos si es necesario.
RS.MI-3 Las vulnerabilidades recientemente identificadas son mitigadas o, se documentan como riesgos aceptados.	Revisa las vulnerabilidades detectadas por el sistema de análisis de vulnerabilidades, por el sistema de hacking ético automatizado, por el proceso de caza de amenazas, y reportadas por el sistema de ciber inteligencia, y asegúrate que hayan sido mitigadas o documentadas como riesgos aceptados.

	Soluciones: Proceso manual
RS.IM-1 Los planes de respuesta incorporan las lecciones aprendidas.	Incorpora los reportes de lecciones aprendidas en RS.AN-2 al Plan de Respuesta a Incidentes y Continuidad de Negocios.
RC.RP-1: El plan de recuperación, se ejecuta durante o después de un incidente de seguridad informática.	Revisa los incidentes del periodo, y asegúrate que el Plan de Recuperación establecido en PR.IP-9, se haya cumplido de acuerdo al plan.

Fuente: adaptado de Instituto de Ciberdefensa (2021)

CONCLUSIONES

- Mediante la identificación de la base teórica que permite implementar procedimientos de análisis forense, se establecen los pasos necesarios para realizar el AFI, que incluyen diferentes fases como lo son, estudio preliminar, adquisición de datos, análisis e investigación, presentación u realización del informe pericial, dicho análisis permite determinar las causas del ataque al servidor de archivos.

- La determinación de una metodología adecuada acorde a los procesos legales vigentes para implementar el análisis forense, permite conocer que no existe una metodológica específica para realizar el AFI a un servidor de archivos, en la presente investigación, se determina como válida la metodología establecida por Tejada (2015), esta incluye las fases indicadas en la conclusión anterior, además, basa su metodología en la implementación de procesos en la gestión de incidentes, para la toma de medidas de seguridad informática y evitar futuros ataques.

- El desarrollarlo de pruebas sobre la metodología de análisis forense planteada, permite conservar la integridad y confidencialidad de los datos obtenidos, guardar y conservar la cadena de custodia de la evidencia, para que la investigación sea válida y usada para los fines respectivos, que se requiera en este tipo de análisis, así también, la metodología aplicada para la investigación permite conocer medidas de seguridad para este tipo de brechas informáticas, por citar una (ID.RA-3 Se identifican y se documentan las amenazas, tanto internas como externas), que si este control, se implementaba el ataque sufrido posiblemente hubiese tenido un grado de afectación menor.

- Al generar el informe sobre el análisis forense realizado al servidor de archivos de la institución, luego de haber recopilado y analizado las evidencias alojadas en varios directorios del servidor de archivos, se concluye que el servidor de archivos sufre un ataque tipo *ransomware* de cifrado, se compromete la integridad y confidencialidad en toda la información almacenada a nivel de datos y software así, también, este ataque usa ofuscamiento en los registros y logs del sistema para evadir los filtros de seguridad e infectar al equipo.

- A través de la generación del informe sobre el análisis forense realizado al servidor de archivos de la institución, se concluye que el uso de puertos por defecto asignados en los diferentes protocolos permite al atacante vulnerar al servidor y tomar acceso de este, es así, como conforme las evidencias, el ataque, se atribuye a la familia Dharma Ransomware, uno de sus métodos de ataque consiste en tomar acceso al equipo con el uso del protocolo DRP (por sus siglas en ingles *Remote Desktop Protocol*) (CVE-2019-0708 y CVE-2018-8453) y alojar un ejecutable en la maquina a infectar para posterior dejar un mensaje de rescate en la pantalla del equipo.

RECOMENDACIONES

- Analizar los registros de *regripper* que almacena el equipo para determinar cuál o cuáles fueron las causas de usar esta herramienta en el ataque de *ransomware* ejecutado, así, como validar, si, a través de esta utilidad, se alteran registros que maneja el equipo en su sistema operativo.

- Una vez identificado el método de ofuscamiento de datos (ROT13) en el servidor, se recomienda buscar información en los logs y registros del sistema, se utiliza este cifrado para continuar con el estudio de este ataque, toda vez que al suscitarse vulneraciones a equipos informáticos existen muchas evidencias dejadas por los atacantes, y así determinar ciertos detalles que no son producto de estudio en la presente investigación.
- Al contar con el archivo ejecutable que provoca el cifrado de archivos (1sass.exe), se recomienda realizar una ingeniería reserva a este ejecutable para establecer e identificar el tipo de cifrado que usa este ataque y obtener o desarrollar la llave de desencriptación para este *ransomware*.

- Toda vez que para la ejecución del *ransomware* en el escenario de prueba, se deshabilitan algunas medidas de seguridad del sistema operativo, se recomienda analizar el mecanismo usado por este *ransomware* para evadir las seguridades que tiene el sistema operativo Windows server para el rastreo de este tipo de ataques y la determinación de medidas de protección más específicas.

- Así, también, en base a las recomendaciones de seguridad propuestas en el capítulo 3, se recomienda implantar en la institución un equipo de respuesta ante emergencias informáticas conocido como CERT O CSIRT o a su vez establecer alianzas con entidades que cuenten con este equipo técnico con la finalidad de contrarrestar estas amenazas.

BIBLIOGRAFÍA

Al, M. P. G. et. (2019). WEB BROWSER ARTIFACTS RECOVERING METHODS FOR DIGITAL FORENSIC INVESTIGATION. *International Journal of Advanced Science and Technology*, *28*(17), 346-353.

Asamblea Nacional del Ecuador. (2021). *Código Orgánico Integral Penal*. Recuperado de http://biblioteca.defensoria.gob.ec/handle/37000/3020

Autopsy. (2021, diciembre 2). Autopsy | Digital Forensics. Recuperado 2 de diciembre de 2021, de Autopsy website: https://www.autopsy.com/

Banquet, P., & Bobillier, S. (2015). *Linux: Administración del sistema y explotación de los servicios de red*. Ediciones ENI.

Cabrera, J. L. R. (2014). *Sistemas Informáticos (GRADO SUPERIOR)*. Grupo Editorial RA-MA.

CheckMAL Inc. (2021). *AppCheck Anti-Ransomware: CrySis Ransomware (.id-{Random}.[data@recovery.sx].data) Block Video*. Recuperado de https://www.youtube.com/watch?v=TfYkDHTOETg

Consejo de la Judicatura. (2020). *Formato informe pericial 2020*. Recuperado de https://www.funcionjudicial.gob.ec/www/pdf/peritos/Formatoinformepericial2020.docx

Cryptii. (2021, diciembre 17). ROT13 decoder: Decrypt and convert ROT13 to text. Recuperado 17 de diciembre de 2021, de Cryptii website: https://cryptii.com/pipes/rot13-decoder

Dija, S., Indu, V., Sajeena, A., & Vidhya, J. A. (2017). A Framework for Browser Forensics in Live Windows Systems. *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 1-5. Coimbatore: IEEE. https://doi.org/10.1109/ICCIC.2017.8524412

Ecuavisa. (2021, agosto 2). Más de 1.200 investigaciones por delitos cibernéticos se registran en Ecuador. Recuperado 22 de noviembre de 2021, de

Www.ecuavisa.com website: https://www.ecuavisa.com/noticias/mas-de-1200-investigaciones-por-delitos-ciberneticos-se-registran-en-ecuador-MF766709

Ekta, & Bansal, U. (2021). A Review on Ransomware Attack. *ICSCCC 2021 - International Conference on Secure Cyber Computing and Communications*, 221-226. https://doi.org/10.1109/ICSCCC51823.2021.9478148

GNU. (2021, diciembre 5). Ddrescue—GNU Project—Free Software Foundation (FSF). Recuperado 5 de diciembre de 2021, de https://www.gnu.org/software/ddrescue/ddrescue_es.html

Gros, T., Dirauf, R., & Freiling, F. (2020). Systematic Analysis of Browser History Evidence. *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 1-12. New York, NY, USA: IEEE. https://doi.org/10.1109/SADFE51007.2020.00010

IBM Docs. (2021, septiembre 8). Recuperado 28 de enero de 2022, de https://prod.ibmdocs-production-dal-6099123ce774e592a519d7c33db8265e-0000.us-south.containers.appdomain.cloud/docs/es/i/7.3?topic=programs-file-server

Instituto de Ciberdefensa. (2021). Certificado en Seguridad Informática Ágil. Recuperado 2 de diciembre de 2021, de Instituto de Ciberdefensa website: https://import.cdn.thinkific.com/209151/courses/1485454/NISTparaKanban-211023-130227.xlsx

ITSafety. (2020, septiembre 15). ITSafety report—1sass.exe in Task Manager. How to delete 1sass.exe. Step-by-step guide. Recuperado 17 de diciembre de 2021, de ITSafety—Remove Malware Blog website: https://itsafety.net/report/20200915-02385fab3a4aac41db22b53e80d5bd91-1sass-exe_general-threat

Kali Linux. (2021, diciembre 2). Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. Recuperado 2 de diciembre de 2021, de Kali Linux website: https://www.kali.org/

Kaspersky. (2021, diciembre 1). El ransomware: Qué es, cómo se lo evita, cómo se elimina. Recuperado 1 de diciembre de 2021, de Latam.kaspersky.com website: https://latam.kaspersky.com/resource-center/threats/ransomware

Lee, G., Shim, S., Cho, B., Kim, T., & Kim, K. (2021). Fileless cyberattacks: Analysis and classification. *ETRI Journal*, *43*(2), 332-343. https://doi.org/10.4218/etrij.2020-0086

López Delgado, M. (2007). *Análisis Forense Digital* (2da ed.). Recuperado de http://www.criptored.upm.es/guiateoria/gt_m335a.htm

Malwarebytes. (2021, diciembre 1). Ransomware: Qué es y cómo eliminarlo. Recuperado 1 de diciembre de 2021, de Malwarebytes website: https://es.malwarebytes.com/ransomware/

Microsoft. (2021, noviembre 29). Windows Server. Recuperado 29 de noviembre de 2021, de https://www.microsoft.com/es-es/windows-server

Mukhopadhyay, A., & Prajwal, A. (2021). EDITH - A robust framework for prevention of cyber attacks in the covid era. *2021 2nd International Conference for Emerging Technology, INCET 2021*. https://doi.org/10.1109/INCET51464.2021.9456186

Nanni, B. (2021, diciembre 2). CAINE Live USB / DVD - informática forense digital forensics. Recuperado 2 de diciembre de 2021, de https://www.caine-live.net/

ONDATA. (2021, diciembre 2). Descripción EnCase Forensic Software I. Recuperado 2 de diciembre de 2021, de Ondata International website: https://www.ondata.es/

Ortiz, D. (2021, septiembre 3). Los ataques informáticos a pymes crecen en el Ecuador. Recuperado 23 de noviembre de 2021, de El Comercio website: https://www.elcomercio.com/tendencias/tecnologia/ataques-informaticos-pymes-crecen-ecuador.html

OSForensics—Digital investigation for a new era by PassMark Software. (2021). Recuperado 24 de febrero de 2022, de https://www.osforensics.com

Security, P. (2017). *Informe Ransomware de la familia Crysis/Dharma*. 9.

Singh, N., V. Krishnaswamy, & Zhang, J. Z. (2022). Intellectual structure of cybersecurity research in enterprise information systems. *Enterprise Information Systems*. https://doi.org/10.1080/17517575.2022.2025545

Smith, B. (2020, diciembre 8). data File ☣ Virus—How to remove & decrypt [data@recovery.sx].data? Recuperado 17 de diciembre de 2021, de How To Fix Guide website: https://howtofix.guide/data-file-virus-datarecovery-sx/

Suma, G. S., Dija, S., & Pillai, A. T. (2017). Forensic Analysis of Google Chrome Cache Files. *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 1-5. Coimbatore: IEEE. https://doi.org/10.1109/ICCIC.2017.8524272

Tanenbaum, A. S. (2003). *Sistemas operativos modernos*. Pearson Educación.

Tejada, E. C. (2015). *Gestión de incidentes de seguridad informática. IFCT0109*. IC Editorial.

Umar, R., Yudhana, A., & Nur Faiz, M. (2018). Experimental Analysis of Web Browser Sessions Using Live Forensics Method. *International Journal of Electrical and Computer Engineering (IJECE)*, *8*(5), 2951. https://doi.org/10.11591/ijece.v8i5.pp2951-2958

ANEXOS

Anexo 1. Formato entrevista

Entrevista		
Existe área de TI en la institución	SI	NO
	✔	X
Existe plan de contingencia para desastres informáticos	SI	NO
	X	✔
Alguna vez ha existido un ataque informático a su institución sin contar el que actualmente se investiga	SI	NO
	X	✔
El equipo atacado es de propiedad de la empresa o de un cliente	Propio	Cliente
	X	✔
Sabe usted que sistema operativo usa el equipo (En caso de respuesta afirmativa indicar cual es)	SI	NO
	✔ (Windows Server 2008)	X
Qué tipo de equipo es	PC	SERVIDOR
	X	✔
El equipo esta virtualizado o físico	Físico	Virtual
	✔	X
Conoce la capacidad de almacenamiento del equipo (de ser afirmativa la respuesta indique el tamaño)	SI	NO
	✔ (500 GB)	X
El equipo está encendido o apagado	**Encendido**	**Apagado**
	X	✔

Se realiza monitoreo en la red de forma constante (en caso de respuesta afirmativa indicar si dispone de respaldos)	**SI**	**NO**
	X	✔
Conoce la fecha que sucedió el evento (en caso de respuesta afirmativa indicar la misma)	**SI**	**NO**
	X	✔
Conoce el tipo de ataque suscitado (en caso de respuesta afirmativa indicar)	**SI**	**NO**
	✔ (Cifrados de datos almacenados)	X
Se ha realizado un respaldo de los datos para realizar el AFI	**SI**	**NO**
	X	✔

Fuente: elaboración propia

Anexo 2. Formato acta entrega recepción

ACTA ENTREGA DE EQUIPOS COMPUTACIONALES

Hoy XX del mes XXXXX de XXX el departamento de TI, mediante el siguiente documento realiza la entrega formal de los equipos computacionales para la realización del análisis forense, quién declara recepción de estos en buen estado y se compromete a cuidar de los recursos y hacer uso de ellos para los fines establecidos.

Datos del encargado de realizar el análisis forense informático

Nombres, Apellidos	
Cédula	
Departamento	
Cargo	

EQUIPOS COMPUTACIONALES ASIGNADOS

Descripción del producto	
Número de serie	
Numero de inventario	

Descripción	Marca	Modelo	Características	Serial

OBSERVACIONES

Añadir en este apartado la cadena de custodia

ENTREGA
Fecha entrega: xx de xx de xx

Entregado por:	**Recibido por:**
NOMBRE	**NOMBRE**
FIRMA	**FIRMA**
Cargo	Analista AFI

DEVOLUCIÓN
Fecha devolución: xx de xx de xx

Entregado por:	**Recibido por:**
NOMBRE	**NOMBRE**
FIRMA	**FIRMA**
Analista AFI	Cargo

Fuente: elaboración propia

Anexo 3. Formato acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN PARA LA REALIZACIÓN DE ANALISIS FORENSE INFORMÁTICO AL SERVIDOR DE ARCHIVOS DE LA EMPRESA XXXXX

Intervienen en la celebración del presente **ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN SOBRE EL USO DE COPIAS DEL SERVIDOR DE ARCHIVOS DE LA EMPRESA XXXXXX** como comparecientes:

Por una parte, la EMPRESA XXXX, representada por su Gerente General, el señor XXXXXXX con cedula de ciudadanía Nro. XXXXXX y por otra parte el Ing. Jaime Daniel Analuisa Muso con cédula de ciudadanía Nro. XXXXXX en calidad de Maestrante de la Pontificia Universidad Católica sede Ambato.

Quienes libre y voluntariamente celebran el presente acuerdo. Los comparecientes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información con base a las siguientes cláusulas.

CLÁUSULA PRIMERA. – ANTECEDENTES:

El artículo 178 del Código Orgánico Integral Penal establece: “La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años…”;

Que el MAESTRANTE y EL INTERESADO están interesados en evaluar las posibles vulnerabilidades en sus activos informáticos para, lo cual, es necesario intercambiar información confidencial entre ellas. LAS PARTES acuerdan que dicha información sea entendida como “INFORMACIÓN CONFIDENCIAL”.

Que se define como Información Confidencial, toda la información relativa o de propiedad del INTERESADO, que cumpla los siguientes requisitos: a. Que sea

reservada, en el sentido de que no sea generalmente conocida ni de fácil obtención por quienes se encuentran en el medio en, el cual, dicha información es manejada; y b. Que sea designada como confidencial por su titular. Esta designación se la realiza de forma escrita o es ratificada de la misma manera, depende de la forma en, la cual, la respectiva Información Confidencial es divulgada por el Titular al Receptor.

La Información Confidencial incluye, pero, sin limitarse a ello: copias de seguridad de sus activos bit a bit, volcado de memoria ram, cadenas de custodia de los activos y otra información que sean comunicados por cualquiera de las PARTES, a la otra parte de este acuerdo, cualquiera que sea la forma en, que se produzca dicha comunicación (oral, escrita, visual, dibujos, ficheros informáticos, etc.), y que sea facilitado por cualquiera de las PARTES a través, en relación o como consecuencia del presente Acuerdo de Confidencialidad, es voluntad de ambas partes el restringir el uso y divulgación de la Información.

CLÁUSULA SEGUNDA. - OBJETO: En virtud de los antecedentes expuestos, por medio del presente instrumento los comparecientes se obligan expresamente a guardar sigilo, confidencialidad y reserva sobre el contenido de toda la información generada, verbal, escrita o en ficheros informáticos, que se comparta entre los comparecientes respecto al desarrollo del análisis forense, mismo, que se comprometen a hacer uso de la información, únicamente para las actividades relacionadas con las funciones que desempeña, conforme a las obligaciones y prohibiciones legales pertinentes.

Por virtud del presente Acuerdo, los Receptores de Información utilizaran la Información Confidencial única y exclusivamente con fines educativos para el cumplimiento del OBJETO del presente acuerdo. Una vez cumplido el OBJETO del Acuerdo, los Receptores no hacen uso alguno de la información

CLÁUSULA TERCERA. - DERECHOS Y OBLIGACIONES: Las partes indistintamente son RECEPTORES y TITULARES de la información según corresponda. El Receptor declara y reconoce que el recibo o el uso de la Información Confidencial que le sea divulgada por el Titular no le concede, ni expresa ni implícitamente, autorización, permiso o licencia de uso de marcas

comerciales, patentes, derechos de autor o de cualquier otro derecho de propiedad intelectual de propiedad del Titular. Ni este acuerdo, ni la divulgación, recibo de información, sea confidencial o no, constituye o implica promesa de efectuar contrato alguno por cualquiera de LAS PARTES. Son obligaciones de los comparecientes:

1. Guardar la reserva y confidencialidad, sin el deterioro de cualquier tipo de información, que se le suministre o a, la cual, llegare a tener acceso o conocimiento;

2. Mantener en forma estrictamente reservada y confidencial toda la información que por razón de su competencia tenga acceso, por lo tanto, se obliga a abstenerse de usar, disponer, divulgar y/o publicar por cualquier medio, oral, escrito, y/o tecnológico y en general, aprovecharse de ella en cualquier otra forma para efectos ajenos a los intereses de la Institución a, la cual, pertenece.

3. Utilizar la información suministrada por EL TITULAR, únicamente para los fines de investigación educativa del proceso de análisis forense.

4. No realizar copia o duplicado alguno de la información mencionada en este acuerdo sin la autorización previa y escrita de la otra parte; tampoco divulgan dicha información a terceras personas sin que medie igualmente la respectiva autorización previa y escrita de la otra parte.

5. Adoptar las medidas de protección de la Información Confidencial que sean necesarias para garantizar su carácter confidencial, se evita su conocimiento por parte de terceros y su divulgación no autorizada.

6. Devolver al Titular y/o destruir (si es solicitado por el Titular) los medios físicos en, los cuales, le haya sido entregada la Información Confidencial, junto con las copias que de la misma haya elaborado, y eliminar cualquier grabación, filmación, archivo electrónico o similar que contenga total o parcialmente Información Confidencial, en uno y otro caso dentro de los quince (15) días calendario siguientes a la fecha de cesación del uso autorizado de la Información Confidencial, o al momento en que así los solicite el Titular, lo que primero ocurra.

7. Informar al Titular de la Información Confidencial respecto de cualquier orden o solicitud de divulgación que reciba de cualquier autoridad, de forma inmediata al recibo de la respectiva orden o solicitud, y en todo caso, de forma que le permita al Titular de la Información Confidencial oponerse de forma oportuna a dicha orden o solicitud.

8. No utilizar la Información, para un propósito distinto al OBJETO del presente acuerdo, sin el previo y expreso consentimiento del Titular. Sin perjuicio de lo anterior, LAS PARTES reconocen que el uso de la Información para un propósito distinto al uso autorizado requiere la firma de otro acuerdo entre LAS PARTES.

9. Se obligan las partes a restringir el acceso a la Información Confidencial recibida del Titular, acceder a la misma única y exclusivamente el investigador y su tutor para, los cuales, el acceso a la Información Confidencial sea necesario para el cumplimiento del OBJETO del presente acuerdo. Las citadas personas están sujetas a las restricciones de confidencialidad previstas en el presente acuerdo.

10. Se comprometen las partes a adoptar las mismas medidas de seguridad, para impedir que la Información Confidencial sea divulgada, que aquéllas que adopta para la protección de su propia Información Confidencial y secretos comerciales.

CLÁUSULA CUARTA. – IMPLICACIONES DE LA RECEPCIÓN DE LA INFORMACIÓN Y RESPONSABILIDAD Los comparecientes actúan con responsabilidad en el buen uso de la información, lo que supone entre otros deberes, el de limitar la divulgación autorizada al menor número de personas, y el de tomar las medidas idóneas y eficaces para evitar el tráfico y fuga indebida de la información, así como su uso por fuera de los límites de este convenio. El incumplimiento del deber de reserva establecido en este acuerdo constituye violación de secreto y justa causa de terminación unilateral de la relación civil con NOMBRE EMPRESA, sin desmedro de las indemnizaciones legales correspondientes.

CLÁUSULA QUINTA. – SANCIONES: Para la aplicación de sanciones se toma en cuenta lo establecido en la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Código Orgánico

Integral Penal, Ley Orgánica del Sistema Nacional de Registro de Datos Púbicos y demás normativa aplicable; sin perjuicio de las acciones civiles y penales que procedan en cada caso. La parte que incumpliera las estipulaciones de este instrumento, son sancionados por la autoridad competente.

CLÁUSULA SEXTA. – VIGENCIA: El presente instrumento tiene una vigencia de 6 meses a partir de la fecha de suscripción.

CLÁUSULA SÉPTIMA – ACUERDO TOTAL: Este acuerdo incluye el total entendimiento entre los comparecientes con relación a la materia de, la cual, se trata este documento. Cualquier añadidura o modificación a este acuerdo es hecha por escrito y firmada por todos los comparecientes. En el evento de, que se produzca el incumplimiento de alguna de las cláusulas estipuladas en el presente acuerdo, la parte afectada, notifica del incumplimiento, sin perjuicio de las acciones y sanciones previstas en la normativa vigente. Una vez comprendido por los comparecientes el contenido y efectos del presente instrumento expresamente se ratifican en él, para fe y constancia se firma el presente documento por quienes en él intervinieron, en la ciudad de XXXX, el día XX del mes de XXX del año XXX, en dos ejemplares del mismo tenor y validez.

NOMBRE REPRESENTANTE	Ing. Jaime Daniel Analuisa Muso
NOMBRE EMPRESA	MAESTRANTE
Firma: _____	Firma: _____
C.C. XXXXXXXXXX	C.C. XXXXXXXXXX

Fuente: elaboración propia

Anexo 4. Formato informe Consejo de la Judicatura

FORMATO DE INFORME PERICIAL

Las y los peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCION JUDICIAL. Por lo tanto, el presente formato puede ser considerado por los auxiliares de justicia para la presentación de los informes periciales, sin perjuicio a lo establecido en normas legales específicas.

"INFORME PERICIAL"

1. **DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA**

Nombre Judicatura o Fiscalía	
No. de Proceso	
Nombre y Apellido de la o el Perito	
Profesión y Especialidad acreditada	
No. de Calificación	
Fecha de caducidad de la acreditación	
Dirección de Contacto	
Teléfono fijo de contacto	
Teléfono celular de contacto	
Correo electrónico de contacto	

2. **PARTE DE ANTECEDENTES**, en donde se debe delimitar claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por el juez, el fiscal y/o lo solicitado por las partes procesales.

3. **PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE**, en donde se debe explicar claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. La o el perito deberá relacionar los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizará si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

4. **PARTE DE CONCLUSIONES,** luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. Se prohíbe todo tipo de juicios de valor sobre la actuación de las partes en el informe técnico. El informe solamente versará sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dirá sobre el accionar de las partes procesales en el caso en particular. Las conclusiones solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no será tomado en cuenta al momento de resolver, y será tomado en consideración para la evaluación de la o el perito.

5. **PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO**, deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, etc); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas de la o el perito para llegar a la conclusión correspondiente. No se cumplirá con este requisito si, no se sustenta la conclusión con documentos, objetos o con la explicación técnica y científica exigida en este numeral. La o el perito deberá razonar y motivar diáfanamente la razón de sus dichos, esto es, justificar desde todo punto de vista las conclusiones que incluya en el informe. En caso de que no fundamente sus conclusiones y esto sea informado por el juez, la jueza, o el/la fiscal, será considerado al momento de la evaluación de la o el perito.

6. **OTROS REQUISITOS,** si la ley procesal correspondiente determina la inclusión de requisitos adicionales a los establecidos por el reglamento, la o el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.

7. **INFORMACIÓN ADICIONAL,** la o el perito podrá incluir cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.

8. **<u>DECLARACIÓN JURAMENTADA</u>,** la o el perito deberá en la parte final del informe, declarar bajo juramento que su informe es independiente y corresponde a su real convicción profesional, así como, también, que toda la información que ha proporcionado es verdadera.

9. **<u>FIRMA Y RÚBRICA</u>,** al final del informe se deberá hacer constar la firma y rúbrica de la o el perito, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."

Nota: el presente ejemplar es una guía de los ítems que al menos deben considerar los auxiliares de justicia al momento de elaborar sus informes periciales.