UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONA DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

"Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencia Digitales"

PRESENTADO PARA OPTAR EL TÍTULO PROFESIONAL DE:

Ingeniero(a) en Computación e Informática

Investigador:

Erick Javier Casas Villar

Rosa Lorena Araceli Llién Valiente

Asesora:

Dra. Ing. Jessie Leila Bravo Jaico

Lambayeque, 2021

“Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencia Digitales”

Tesis para optar el Título Profesional de Ingeniero(a) en Computación e Informática, presentado por:

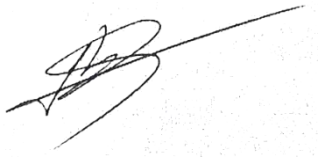
Bach. Erick Javier Casas Villar

Bach. Rosa Lorena Araceli Lluén Valiente

.....

Msg. Luis Alberto Reyes Lescano

Presidente



.....

Ing. Franklin Édison Terán Santa Cruz

Secretario

.....

Ing. Denny Fuentes Adrianzen

Vocal

.....

Dra. Ing. Jessie Leila Bravo Jaico

Asesora

COPIA ACTA DE APROBACIÓN DE PROYECTO

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
D E C A N A T O

Año del Bicentenario del Perú: 200 Años de Independencia

RESOLUCION Nº 385-2021-VIRTUAL-D/FACFyM

Lambayeque, 21 de Junio del 2021

VISTO:

El documento virtual S/N presentado por el docente, M.Sc. Ing. Luis Alberto Reyes Lescano mediante el cual solicita se oficialice el desarrollo del Proyecto de Tesis que se encuentra bajo responsabilidad del Bachiller y la Bachiller en Ingeniería en Computación e Informática, **Casas Villar Erick Javier y Lluén Valiente Rosa Lorena Araceli**

CONSIDERANDO:

- Que, por Resolución N°224-VIRTUAL-2020-D/FACFyM se nombra a los docentes, M.Sc. Ing. Luis Alberto Reyes Lescano, Ing. Franklin Edinson Terán Santa Cruz, y Mg. Ing. Denny John Fuentes Adrianzén como miembros del jurado para revisión y aprobación del proyecto de tesis "Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencias Digitales" desarrollado por los Egresados de la Escuela Profesional de Ingeniería en Computación e Informática, Casas Villar Erick Javier y Lluén Valiente Rosa Lorena Araceli;
- Que, el docente M.Sc. Ing. Luis Alberto Reyes Lescano, mediante documento virtual S/N comunica que el jurado designado por Resolución N° 224-VIRTUAL-2020-D/FACFyM, cual preside, han revisado el Proyecto de Tesis "Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencias Digitales" que se encuentra bajo responsabilidad del Bachiller y la Bachiller en Ingeniería en Computación e Informática, Casas Villar Erick Javier y Lluén Valiente Rosa Lorena Araceli, concluyendo que el proyecto se encuentra apto para ser ejecutado, solicitando por ello se oficialice mediante la respectiva resolución;

En uso de las atribuciones que le confiere al señor Decano la Ley Universitaria 30220 y el artículo 34º del Estatuto de la Universidad Nacional Pedro Ruiz Gallo.

SE RESUELVE:

1° **OFICIALIZAR,** el desarrollo del Proyecto de Tesis **"Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencias Digitales"** que se encuentra bajo responsabilidad del Bachiller y la Bachiller en Ingeniería en Computación e Informática, **Casas Villar Erick Javier y Lluén Valiente Rosa Lorena Araceli**.

2º Da a conocer la presente resolución a la Escuela Profesional de Ingeniería en Computación e Informática, Unidad de Investigación FACFyM, Asesora: Dra. Ing. Jessie Leila Bravo Jaico, Jurado: M.Sc. Ing. Luis Alberto Reyes Lescano, Ing. Franklin Edinson Terán Santa Cruz, Mg. Ing. Denny John Fuentes Adrianzén, Interesados, y Archivo.

REGISTRESE, COMUNIQUESE y ARCHIVESE

SECRETARIO DE FACULTAD
Dra. Iris Margarita Tejada Romero
Secretaria Docente FACFyM

DECANO
Dr. Enrique Wilfredo Carpena Velásquez
Decano

DECLARACIÓN JURADA DE ORIGINALIDAD

Nosotros, Erick Javier Casas Villar y Rosa Lorena Araceli Lluén Valiente, investigadores principales, y Jessie Leila Bravo Jaico, asesora del trabajo de investigación "Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencia Digitales" declaramos bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se demostrará lo contrario, asumimos responsablemente la anulación de este informe y por ende el proceso administrativo a que hubiera lugar. Que puede conducir a la anulación del título o grado emitido como consecuencia de este informe.

Lambayeque, julio del 2021

Bach. Erick Javier Casas Villar

Bach. Rosa Lorena Araceli Lluén Valiente

Dra. Ing. Jessie Leila Bravo Jaico

COPIA ACTA DE SUSTENTACIÓN

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DECANATO
Ciudad Universitaria - Lambayeque

ACTA DE SUSTENTACIÓN VIRTUAL N°004-2022-D/FACFyM

Siendo las 08:00 am del día 18 de enero del 2022, se reunieron vía plataforma virtual, https://meet.google.com/ofk-kyqh-pxe los miembros del jurado evaluador de la Tesis titulada:

"Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencia Digitales"

Designados por Resolución N° 224-VIRTUAL-2020-D/FACFyM de fecha 02 de octubre del 2020.

Con la finalidad de evaluar y calificar la sustentación de la tesis antes mencionada, conformada por los siguientes docentes:

M.Sc. Ing. Luis Alberto Reyes Lescano	Presidente
Mg. Ing. Franklin Edinson Terán Santa Cruz	Secretario
Mg. Ing. Denny John Fuentes Adrianzén	Vocal

La tesis fue asesorada por la Dra. Jessie Leila Bravo Jaico, nombrada por Resolución N°1679-2019-D/FACFyM de fecha 17 de diciembre del 2019.

El Acto de Sustentación fue autorizado por Resolución N° 036-2022-VIRTUAL-D/FACFyM de fecha 13 de enero del 2022.

La Tesis fue presentada y sustentada por los Bachilleres: Casas Villar Erick Javier y Lluén Valiente Rosa Lorena Araceli, y tuvo una duración de 65 minutos.

Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado se procedió a la calificación respectiva, otorgándole el Calificativo de **17 (Diecisiete)** en la escala vigesimal, mención **Bueno**.

Por lo que quedan aptos para obtener el Título Profesional de **Ingeniero(a) en Computación e Informática**, de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ciencias Físicas y Matemáticas y la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 09:05 am se dio por concluido el presente acto académico, dándose conformidad al presente acto con la firma de los miembros del jurado.

M.Sc. Ing. Luis Alberto Reyes Salazar
Presidente

Mg. Ing. Franklin Edinson Terán Santa Cruz
Secretario

Mg. Ing. Denny John Fuentes Adrianzén
Vocal

Dra. Ing. Jessie Leila Bravo Jaico
Asesora

CERTIFICO: Que, es copia fiel del original
Fecha: 08 / 02 / 2022
M.Sc. Marco Antonio Martín Peralta Lui
SECRETARIO DOCENTE - FACFyM
VÁLIDO PARA TRÁMITES INTERNOS DE LA UNPRG

COPIA DE CONSTANCAI DE TURNITIN

Aplicación de la Informática Forense para la Recuperación de Datos y Reconocimiento de Evidencia Digitales

INFORME DE ORIGINALIDAD

8%	8%	0%	%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	docplayer.es Fuente de Internet	1 %
2	hdl.handle.net Fuente de Internet	1 %
3	www.researchgate.net Fuente de Internet	1 %
4	v1.overleaf.com Fuente de Internet	<1 %
5	es.slideshare.net Fuente de Internet	<1 %
6	repositorio.uladech.edu.pe Fuente de Internet	<1 %
7	repositorio.usmp.edu.pe Fuente de Internet	<1 %
8	es.scribd.com Fuente de Internet	<1 %
9	repositorio.unasam.edu.pe Fuente de Internet	

DEDICATORIA

A mi hermano César, que tome como ejemplo su esfuerzo y dedicación para alcanzar sus metas.

A mi madre Nancy Villar, por su apoyo incondicional, por sus consejos y motivación constante para lograr cumplir mis objetivos.

A mi padre Cesar Casas, por enseñarme a ser perseverante y constante para alcanzar mis metas.

TuMi

Erick Javier Casas Villar

A Dios por siempre estar guiando mi camino para poder lograr mis metas.

A mi madre, por su apoyo en todo momento, y no dejar que me rinda nunca a pesar de las circunstancias.

A mi padre, por darme todo lo que siempre necesite y permitirme llegar a ser la profesional que hoy en día soy.

MiTu

Rosa Lorena Araceli Lluén Valiente

AGRADECIMIENTO

A Dios, por permitirnos llegar hasta el final y lograr convertirnos en profesionales de bien.

A la ingeniera Jessie Leila Bravo Jaico, por la paciencia y dedicación en la orientación para poder llevar a cabo el desarrollo de esta tesis.

A nuestros familiares, por su constante apoyo y respaldo frente a las adversidades que se nos presentaron.

Resumen

Durante el desarrollo de la presente tesis, se ha realizado una investigación donde se obtuvo un alto grado de fiabilidad en los procesos, programas y técnicas utilizados en los casos de delitos informáticos. Además, se ha revisado la veracidad de los resultados con ayuda de equipos y software, los cuales ofrecen resultados al usuario a partir de las evidencias o información obtenida.

El uso de los programas tecnológicos existentes en la actualidad, las cuales han tenido una gran acogida en el área de la informática forense, fueron de gran ayuda para el desarrollo de esta tesis.

El objetivo principal de esta tesis es la implementación de una metodología que se pueda aplicar en la informática forense en el área de delitos informáticos, beneficiando a las personas que lo utilicen. Sin embargo, el uso de estos programas tecnológicas requiere una investigación muy detallada y concisa.

Palabras claves

Delitos informáticos, software, informática forense, metodología

Abstract

During the development of this thesis, an investigation has been carried out where a high degree of reliability was obtained in the processes, tools and techniques used in cases of cybercrimes. In addition, the veracity of the results has been reviewed with the help of equipment and software, which offer results to the user from the evidence or information obtained.

The use of the technological tools existing today, which have had a great reception in the area of computer forensics, were of great help for the development of this thesis.

The main objective of this thesis is the implementation of a methodology that can be applied in computer forensics in the area of cybercrimes; benefiting people who use it. However, the use of these technological tools requires very detailed and concise research.

Keywords: Cybercrimes, software, computer forensics, methodology

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

INDICE DE ANEXOS DE LOS CASOS

Anexo de Caso 01

Anexo de Caso 02

INTRODUCCIÓN

En la actualidad, la mayoría de las personas almacenan y comparten su información personal en la internet y en dispositivos digitales, por este motivo ocurren diversos delitos informáticos que atentan contra la seguridad del usuario. Este proyecto de investigación nos muestra la importancia de la seguridad informática, ya que el medio más común para cometer delitos e infracciones es la tecnología.

Para el desarrollo de esta investigación tenemos algunos antecedentes relacionados, como la "Metodología de la informática forense en la atención de delitos informáticos de cibergrooming" (Quizphe, 2015), nos explica sobre el desarrollo de las fases para la implementación del proceso de investigación en el análisis de la evidencia. En la tesis "Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la policía nacional del Perú – Huaraz" (de la Cruz, 2017), permite analizar las metodologías y herramientas existen, las cuales determinan la relación entre la informática forense y la seguridad informática. Otro antecedente relacionado con nuestro proyecto es del autor Tapia (2017) en su tesis "Implementación de metodología de análisis forense para la dirección de tecnologías de información y comunicaciones de la armada del ecuador (DIRTIC)" el cual explica el desarrollo de una metodología que consta de una serie de pasos que permitirá analizar y presentar las evidencias ante las vulnerabilidades en la infraestructura informática. También tenemos como referencia al autor Cacha Arana (2019) en sus tesis "Peritaje Informático basado en una nueva metodología híbrida en 2M % J Ingenieros – Huaraz", el cual explica la elaboración de una guía de procesos estandarizada con la finalidad de resolver los casos de delitos informáticos. Finalmente, como última referencia tenemos a Ramírez (2008) en su tesis "Sistema informático basado en algoritmos evolutivos para mejorar el proceso de identificación forense de evidencias digitales", el cual explica la falta de

tecnologías y herramientas existentes para la identificación de evidencias digitales, para ello se tiene como objetivo la elaboración de un sistema que permitirá identificar y agilizar el proceso de identificación de las evidencias digitales.

La problemática que abarca el proyecto de investigación es la falta de una guía de procesos definidos para la aplicación de la informática forense que permita resolver los casos de delitos informáticos en la DIVINCRI de la ciudad de Chiclayo.

El objetivo principal de este proyecto de investigación es la elaboración de una guía de procesos para aplicar la informática forense a través de la metodología PURI (Proceso Unificado de Recuperación de Información) permitiendo recuperar información y evidencias digitales a través de los diferentes procesos y herramientas.

La aplicación de la informática forense permitirá agilizar los procesos para la recuperación de datos y evidencias digitales que servirán en los casos de delitos informáticos.

Para el desarrollo del proyecto usaremos los conceptos definidos de la metodología PURI, el cual nos ofrece información de los pasos a seguir para la obtención de datos y evidencias digitales en los casos de delitos informáticos como es la identificación, adquisición, preservación, análisis y presentación. Además, emplearemos el uso de diferentes programas que nos permitirán verificar el estado de integridad de los dispositivos de almacenamiento (USB, disco duro, DVD) como también recuperar archivos eliminados, ocultos y encriptados según sea el caso que se presente.

En base lo mencionado anteriormente, a continuación, se detallará la estructura del proyecto por capítulos:

En el capítulo I, se abordará el Diseño Teórico, el cual describirá la realidad problemática, los objetivos de la investigación, el marco metodológico, marco teórico y la base teórica.

A continuación, en el capítulo II, Métodos y materiales, se detalla el diseño de contratación de hipótesis, la descripción de la población y muestra, la explicación de las técnicas, instrumentos, equipos y materiales utilizados en este proyecto como también el desarrollo de la metodología PURI.

Asimismo, en el capítulo III, Resultados y Discusión, se muestran los resultados de los objetivos propuestos en el proyecto de investigación.

Finalmente, en el capítulo IV y V, Conclusiones y Recomendaciones, se detalla los argumentos, confirmaciones y recomendaciones de los objetivos desarrollados.

Capítulo I: Diseño Teórico

1.1. Planteamiento de Investigación

1.1.1. Síntesis de la Situación Problemática

En la actualidad, el medio más común para cometer delitos e infracciones es la tecnología. Por ese motivo, el área forense está obteniendo una mayor importancia dentro de la ingeniería informática ya que la mayoría de las personas usan los dispositivos digitales como principal medio de almacenamiento de información, así que la manipulación de datos, daños en la información confidencial o violación a la seguridad informática, son algunos de los delitos informáticos más comunes que se realizan a través de un escritorio.

En el entorno internacional los delitos informáticos son muy comunes, según Rosa (2020) en el periódico "El diario del centro del país" indica que cada día un millón de personas son víctimas de delitos informáticos. El principal problema es que en algunas ciudades del mundo no se aplica la informática forense debido a que no se conoce las diversas técnicas, herramientas o metodologías que se requiere para la obtención de pruebas con el objetivo de esclarecer algún acto ilegal y así lograr descubrir al responsable de estos actos. Sin embargo, a comparación de nuestro país, se puede decir que el desarrollo de sus casos es de manera más eficaz, ya que, si bien no cuentan con la metodología adecuada, si tienen los recursos necesarios para actuar de manera inmediata.

En el Perú, la informática forense no se encuentra aplicado en todo el país, ya que se carece de conocimiento y recursos para salvaguardar la información y dar una respuesta o una solución a los delitos informáticos. Sin embargo, el Perú cuenta con una oficina central de investigación en la ciudad de Lima donde se realiza los procesos de investigación de los delitos informáticos, pero tiene como problema, no poder dar solución a todos los casos.

Un ejemplo de delitos informáticos en nuestro país según la noticia en el portal web Agencia Peruana de noticias (Anonimo, 2016), es el caso de Kaspersky Lab., donde el 42% de usuarios peruanos sufrieron un intento de ataque de malware. El panorama fue preocupante ya que Perú está en segundo lugar en el ranking regional debajo de Brasil (2015). La tasa de denuncias según la policía nacional del Perú es de 30 a 35 delitos informáticos semanales, entre los que resaltan los fraudes electrónicos (50%), suplantación de identidad (10%) y manipulación de información como fotos y videos de menores (20%).

Mientras tanto en los últimos años en la ciudad Chiclayo se está siendo más frecuentes las denuncias sobre los delitos informáticos. El principal problema radica en que no cuenta con un estándar de procesos definido donde se pueda desarrollar y aplicar la informática forense. Según lo explicado por el superior del área de Delitos contra la Libertad de la DIVINCRI (División de Investigación Criminal), las denuncias de mayor nivel son derivados a la DIRINCRI (Dirección de Investigación Criminal) de la ciudad de Lima para que se realice el proceso correspondiente; sin embargo, esto ocasiona la innecesaria dilatación de tiempo en la verificación del caso, ya que el área encargada de seguir los procesos de la denuncia atiende a la vez las denuncias de otras ciudades del país, lo que genera incomodidad en las personas que desean una respuesta de manera inmediata. Debido a esto es necesario aplicar la informática forense para que los procesos se realicen de manera eficiente con ayuda de diferentes herramientas, técnicas y metodologías que facilite el análisis, como podría ser el caso de un computador personal que haya sido objeto de un proceso delictivo extrayendo toda su información, como también casos donde se analizarán los dispositivos de almacenamientos externos como el USB, CD, disco duro, entre otros dispositivos digitales.

En conclusión, la aplicación de la informática forense es de vital importancia en la respuesta inmediata a los delitos informáticos ya que de esta manera se lograría obtener toda

la información perdida o manipulada, rastrear el origen y determinar cuál sería el resultado de los procesos.

1.2. Formulación del Problema de Investigación

¿Cómo la aplicación de la informática forense permitirá la recuperación de datos y evidencias digitales para resolver los casos de delitos informáticos?

1.3. Objetivos

1.3.1. Objetivo General

Aplicar la informática forense para la recuperación de datos y reconocimiento de las evidencias digitales, permitiendo resolver los casos de delitos informáticos.

1.3.2. Objetivo Específico

- Realizar una guía de procesos para la aplicación de la informática forense.
- Realizar estudios sobre las diferentes herramientas existentes para la recopilación de datos y evidencias digitales.
- Plantear un procedimiento para la identificación, adquisición, análisis y presentación de los datos.
- Plantear un procedimiento para la identificación, preservación, análisis y presentación de las evidencias digitales.
- Realizar la evaluación económica de la propuesta.

1.4. Marco Metodológico

1.4.1. Tipo de Investigación

Investigación teórica - aplicada

1.4.2. Hipótesis

La aplicación de la informática forense permitirá obtener datos y evidencias digitales que ayudará en los procesos de los delitos informáticos.

1.4.3. Definición y Operacionalización de variables

- Variable Independiente: Aplicación de la informática forense
- Variable Dependiente: Recuperación de datos y evidencias digitales

Tabla 1: Operacionalización de Variable

¡Error! No se encuentra el origen de la referencia. Fuente: Elaboración Propia

1.5. Marco Teórico

1.5.1. Antecedentes

Internacionales

Quizphe (2015) en su tesis "Metodología de la informática forense en la atención de delitos informáticos de cibergrooming". Explica como implementar una metodología para el cibercrimen, específicamente en los delitos de acoso sexual a menores de edad, en el cual se desarrolla las fases de investigación y análisis de la evidencia, aplicando técnicas y herramientas para posteriormente realizar la presentación de las pruebas. Este proyecto de investigación ayudará en nuestro tema propuesto en la aplicación de los pasos de la metodología (identificación, adquisición, preservación, análisis y presentación) obteniendo como resultado una guía para la recuperación de datos y evidencia digitales.

Tapia (2017) en su tesis "Implementación de metodología de análisis forense para la dirección de tecnologías de información y comunicaciones de la armada del ecuador (DIRTIC)". Propone implementar una metodología que permita a la dirección de tecnologías identificar los diversos problemas de vulnerabilidad en la infraestructura informática, para ello se hará uso de diferentes herramientas con el fin de obtener resultados mucho más eficaces y confiables. Este proyecto nos ayudará a mejorar en el análisis de la investigación con la finalidad de esclarecer el acto delictivo.

Nacionales

De la Cruz (2017) en su tesis "Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la policía nacional del Perú – Huaraz- 2015". Este proyecto de investigación explica el problema que tiene el departamento de investigación de la Policía Nacional de Huaraz al no contar con un área especializada de ingeniería forense, por lo cual se elaboró una investigación que explica el uso de las técnicas,

herramientas y metodologías que se aplicarían en los crímenes cibernéticos. Esta tesis tiene relación con nuestra propuesta debido a que en la actualidad en la ciudad de Chiclayo no se cuenta con un área de investigación forense ni estándares de procesos definidos para los procesos de los delitos informáticos. Esta información nos sirve como guía para elaborar y explicar el desarrollo de una metodología, con el uso de diferentes herramientas, que serán de gran utilidad en los casos de delitos informáticos.

Cacha Arana (2019) en su tesis "Peritaje Informático basado en una nueva metodología híbrida en 2M % J Ingenieros – Huaraz". Este proyecto explica la falta de una metodología estandarizada en la empresa 2M & INGENIEROS, lo cual permitirá resolver los problemas de peritaje informático. Su objetivo principal es lograr estandarizar una metodología la cual pueda aplicarse todos en los procesos de investigación sobre peritaje informático. La relación que tiene con nuestro proyecto es que busca crear una guía de procedimientos para los procesos de investigación en la recopilación de datos y presentación de resultados.

Regional

Ramírez (2008) en su tesis, "Sistema informático basado en algoritmos evolutivos para mejorar el proceso de identificación forense de evidencias digitales". Este proyecto explica la falta de la tecnología existente para la automatización de los procesos de identificación de evidencias en la informática forense, para ello se tiene como objetivo realizar un sistema que permita identificar la evidencia y así agilizar los tiempos de búsqueda y respuesta de cada proceso. Este proyecto nos brinda la información necesaria para posteriormente lograr su automatización para que los procesos sean de manera más rápida y concisa.

1.6. Base Teórica

1.6.1. Conceptos Generales

1.6.1.1. Seguridad Informática

La seguridad informática se define como una disciplina encargada de establecer las diferentes normas y políticas de una empresa con la finalidad de proteger la información de los diferentes sistemas que se puedan manejar a través de un conjunto de medidas de seguridad conformado por programas, antivirus, software y otras adicionales. (Gómez Vieites, 2017).

- *Áreas de la seguridad informática*

Velázquez López & Díaz Aguado (2015) divide al área de la seguridad informática en:

- Confidencialidad: La información solo puede ser adquirida por los usuarios autorizados.
- Integridad: Cualquier modificación de la información debe ser permitida solo por los usuarios autorizados.
- Disponibilidad: Los usuarios deben tener disponible la información cuando lo necesiten.
- Autenticación**:** Todo usuario se debe identificar para acceder a la información.

- *Clasificación de la Seguridad Informática*

Según los autores Romero Castro y otros (2018), clasifican a la seguridad informática en:

- Usuarios: Son los más propensos en cometer errores y romper las reglas, realizando acciones las cuales pueden ocasionar pérdida de información por lo que es imposible controlar las acciones de las personas. Existen diferentes tipos de usuarios (hacker, cracker, phraker, entre otros). Por este motivo, toda la información debe estar protegido del mismo usuario.

- Información: Es el principal activo de la seguridad informática por lo que se debe proteger y mantener su integridad.
- Infraestructura: Es la parte esencial para el buen funcionamiento de la organización. Sin embargo, se debe tener en cuenta los diferentes problemas que se puedan presentar en los procesos que se manejan como el acceso no permitido, robo de información, robo de identidad como también robo de equipos o daños permanentes que estos puedan sufrir, los cuales afectarían de manera directa a la empresa.

- *Tipos de Seguridad Informática*

El autor Postigo Palacios (2020) señala los siguientes tipos de Seguridad Informática

- Seguridad de Red: Se encarga de priorizar la protección de la información que esta almacenada en la internet (bancas móviles, documentos en la nube, entre otros) para evitar robo de datos personales o información con el fin de mantener su integridad. Para ello se usan softwares las cuales se actualizan de manera constante para poder salvaguardar la información. Los instrumentos que se usan en este caso son antivirus, firewall o redes privadas.
- Seguridad de Software: Se encarga de proteger las aplicaciones, programas y al software de amenazas externas como ataques maliciosos, virus, etc. Estos problemas se deben por fallas en la implementación del software, errores en el diseño o por la falta de respuestas antes los problemas.

Para mantener la integridad de los datos es necesario utilizar diferentes programas o herramientas como los antivirus, firewall, filtros de contenido, entro otros.

- Seguridad de Hardware: Se encarga de proteger de manera física los equipos, ordenadores y dispositivos ante los posibles daños que puedan llegar a tener. Para garantizar su seguridad se utilizan firewalls, servidores proxy o incluso claves encriptadas con el fin de mantener la integridad de la información.

Podemos concluir que la seguridad informática tiene como función principal minimizar los riegos que alteren la integridad de la información ya sea por los mismos usuarios al momento de transmitir o recibir datos o por fallas en los protocolos que se han implementado.

Dentro de la seguridad informática tenemos:

1.6.1.1.1. Dato

Los datos son definidos como instrucciones las cuales son recibidas e interpretadas en código binario por el CPU (Unidad central de proceso) para luego ser convertido en recursos aprovechados por el usuario.

Un dato es un fragmento de información que no aporta significado por sí mismo, pues no tiene un contexto de interpretación. Los datos representan de manera empírica la realidad, pero no proporcionan un valor determinado para la verificación de la información, y por tanto no pueden guiarnos en la toma de decisiones o acciones. Los datos son representaciones simbólicas de un atributo o una característica de una entidad. (Cartín, pág. 3).

1.6.1.1.2. Información

El concepto de información no se ha definido solo desde el punto de vista técnico puesto que existen varios enfoques con respecto al estudio de la misma, el autor Chiavenato (2006) define a la información como: "Un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones".

- *Clasificación de la información.*

Según la Guía de almacenamiento de seguro de la información del Instituto Nacional de Ciberseguridad de España (Instituto Nacional de Ciberseguridad, 2016), clasifica la información en tres niveles: confidencial, de uso interno e información pública.

- Confidencial: Información privada de una organización cuyo acceso está permitido únicamente a los miembros que lo necesiten para desempeñar sus funciones.
- Interna: Información propia accesible para todos los involucrados dentro de la organización. Por ejemplo, la política de seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.
- Pública: Información disponible a todos los miembros de la organización sin ninguna restricción. Por ejemplo, información publicada en una página web.

o *Almacenamiento de la información.*

Teniendo una vez más como referencia al Instituto Nacional de Ciberseguridad (2016), el cual divide al almacenamiento de la información en:

- Almacenamiento local: Información almacenada de manera local en equipos personales, normalmente discos duros donde se guarda la información, como también lo utilizado en tabletas, dispositivos móviles o tarjetas de memoria (microSD). Por lo tanto, no requiere conectarse a una red para comunicarse.
- Almacenamiento en red: Información contenida en servidores de almacenamiento en red donde se alojan los datos en discos dedicados, esto permite almacenar, recuperar y realizar copias de seguridad de los datos, de modo que siempre se puedan acceder y compartir con todos los usuarios autorizados en la red. Este almacenamiento es expansible, lo que significa que puede añadirse más capacidad conforme se vaya requiriendo.

Además, cuenta con los beneficios como el de un almacenamiento en la nube, con un menor costo y mayor velocidad (Vásquez Moctezuma, 2015) .

- Dispositivos externos: Información almacenada en CD, DVD, pendrive, discos duros externos, entre otros, que están conectados directamente a los equipos a través de distintos interfaces físicos, obteniendo así un almacenamiento adicional de la información, evitando que se ocupe espacio en el equipo.

CD/DVD: Es un soporte digital óptico de almacenamiento utilizado para almacenar información en formato digital como videos (AVI, WMV/WMA, MOV, FL, MP4, etc), imágenes (JPG, PNG, GIF, PSD, etc). Documentos (TXT, PDF, ZIP, DOC, etc), entre otros. La diferencia entre estos dos dispositivos es la capacidad de almacenamiento, el CD almacena hasta 700MB y el DVD hasta 4.7GB (Oliva Haba, Martín Márquez, & Manjavacas Zarco, 2008).

USB: También conocido como pendrive, es un dispositivo de almacenamiento de memoria flash que puede almacenar cualquier información digital la cual puede borrarse y modificarse. La diferencia con otros dispositivos de almacenamiento externos como el DVD/CD es su resistencia a los daños físicos que puedan presentar como rayaduras, polvo, agua, etc. A lo largo del tiempo los USB han ido evolucionando desde su capacidad de almacenamiento (de 1GB a 512GB) hasta su velocidad de transferencia de archivos (Anderson, 1997).

Disco duro externo: Es un dispositivo de almacenamiento el cual permite intercambiar cualquier tipo de información digital entre ordenadores. La información almacenada en el disco duro externo puede ser fácil de transportar y compartir. También es utiliza para hacer respaldos de copias de seguridad (Herrerías Rey, 2012).

- Almacenamiento en la nube

Es un modelo de almacenamiento basado en redes de computadoras donde la información es alojada en servidores de almacenamiento en la nube como un medio externo, con el fin de archivar, organizar, compartir y distribuir la información o para realizar copias de seguridad (backup) en diferentes volúmenes.

Algunos ejemplos de servicios de almacenamiento:

- Box
- Dropbox

- OneDrive
- Google Drive
- Mega
- iCloud
- Amazon Web Service

Tipos de Almacenamiento en la nube

Según el autor Ruiz Larrocha (2017), los tipos de almacenamiento en la nube son:

Nube Pública: Este tipo de almacenamiento es la más usada por los usuarios ya que tiene pocos controles de seguridad y cualquier persona autorizada puede acceder a la información mediante un correo. Es de manera gratuita y tiene un costo no tan elevado. Entre los almacenamientos públicos más conocidos tenemos iCloud, Google Drive. Dropbox, etc.

En conclusión, el almacenamiento en nube pública es ideal para el uso personal u organizaciones pequeñas que están empezando a utilizar este servicio y no necesiten grandes volúmenes de almacenamiento.

Nube Privada: Este tipo de almacenamiento tiene mayor control de seguridad y capacidad de almacenamiento en comparación con la pública. Tiene un número limitado de usuarios que pueden acceder a la nube.

Este tipo de almacenamiento es usado por empresas grandes que necesitan mayor cantidad de almacenamiento y realizar copias de seguridad de manera personalizada, consultas, entre otros.

Nube Híbrida: Es una fusión entre nube pública y privada, lo que permite personalizar sus funciones. Es ideal para las empresas que desean reservar los datos importantes y a su vez volver pública los datos menos importantes.

Las empresas que utilizan Big Data necesitan este tipo de nube híbrida para guardar información sensible de la empresa y al mismo tiempo compartir alguna información útil en la nube pública.

- *Dispositivos de almacenamiento.*

El autor Rebollo (2011) en su informe "Dispositivos de Almacenamiento", divide a los dispositivos de almacenamiento en:

Dispositivos magnéticos: Son dispositivos auxiliares que se utilizan para almacenar o leer información cuyos materiales están compuestos por propiedades magnéticas. Podemos llamar dispositivos magnéticos en la actualidad al disco duro, USB, disquete, CD/DVD, entre otros.

Dispositivos ópticos: Son dispositivos que permiten la lectura y escritura de la información mediante rayos de luz que se refleja en el disco. La capacidad de los dispositivos cambia según la función de su tipo y el número de capas de datos que contengan. (Pérez Ríos & Rodríguez Cabrera)

- Libro rojo CD-DA (compact disc-digital audio): Es un disco compacto diseñado para almacenar audio.
- Libro amarillo CD-ROM: Disco compacto de sólo lectura que almacena información no volátil.
- Libro naranja CD-R y CD-RW: Discos compactos grabables y regrabables.
- Libro blanco VCD: Disco de vídeo, antecesor del DVD (incompatible).

Memorias de estado sólido: Es un dispositivo de almacenamiento que consta de una memoria flash, compuesto por componentes electrónicos en estado sólido, reemplazando así a los discos magnéticos de los discos duros. Algunos dispositivos de almacenamiento solido son:

- Compact Flash (CF)
- Secure Digital (SD)

- Memory Stick (MMC)
- Multimedia Card (MMC)

1.6.1.1.3. Análisis de Riesgo

Un proceso de gestión de riesgo determina con anticipación los posibles riesgos del sistema con la finalidad reducir su vulnerabilidad y protegerlo de cualquier amenaza, así como la recuperación de este. Es decir, trata de que el proceso cumpla con sus funciones de la manera óptima para el buen funcionamiento del sistema (Goméz, 2014).

Según Garrido Buj & Romero Cuadraro (2019), algunos factores que posibilitan una amenaza a la infraestructura informática son:

- El ambiente donde la empresa realiza sus actividades.
- Modificación en las políticas de seguridad de la empresa.
- Mal uso de la tecnología disponible.
- Personal poco calificado.

Para evitar los riesgos se debe tener en cuenta lo siguiente:

- Limitar el acceso de los usuarios a los programas y archivos según su autorización.
- Supervisar a los usuarios para que no alteren la integridad de los datos y los programas.
- Garantizar que la información enviada sea la misma que la reciba.
- Renovar constantemente las contraseñas.

El autor Areitio Bertolin (2008), menciona los elementos de análisis de riesgo:

- Detallar los recursos de la organización.
- Identificar las amenazas de los recursos de la organización.
- Identificar las fallas de la infraestructura informática.
- Evaluar los riesgos ante las amenazas.

- Implementar estrategias para reducir los riesgos que afecten a los recursos de la organización.

- *Amenazas.*

Se entiende por amenaza la presencia de uno o más elementos que tienen como propósito dañar la seguridad de la información, aprovechándose de su nivel de vulnerabilidad.

Para reducir el riesgo se debe tener en cuenta lo siguiente:

- Mantener a los usuarios informados en temas de ciberseguridad para identificar y evitar las nuevas amenazas.
- Realizar evaluaciones en el sistema cada cierto tiempo para protegerlo contra amenazas.
- Realizar pruebas para descubrir fallas en la infraestructura informática.

Aguilera López (2010) clasifica a las amenazas en 6 grupos:

De interrupción: Deshabilita el acceso a la información provocando la eliminación y el bloqueo de datos en los dispositivos físicos como el disco duro.

De interceptación: Acceso a información confidencial de una organización por parte de personas no autorizadas, causando filtración de datos, programas o identidades de personas.

De modificación: Personas, programas o equipos no autorizados que alteren los datos de un sistema de información.

De fabricación: Altera la integridad del sistema agregando información falsa al sistema.

Accidentales: Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

Intencionales: Introducción de software maliciosos, intrusión informática, robos o hurtos.

- Tipos de Amenazas

- Amenaza Interna

Las amenazas internas por lo general son más graves que las amenazas externas ya que pueden acceder a información privada de la organización. Esto se debe a ingresos no

autorizados a la red por usuarios que conocen la infraestructura informática y tienen la intención de perjudicar el sistema y dañar los datos de la organización (Ganivet Sánchez, 2017).

Amenaza Interna por Negligencia: Causado por usuarios que por error o descuido ponen en riesgo a la organización al manipular de manera negligente información confidencial de la empresa. Esto se puede deber al mal uso de los recursos informáticos o por la instalación de programas no autorizados sin tener conocimiento previo de su funcionalidad (Picu, 2020).

Amenaza Interna por Conveniencia: Causada por personas ajenas a la organización que cooperan con los usuarios que pertenecen a la empresa. Las amenazas más comunes son los fraudes, robo de información confidencial, alteración de datos, entre otros. Esta amenaza es poca común, pero puede causar muchos costos a la organización (Picu, 2020).

- Amenaza Externa

Troyano: Son programas maliciosos que se instalan en los ordenadores de la organización permitiendo el ingreso no autorizado de usuarios externos. Los troyanos pueden pasar inadvertidos por los usuarios, causando daño en el funcionamiento del sistema del ordenador. Su objetivo principal es ayudar a que otro software malicioso se pueda instalar en el ordenador (Aguilera López , 2010).

Virus: Software malicioso que se instala en un ordenador o viene acompañado en aplicaciones que al abrirse pueden dañar los archivos del sistema. Los virus también se pueden obtener al descargar archivos, intercambiar información por medio de dispositivos de almacenamiento (USB, discos) o a través de e-mail infectados (Aguilera López , 2010).

Gusano: Es similar al virus, un gusano es un malware común que no necesita de terceros para infectar los ordenadores y al sistema dentro de una organización. El objetivo de este malware es conectarse a través de la red para poder infectar a todos los dispositivos conectados (Aguilera López , 2010)

Spam: Es todo e-mail que se envía de manera simultánea. Es una de las amenazas más comunes en el mercado, muchos usuarios se ven afectados al brindar su información en enlaces que contienen falsos formularios (Marco Galindo & Marco Simó, 2010).

Phishing: Es un malware fácil de ejecutar por los ciber delincuentes. Se encarga de robar información personal de los usuarios a través de correos electrónicos falsos usando el nombre de compañías legales solicitando datos como, contraseñas, tarjetas de créditos, número de cuenta bancarias, entre otros (Postigo Palacios, 2020).

- *Riesgos.*

Se denominan riesgo a la probabilidad de que se detecte o no una amenaza en el sistema aprovechando una falla o vulnerabilidad y determinar cuál es el impacto que tendrá en el sistema.

Ante un determinado riesgo en una organización, Aguilera López (2010) opta por tres alternativas distintas:

- Asumirlo sin hacer nada.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (contratar un seguro).

Según Chicano Tejada (2015), los riesgos se clasifican en tres niveles:

Nivel bajo: No se considera una amenaza importante para la organización, aunque se deben de inspeccionar para que no pase a mayores.

Nivel medio: Se considera de riesgo medio cuando la amenaza afecta de forma relativa a la empresa. Es necesario tomar medidas para minimizar el riesgo.

Nivel alto: Se denomina de riesgo alto cuando la organización se ve afectada de manera considerada. Es necesario tomar acciones inmediatas.

- Tipos de Riesgo

Corda, Viñas, & Coria, señala los siguientes tipos de riesgos:

Riesgo de integridad: Este tipo de riesgo está relacionado con las autorizaciones, procesamientos y reportes de los programas utilizados en las empresas. Están presente en múltiples aspectos del sistema, por tal motivo las organizaciones buscan tecnologías las cuales puedan tener integración tanto de hardware y software para poder minimizar los riesgos. Estos riesgos se presentan en: interfaz de usuario, procesamiento de errores, gestión de cambios.

Riesgo de relación: Los riesgos de relación se originan por el uso conveniente de la información en toma de decisiones (datos de personas o del sistema) proveniente de una aplicación.

Riesgo de acceso: Este riesgo se refiere a los accesos no autorizados al sistema que intentan adquirir datos e información confidencial de las organizaciones.

Riesgo de utilidad: Este tipo de riesgo se presenta 3 niveles:

- Puede afectar el funcionamiento del sistema antes que presenten inconvenientes.
- Riesgos en las técnicas usadas para restaurar los sistemas dañados.
- Riesgos en los backup usados tras la pérdida de información.

Riesgo de infraestructura: Este tipo de riesgo está relacionado con la falta de una infraestructura tecnológica y procesamiento de información (usuarios, interfaces) adecuadas que se puedan adaptar a los futuros cambios y necesidades de la empresa.

- *Vulnerabilidades*

Una vulnerabilidad es un defecto del sistema que puede ser aprovechado por un ataque cibernético causando la perdida de información y daño a la integridad del sistema. Estas vulnerabilidades pueden estar ligadas a aspectos organizativos (falta de procesos que no fueron definidos previamente), como también el factor humano, incluyendo los equipos, programas y herramientas lógicas del sistema. Para definir el nivel de vulnerabilidad de un

determinado equipo o recurso, se emplea una escala cuantitativa o cualitativa: Bajo, Media y Alta. (Goméz, 2014)

- Tipos de Vulnerabilidad

Según Cebrián Marín (2015), las vulnerabilidades se pueden dividir en:

Vulnerabilidad de desbordamiento de buffer: Se produce cuando una cantidad de datos supera la capacidad de almacenamiento de la memoria, ocasionando que los datos se reescriban y borren su contenido inicial.

Vulnerabilidad de race condition: Se produce cuando un recurso compartido es accedido por varios procesos al mismo tiempo.

Vulnerabilidad de format string bugs: Conocido en español como errores de cadena de formato. El principal problema de esta vulnerabilidad es no tener un control de los datos ingresados que se origina por fallas, errores o despistes en la programación de las aplicaciones ocasionando que la información se filtre y facilite el robo de los datos.

Vulnerabilidad de XSS: Se produce cuando se ejecutan ataques de scripts como VBScript o JavaScript en sitios web. El objetivo de esta vulnerabilidad es robar información personal (pishing).

Vulnerabilidad de denegación de servicio: Se produce cuando los usuarios no pueden acceder a un recurso de la organización ocasionando perdida de conectividad en la red.

Vulnerabilidad de ventanas engañosas: Es popular entre los usuarios. Se produce cuando aparecen ventanas engañosas afirmando que ganaste premios o sorteos con el fin de que le brindes información personal.

1.6.1.2. Informática Forense

Se define a la informática forense como la ciencia que se encarga del proceso para identificar, adquirir, analizar y presentar datos con el objetivo de garantizar la información y reconstruir las evidencias digitales.

Los objetivos de la Informática Forense son técnicas que permiten localizar, reproducir y analizar evidencias digitales con fines legales.

López, Amaya, & León (2001) divide a la informática forense en 3 objetivos a saber:

- La compensación de los daños causados por los criminales o intrusos.
- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

Colmenares & Cruz (2003) definen varios conceptos de la informática forense:

- *Computación Forense*

Gutiérrez (citado en Colmenares & Cruz, 2003) menciona que la computación forense es: La aplicación de medidas para prevenir delitos informáticos a través de técnicas científicas y analíticas, para identificar, preservar, analizar y presentar evidencia que sea aceptable en un procedimiento legal. Pretende descubrir e interpretar la información para aclarar los hechos y formular las teorías relacionadas con el caso.

- *Forensia en redes.*

Camona (citado en Colmenares & Cruz, 2003) menciona que la forensia en redes se dedica a enlazar los eventos de la red, a través de los procesos para capturar, registrar, almacenar y analizar los datos con la finalidad de dar con la fuente de los ataques a la red.

- Tipos de Informática Forense

Los autores Triana Fuentes & Ballesteros Ricaurte definen los tipos de informática Forense en:

<u>De sistemas operativos:</u> Tiene como objetivo reunir información y evidencia de los sistemas operativos de los ordenadores o dispositivos móviles que sirva para las investigaciones.

De redes: Se realiza un análisis informático cuando se ejecutan ataques a la red. Tiene como finalidad recuperar, supervisar y analizar la red para descubrir amenazas contra la seguridad, reuniendo pruebas para determinar la fuente de ataque.

De dispositivos móviles: Tiene como objetivo recuperar evidencia de los dispositivos móviles a través de la recopilación de datos y evidencias digitales. Para ello se debe seguir una serie de normas que permitan extraer, almacenar y conservar las pruebas de los dispositivos móviles.

De nube o cloud: En la actualidad la información confidencial de las empresas es diferido a proveedores en la nube, con la finalidad de tener mayor seguridad. Sin embargo, esto tiene algunas desventajas como el hecho de tener que confiar en el proveedor para que entregue la información almacenada para que sirva como evidencia en las investigaciones si ocurre algún ataque cibernético.

1.6.1.2.1. Programas utilizados en la informática forense

- *Para USB*

Check Flash

Es un software portable que permite comprobar el estado de la unidad flash USB. Cuando se ejecuta esta aplicación, reconoce automáticamente cualquier dispositivo de este tipo. Permite editar la información del USB, guardar y restaurar imágenes completas de la unidad como también formatearlas. (Cherkes, 2017)

Disk Drill:

Es un programa que nos permite recuperar cualquier tipo de archivo oculto como documentos, mensajes y archivos multimedia de Office de forma rápida y sencilla de un disco duro, USB o cualquier tipo de medio de almacenamiento. (Cleverfiles, 2021)

Stellar Data Recovery:

(Stellar, 2021) Es un software que nos permite recuperar cualquier tipo de archivo que haya sido perdido o eliminado en nuestra PC o en dispositivos de almacenamientos.

- *Para CD/DVD*

CDReader

Es un programa portable que permite verificar y comprobar el estado de los CD/DVD. Al finalizar el análisis del programa nos muestra la cantidad de archivos y carpetas que contiene el disco, como también la ruta de los archivos ilegibles. (Softpedia, 2015)

Recovery Toolbox for CD

(Recovery Toolbox Inc., 2003) Es un programa que nos permite recuperar la mayor cantidad posible de información almacenada en CD, DVD o Blu-ray que estén dañados físicamente por arañazos, polvo o por una mala grabación.

- *Para desencriptar archivos RAR*

Passware Kit Forensic:

Es un programa que permite descifrar todos los elementos que contengan contraseña. Este programa admite más de 300 tipos de archivos y funciona en modo por lotes recuperando contraseñas (Passware, 1998).

1.6.1.3. Delitos Informáticos

Los Delitos informáticos son también llamados delitos cibernéticos. Cinta Castillo & Ramallo (citado en Acurio, 2016) explica que: son todas aquellas acciones ilegales que provocan daños y perjuicios a través de los dispositivos electrónicos para obtener beneficios materiales que perjudiquen de manera directa o indirecta a las personas o entidades mediante la alteración o eliminación de datos. Sin embargo, la definición más simple de delito informático es que tiene como fin causar daño a través de cualquier sistema informático y de esta manera se abarquen todas las modalidades delictivas de acuerdo con el marco legal de cada país.

- *Tipos de delitos informáticos.*

Existen diferentes tipos de delitos informáticos, el autor Camacho Losa (citado en Acurio, 2016) menciona que, la única limitación para cometer delitos informáticos se base en tres factores principales:

La creatividad del usuario, su capacidad técnica para el manejo de sistemas informáticos y las vulnerabilidades existentes de las infraestructuras informáticas.

Algunos de los diferentes delitos informáticos son: Los fraudes, extorsión, sabotaje o espionaje informático, robo de software y el acceso no autorizado a servicios informáticos. (Acurio, 2016)

1.6.1.4. Evidencias Digitales

La evidencia digital es todo aquel registro informático que se almacena en dispositivos digitales y se transfieren a través de redes informáticas. Estas evidencias tienen una gran importancia y pueden ser utilizadas en un proceso jurídico. Se considera como evidencia digital a toda información que haya sido manipulada por medio de un usuario o a través de un sistema informático. Otro concepto citado por el autor Martín (2017) nos dice que la evidencia digital:

> *"Técnicamente, es un tipo de evidencia física que está constituida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas técnicas especiales"*

- *Importancia de la Evidencia Digital.*

La importancia de la evidencia digital reside en la necesidad de proporcionar y dar a conocer las pruebas de los delitos informáticos que convierte al sospechoso en responsable.

La correcta manipulación de la evidencia digital es necesaria para poder realizar todos los procesos de obtención, preservación, análisis y presentación, cuyos pasos dependerán del manual de buenas prácticas. (Martín, 2017)

- *Principios de la Evidencia Digital*

Según López Urrea (2017), los describe de la siguiente manera:

Objetividad: La recolección y extracción de la evidencia debe ser objetiva, cumpliendo con todas las normas profesionales.

Autenticidad: Se debe mantener la integridad de la evidencia digital durante todo el proceso de investigación.

Legítima: El personal a cargo del proceso de investigación debe ser conciso en los detalles obtenidos de la evidencia digital, cumpliendo con las fases establecidas por ley.

Idoneidad: Todos los programas tienen que ser eficaces y apropiados durante el desarrollo de los casos.

Inalterabilidad: En todo el proceso de investigación se debe tener pruebas que demuestre que no hubo alteración de la evidencia recolectada.

Documentación: Se debe documentar por escrito cada etapa de la investigación.

- *Característica de la Evidencia Digital.*

Martín (2017) define las siguientes características:

Volátil: Evidencia de naturaleza inestable que si no es preservada adecuadamente puede cambiar o variar con facilidad de forma poco previsible.

Duplicable: Puede ser duplicada de manera exacta y copiada tal como si fuese el original.

Alterable y modificable: Con los programas adecuados es fácil de destruir, alterar o modificar.

Eliminable: Con los programas adecuados la evidencia puede ser eliminada por completo.

- *Fuentes de la Evidencia Digital.*

Dentro de la escena del crimen podemos establecer las fuentes de la evidencia digital a un sin número de componentes cibernéticos, Salas (2016) comprende lo siguiente:

Dispositivos de almacenamiento: Discos duros, flash drive, tarjetas móviles de almacenamiento o cualquier otro dispositivo que guarde información.

Dispositivos electrónicos de procesamiento de información: Juegos electrónicos, tabletas, cámaras digitales, teléfonos celulares, GPS y demás dispositivos que procesen información.

Comunicación de datos: Dispositivos de redes, servidores, base de datos, correo electrónico local, nubes con (sistemas de almacenamiento, sistemas virtualizados, servicios web y más) y demás servicios de transferencia y almacenamiento de información.

Internet: Páginas web, redes sociales, y demás sitios privados o públicos que presenten información vinculada en una investigación.

- *Aseguramiento De La Evidencia Digital.*

En el informe "Fundamentos aplicables para el abordaje de la Examinación Forense" Ortiz (2019), menciona los siguientes pasos para el aseguramiento de la evidencia digital:

- Antes de tener contacto con el lugar utilice pulsera antiestática y guantes.
- Si el ordenador está apagado, no lo encienda.
- Si el equipo está encendido, fotografíe la pantalla.
- Recopilar datos en vivo.
- Diagramar y etiquete todos los cables.
- Documentar todos los números de modelo de dispositivo y números de serie.
- Desconectar todos los cables y dispositivos.
- Empaquetar todos los componentes (usando bolsas de pruebas antiestáticas).
- Aprovechar todos los medios de almacenamiento adicional.
- Mantener todos los medios de comunicación fuera de los imanes, transmisores de radio y otros elementos potencialmente dañinos.
- Recoger instrucciones, manuales, documentación y notas.

- Documentar todos los pasos utilizados en la recolección de datos volátiles y aseguramiento de los dispositivos de almacenamiento.

1.6.2. Metodología por Aplicar

Diferentes organizaciones o instituciones han publicado sus metodologías según el tipo de investigación que deseen realizar, siendo algunos procesos mejor que otros. Desde el punto de vista del grupo encargado del hecho delictivo y del accionar de las Fuerzas de Seguridad de la DIVINCRI de Chiclayo, se puede establecer una metodología aplicable a la informática forense.

- *Identificación.*

En esta primera fase se identifica los equipos y dispositivos de almacenamiento en los cuales se obtiene y examina la evidencia cuyo resultado será útil para la investigación penal.

Es decir, esta etapa se encarga de planificar las fases de recolección y/o adquisición para garantizar que la evidencia digital sea confiable y legalmente válida. (Martín, 2017)

- *Adquisición.*

Después de la fase de identificación, se procederá a recolectar la información necesaria eligiendo los dispositivos adecuados que almacenará la evidencia digital para posteriormente ser enviados al área especializada donde se realizará su análisis correspondiente.

Al recolectar la evidencia, se debe emplear las técnicas adecuadas que estén dentro de los requerimientos establecidos, registrando y documentando cada paso realizado en el acto. Con esto aseguramos que la evidencia obtenida mantendrá su integridad y será de utilidad en los procesos correspondientes. (Martín, 2017)

- *Preservación.*

Este paso incluye revisar y preservar la evidencia digital para posteriormente efectuar su respectivo análisis. Al realizar una duplicidad es necesario tener las herramientas que

garanticen la integridad y periodo de validez. Es decir, nos referimos al proceso que se requiere para generar una copia de seguridad de toda la información obtenida. (Ferro, 2020)

- *Análisis.*

Al analizar metódicamente la evidencia, se interpretan los datos y se interrelacionan adecuadamente con la finalidad de explicar los hechos y su distribución temporal. Es la fase más larga de todo el proceso, y está vinculada con el hecho que se está investigando. (Ferro, 2020)

- *Presentación.*

Es el paso final de todo el proceso, ya que ofrece y muestra información de datos y resultados de la investigación. Se utiliza generalmente para expresar los resultados de la investigación. Es informar por escrito de una forma exacta, comprensible, clara, y completa, todos los pasos realizados en los hallazgos, análisis, interpretación y la conclusión que de ellos se derivan. (Rodríguez & Dómenech).

Capitulo II: Métodos y Materiales

2.1. Diseño de contrastación de Hipótesis

El diseño de contrastación de hipótesis para este proyecto es de tipo de investigación aplicada, por lo cual se tiene en cuenta las diferentes técnicas, herramientas y metodologías para un mejor proceso en la recuperación de datos y reconocimiento de las evidencias digitales.

2.2. Población y Muestra

2.2.1. Población

Para el desarrollo de este proyecto se considera a la población comprendida por el personal involucrado en las diferentes áreas de investigación de la División de Investigación Criminal (DIVINCRI) y DIRINCRI en todo el Perú.

La Tabla 2 presenta la población referencial en el proyecto de investigación.

Tabla 2: Población

Departamento	Cantidad	
	DIVINCRI	DIRINCRI
Amazonas	1	0
Ancash	1	0
Arequipa	1	0
Ayacucho	1	0
Cajamarca	1	0
Callao	1	0
Cusco	1	0
Huancavelica	1	0
Huánuco	1	0
Ica	1	0
Junín	1	0
La Libertad	1	0
Lima	11	10
Loreto	1	0
Madre de Dios	1	0
Moquegua	1	0
Pasco	1	0
Piura	1	0
Puno	1	0
San Martín	1	0
Tacna	1	0
Tumbes	1	0
Ucayali	1	0

Fuente: Elaboración Propia

2.2.2 Muestra

Para lograr obtener información adicional y que el desarrollo de la investigación sea de forma adecuada, se consultó con los diferentes encargados de cada área de la DIVINCRI de Chiclayo, los cuales varían según su rango de: comandantes, tenientes, alférez/técnicos y suboficiales, teniendo como fuente principal al técnico Santa Cruz del Departamento de investigación criminal de la DIVINCRI de Chiclayo.

2.3. Técnicas, instrumentos, equipo y Materiales

La Tabla 3, presenta los recursos usados para el desarrollo de la investigación

Tabla 3: Técnicas, instrumentos, equipo y materiales

TÉCNICA	INSTRUMENTO	EQUIPOS Y MATERIALES
Revisión bibliográfica	fichas bibliográficas	Documentos
Entrevistas	Cuestionario	Papel
Análisis Documental	Análisis de contenidos	Revisas y Libros

Fuente: Elaboración Propia

2.4. Metodología

2.4.1. Comparación de Metodología

En la informática forense existen varios tipos de metodologías para los procesos de investigación en los delitos informáticos.

Para el desarrollo de nuestra investigación, hemos optado por realizar un cuadro informativo de las siguientes metodologías: SANS, Kevin Madia y Chris Prosise, DFRW y PURI.

La Tabla 4, presenta los valores que se asignarán a cada metodología según sea conveniente para el desarrollo del proyecto

Tabla 4 : Valores para comparar metodologías

Lectura del cuadro comparativo	
3	Representa un alto grado de cumplimiento del criterio
2	Representa que el criterio se cumple parcialmente
1	Significa que el criterio no se satisface lo suficiente

Fuente: Elaboración Propia , muestra los criterios de la metodología que hemos tomado en cuenta para el desarrollo de la investigación

Tabla 5 : Metodología PURI

Fuente: Elaboración Propia

La **¡Error! No se encuentra el origen de la referencia.** nos presenta las ventajas y desventajas de las diferentes posibles metodologías que se pudieron usar en la investigación.

Tabla 6: Cuadro comparativo de Metodologías

METODOLOGÍA	VENTAJAS	DESVENTAJAS
SANS	- Engloba todas las fases para realizar una investigación forense. - Tiene en consideración el cuidado a la cadena de custodia.	- No brinda procedimientos para la adquisición de grandes volúmenes de datos. - No brinda procedimientos de análisis para grandes volúmenes de datos. - Es específica para ordenadores con sistemas operativos Windows o Linux. No aplica a dispositivos móviles.
Kevin Madia y Chris Prosise	- Engloba todas las fases para realizar una investigación forense. - Proporciona métodos para realizar el análisis de datos.	- No brinda procedimientos para la adquisición de grandes volúmenes de datos. - Enfocada a plataformas Windows NT/2000, UNIX y routers Cisco. No utiliza otra plataforma diferente, dejando de lado cualquier otro dispositivo digital.
DFRW	- Engloba todas las fases para realizar una investigación forense. - Plantea formas de análisis en una investigación de cómputo forense para todos los dispositivos.	- No cuenta con un procedimiento para realizar las actividades.

	- Se centra en conservar la integridad de la cadena de custodia. - Ofrece técnicas y métodos para la extracción de datos ocultos y análisis de grandes volúmenes de información. - Es una metodología que está en constante actualización.	

Fuente: Elaboración propia

Según las metodologías explicadas, podemos concluir que la metodología PURI (Proceso Unificado de Recuperación de Información) es la más adecuada para el desarrollo de esta investigación, debido a que nos brinda los pasos para el desarrollo de los procesos de investigación en un hecho delictivo: Identificación, Adquisición, Preservación, Análisis y Presentación.

La Tabla 7, nos muestra la calificación según los criterios mostrados en la Tabla 4.

Tabla 6: Criterio de selección de Metodologías

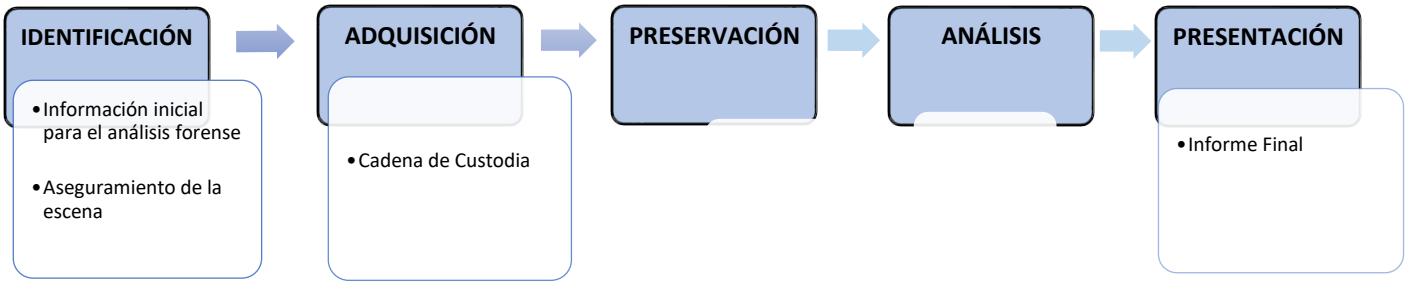
CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE LAS METODOLOGÍAS				
CRITERIOS	**PURI**	**SANS**	**Kevin Madia y Chris Prosise**	**DFRW**
Proporciona una guía para el proceso	3	1	2	1
Metodología compuesta de todas las etapas de investigación	3	3	3	3
Es una metodología conocida y más utilizada	2	1	1	1
Fácil acceso para el equipo de trabajo	3	2	2	2
TOTAL	**11**	**7**	8	**7**

Fuente: Elaboración propia

2.4.2. Metodología PURI

Fases de la Metodología PURI

Ilustración 1 : Fases de la metodología PURI



Fuente: Elaboración propia

- *FASE I*

  - IDENTIFICACIÓN PARA DATOS

Es el primer paso de la Metodología PURI, en esta etapa los investigadores forenses pueden identificar los dispositivos que serán la fuente de información para empezar la investigación. Existen varios tipos de fuente de información, tanto en dispositivos físicos: computadores, servidores, dispositivos de almacenamiento (USB, disco duro, DC/DVD), celulares, tablets, switchers, routers, etc; como en dispositivos lógicos: memoria RAM, memoria cache, aplicaciones, software.

La fase de identificación comprende 2 etapas:

<u>Información inicial para el Análisis Forense</u>

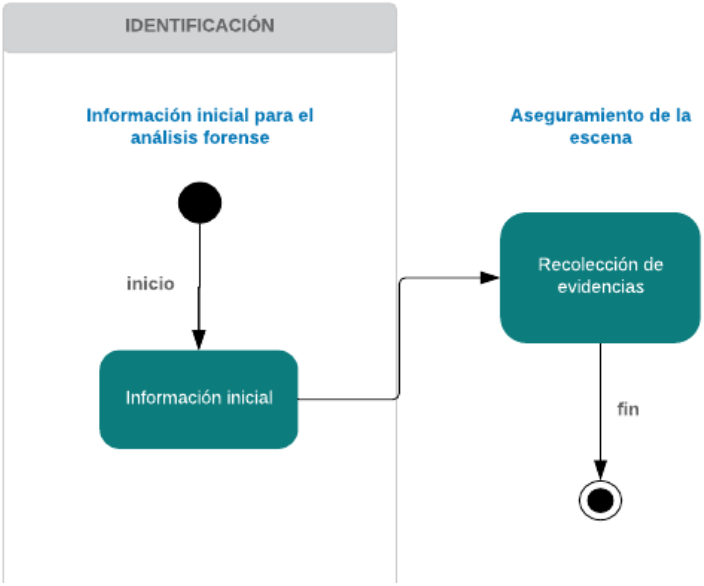
Es una ficha técnica donde el personal de turno del área de investigación de delitos informáticos notifica a los investigadores la ejecución de un incidente, la cual incluye información necesaria para iniciar una investigación (Anexo 1 – **FORM N° 001**).

<u>Aseguramiento de la escena</u>

En esta etapa los investigadores capacitados a través de las diferentes herramientas y equipos adecuados identificarán y recolectarán toda la evidencia encontrada en la escena del

crimen, detallando y seleccionando los dispositivos para la obtención de información. (Anexo II - **FORM N° 00 2**)

Ilustración 2: Fase de Identificación



Fuente: Elaboración propia

- IDENTIFICACIÓN PARA EVIDENCIAS

En esta etapa se identificará los dispositivos que serían la fuente de información, empleando el mismo método que se utiliza en la "Identificación de datos" (Anexo I - **FORM N° 00 1** y II - **FORM N° 00 2**).

El siguiente paso es la recuperación de información, en el cual se utiliza diferentes programas y herramientas (Anexo III - **FORM N° 00 5**).

- *FASE II: Adquisición*

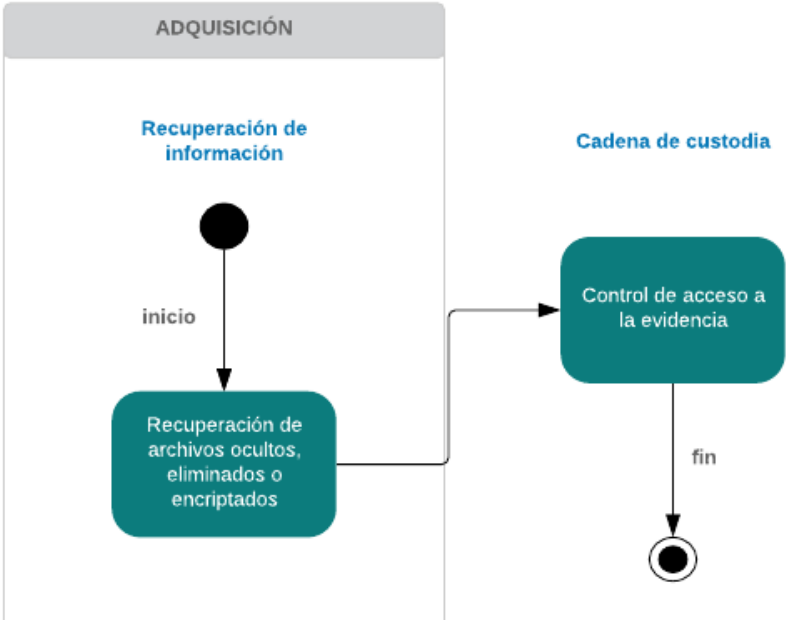
Después de identificar y seleccionar la evidencia, se dispondrá a adquirir toda la información posible empleando diferentes técnicas y programas que estén dentro de los requerimientos establecidos, registrando y documentando cada paso realizado en el acto. (Anexo IV - **FORM N° 00 3**)

La fase de adquisición comprende 1 etapa:

Cadena de Custodia

Es una etapa importante en la fase de adquisición ya que se debe tener un control de los responsables que han tenido acceso a la evidencia obtenida, registrando en un documento los datos de las personas implicadas en la manipulación de la evidencia. (Anexo V - **FORM N° 00 4**)

Ilustración 3: Adquisición



Fuente: Elaboración propia

- *Fase III: Preservación*

La fase de preservación consiste en salvaguardar y preservar la evidencia, tanto física como digital, para que de esta manera no se vea afectada su integridad y posteriormente se realice su respectivo análisis.

Para preservar la evidencia, solo el personal forense debe tener acceso a esta, realizando copias de seguridad de la información extraída de los dispositivos utilizando herramientas que garanticen la integridad de la información.

Se debe tener en cuenta quién está manipulando la evidencia en todo momento, documentando cada movimiento que pruebe y responsabilice lo mencionado. (Anexo VI - **FORM N° 00 6**)

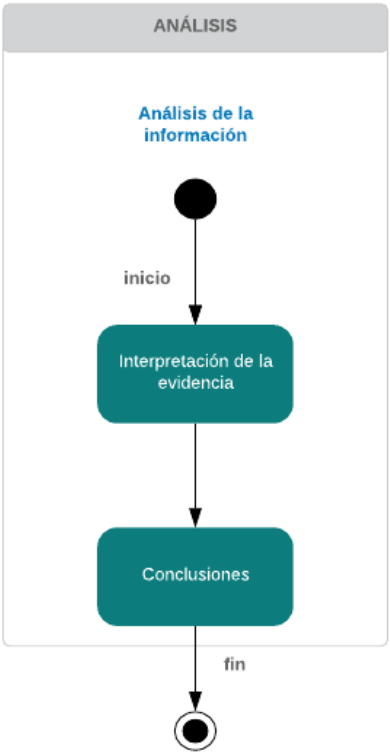
Ilustración 4: Preservación

Fuente: Elaboración propia

- *Fase IV: Análisis*

Esta etapa incluye el análisis de la información obtenida de los dispositivos incautados en la fase 1 con el propósito de reconstruir todos los acontecimientos que tuvieron lugar en el incidente, interpretando la evidencia obtenida para poder obtener conclusiones y facilitar en la toma de decisiones (Anexo VII - **FORM N°007**.

Ilustración 5: Análisis



Fuente: Elaboración propia

- *Fase V: Presentación*

Es la fase final de la metodología PURI donde se realiza el informe con los resultados de los análisis. En esta fase, el investigador forense deberá documentar detalladamente todos los procesos realizados utilizando una explicación no técnica, es decir, en lenguaje común, describiendo la metodología, programas y herramientas utilizadas en el desarrollo del caso incluyendo la información extraída de los dispositivos. (Anexo VIII - **FORM N°008**)

Este informe tiene que contener:

N° de Expediente:

1. Precedente

    a) Descripción del incidente

    b) Objetivo

2. Tareas Realizadas

   a) Descripción de la evidencia

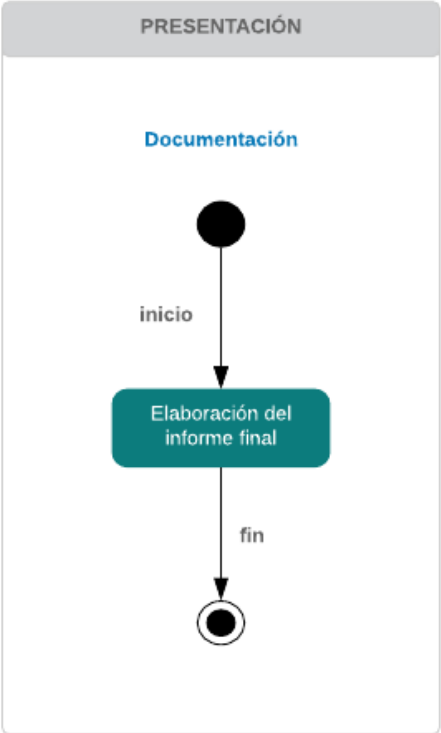
   b) Descripción de las herramientas utilizadas

   c) Descripción de la información obtenida

3. Resultado Final

4. Anexos

Ilustración 6: Presentación



Fuente: Elaboración propia

Capítulo III: Resultados y Discusión

3.1. Resultado

3.1.1. Elaboración de una Guía de procesos para la informática forense

Con la elaboración de la guía procesos explicada en el capítulo II: Métodos y Materiales, basándonos en diferentes conceptos de metodologías y realizando un cuadro comparativo explicando sus ventajas y desventajas, logramos calificar los criterios propuestos de selección de metodología, obteniendo como resultado la selección de la metodología PURI para el desarrollo de nuestro proyecto de investigación, debido a que es una metodología conocida y la más utilizada, la cual cuenta con información actualizada de los pasos para la recuperación de datos y evidencias digitales, como también una estructura propia del modelo.

3.1.2. Estudio de las herramientas existentes para la recuperación de datos y evidencias digitales

Para el desarrollo de los casos de delitos informáticos, se optó por el uso de diferentes programas que permitan recuperar información eliminada, oculta o encriptada, como también de verificación de integridad del dispositivo.

Para una selección correcta de los programas, hemos realizado un cuadro comparativo con las diferentes características que cuentan los programas, el cual se muestra a continuación:

Tabla 7: Programa para verificar estado de la unidad flash

PROGRAMAS PARA VERIFICAR ESTADO DE UNIDAD FLASH USB		
PROGRAMAS	**VENTAJAS**	**DESVENTAJAS**
Check Flash	Analiza discos duros portables y memorias USB Busca errores por sectores en memorias USB o discos duros portables Mide velocidades de lectura y grabación Ofrece varios tipos de análisis de longitud de prueba Es portable y gratuita	No corrige los errores detectados Falta de documentación Mala organización de la interfaz
H2testw	Analiza discos duros portables y memorias USB Busca errores por sectores en memorias USB o discos duros portables Es portable y gratuita	La información se pierde cuando se detecta un error Se necesita realizar una copia de seguridad antes de analizar
USB Flash Drive Tester	Detecta sectores dañados o inestables. Prueba los tamaños falsos en USB de baja calidad Guarda el informe de exploración en un archivo de texto Ofrece varios tipos de pruebas de análisis Es gratuita	El tiempo de análisis es superior a los programas anteriores
USB Memory Stick Tester	Analiza medios de almacenamiento extraíbles USB Permite localizar problemas en el USB Es gratuita y portable	El programa está descontinuado Se necesita realizar una copia de seguridad antes de analizar todo el dispositivo Mala organización de la interfaz

Fuente: Elaboración propia

Tabla 8:Criterios de selección de los programas para análisis de USB

CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE PROGRAMA PARA ANALIZAR ESTADO DE USB				
CRITERIOS	Check Flash	H2testw	USB Flash Drive Tester	USB Memory Stick Tester
Facilidad de uso de interfaz	3	3	3	3
Accesibilidad económica	3	3	3	3
Adaptación al desarrollo del caso	3	2	2	1
Software conocido y utilizado	3	2	2	2
TOTAL	12	10	10	9

Fuente: Elaboración propia

Comparando las características de los programas y teniendo en cuenta el cuadro de criterio, se optó por escoger el programa Check Flash, debido a que es el que mejor se adecua a las necesidades del caso propuesto en nuestro proyecto.

Tabla 9: Programas para desencriptar archivos

PROGRAMAS PARA DESENCRIPTAR ARCHIVOS RAR		
PROGRAMAS	**VENTAJAS**	**DESVENTAJAS**
PassFab for RAR	Contiene un algoritmo de recuperación avanzada de contraseñas Ofrece diferentes modos de desencriptación de contraseñas Velocidad de recuperación moderada Requisitos mínimos del sistema	Tasa de éxito no tan eficiente Precio elevado No está disponible en español
Free Rar Password Recovery	Ofrece diferentes modos de desencriptación de contraseñas Velocidad de recuperación moderada Compatibilidad con ficheros ZIC y ACE	Tasa de éxito no tan eficiente Precio muy elevado No está disponible en español

	Puedes cambiar la contraseña de acceso en el mismo momento que se descifra la contraseña Extrae documentos alojados en su interior para abrirlos con otros programas Permite recuperar contraseñas de archivos RAR utilizando fuerza bruta	
RAR Password Recovery Professional	Velocidad de acción rápida (3000 contraseñas por segundo)	No recupera las contraseñas que se componen de más de 3 caracteres
	Ofrece diferentes opciones de configuración para la recuperación de contraseñas Guardado automático del proceso de recuperación	No está disponible en español
	Permite la recuperación de contraseñas para más de 300 tipos de archivos	Precio elevado
Passware Kit Forensic	Velocidad de recuperación acelerada dependiendo del computador Ofrece diferentes modos de desencriptación de contraseñas. Cuenta con una versión empresarial para desencriptar bases de datos y otras aplicaciones.	No está disponible en español

Fuente: Elaboración propia

Tabla 10: Criterios de selección de los programas para desencriptar archivos RAR

CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE PROGRAMA PARA DESENCRIPTAR ARCHIVOS RAR				
CRITERIOS	PassFab for RAR	Free Rar Password Recovery	RAR Password Recovery Professional	Passware Kit Forensic
Facilidad de uso de interfaz	3	3	3	3
Accesibilidad económica	1	1	1	2
Adaptación al desarrollo del caso	2	2	2	3
Software conocido y utilizado	3	2	2	3
TOTAL	9	8	8	11

Fuente: Elaboración propia

Comparando las características de los programas y teniendo en cuenta el cuadro de criterio, se optó por escoger el programa Passware Kit Forensic, debido a que es el que mejor se adecua a las necesidades del caso propuesto en nuestro proyecto y su precio es accesible.

Tabla 11: Programas para recuperar archivos eliminados del USB

PROGRAMAS PARA RECUPERAR ARCHIVOS ELIMINADOS DEL USB		
PROGRAMAS	**VENTAJAS**	**DESVENTAJAS**
EaseUS Data Recovery Wizard	Permite recuperar archivos de una partición formateada, disco duro, USB, tarjeta de memoria, entre otras. Recupera archivos perdidos por ataques de virus, errores humanos, caídas del sistema u otras razones desconocidas. Realiza la recuperación mientras está escaneando. Posee un filtrado de tipo de archivo en específico.	Todas las funcionalidades del programa se adquieren con la versión pagada. No permite clonar un disco duro para usarlo como arranque de un PC.
Puran File Recovery	Permite escanear los archivos eliminados en pocos segundos Recuperación rápida de archivos Ofrece más de 50 tipos de formatos de archivos recuperables Cuenta con una versión portátil	El programa solo está disponible en versiones para el hogar
Stellar Data Recovery	Recupera datos perdidos de unidades formateadas, corruptas e infectadas con virus Recupera diferentes tipos de formatos de archivos en diferentes dispositivos de almacenamiento Proporciona una opción de filtrado para clasificar los archivos Permite pausar y guarda la recuperación de archivos eliminados para posteriormente reanudar el proceso	Todas las funcionalidades del programa se obtienen al adquirir el programa completo
Glary Undelete	Permite la recuperación de archivos eliminados, comprimidos o encriptados Ofrece una vista de archivos al estilo del Explorador y una indicación de Estado Soporta Fat, Fat 16, Fat32, NTFS, NTFS5, NTFS + EFS Recupera archivos borrados por virus y errores del sistema.	El programa solo está disponible en versiones para el hogar

Fuente: Elaboración propia

Tabla 12: Criterios de selección de los programas para recuperar archivos eliminados

CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE PROGRAMA PARA RECUPERAR ARCHIVOS ELIMINADOS				
CRITERIOS	EaseUS Data Recovery Wizard	Puran File Recovery	Stellar Data Recovery	Glary Undelete
Facilidad de uso de interfaz	3	3	3	3
Accesibilidad económica	3	3	3	3
Adaptación al desarrollo del caso	2	2	3	2
Software conocido y utilizado	2	1	3	2
TOTAL	10	9	12	10

Fuente: Elaboración propia

Comparando las características de los programas y teniendo en cuenta el cuadro de criterio, se optó por escoger el programa Stellar Data Recovery, debido a que es el que mejor se adecua a las necesidades del caso propuesto en nuestro proyecto y es el programa más conocido por los usuarios.

Tabla 13: Programas para recuperar archivos ocultos del USB

PROGRAMAS PARA RECUPERAR ARCHIVOS OCULTOS DEL USB		
PROGRAMAS	**VENTAJAS**	**DESVENTAJAS**
UNERASER	Recuperación rápida de ficheros y carpetas ocultas en cualquier tipo de almacenamiento. Permite la recuperación de archivos fragmentados, comprimido, dispersos y cifrados. Permite navegar por los ficheros y carpetas del explorador de Windows. Muestra el estado de la integridad y evalúa la posibilidad de recuperación de archivos.	Se debe obtener las versiones pagas para acceder a funciones avanzadas. Solo está disponible en inglés.
Disk Drill	Permite la recuperación de archivos ocultos de cualquier dispositivo de almacenamiento Permite obtener una vista de los archivos antes de recuperarlos	No hay versión portátil de este programa. Todas las funcionalidades del programa se obtienen al adquirir el programa completo

	Realiza copias de seguridad de una unidad completa	
	Cuenta con un método de filtrado de archivos por fecha o tamaño	
	Restaura Archivos y carpetas ocultos del USB	No alerta sobre archivos corruptos
USB Rescate	Administra las memorias USB con detalles	No avisa de la presencia de virus
	Eliminar carpetas y archivos ocultos que se crean automáticamente por los virus	
USB Show	Detecta archivos o carpetas ocultas contenidas en memorias extraíbles USB	No puede actuar contra el malware
	Detecta presencia de malware	Funcionalidades limitadas
	Es portable	

Fuente: Elaboración propia

Tabla 14: Criterios de selección de los programas para recuperar archivos eliminados

CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE PROGRAMA PARA RECUPERAR ARCHIVOS OCULTOS				
CRITERIOS	UNERASER	Disk Drill	USB Rescate	USB Show
Facilidad de uso de interfaz	3	3	3	3
Accesibilidad económica	3	3	3	3
Adaptación al desarrollo del caso	2	3	2	1
Software conocido y utilizado	2	3	1	1
TOTAL	10	12	9	8

Fuente: Elaboración propia

Comparando las características de los programas y teniendo en cuenta el cuadro de criterio, se optó por escoger el programa Disk Drill, debido a que es el que mejor se adecua a las necesidades del caso propuesto en nuestro proyecto y es el programa más conocido por los usuarios.

Tabla 15: Programa para verificar la integridad de los discos DVD

PROGRAMAS PARA VERIFICAR ESTADO DE INTEGRIDAD DE LOS DISCOS DVD		
PROGRAMAS	**VENTAJAS**	**DESVENTAJAS**
CDReader	Escanea unidades o directorios en busca de archivos ilegibles Genera reportes de los elementos que no pueden ser leídos Su diseño sigue la estética de los exploradores clásicos Es portable	Funcionalidades limitadas
VSO Inspector	Analiza detalladamente todos los componentes y drivers de las unidades de CD o DVD Comprueba si existen fallos en algún CD o DVD Realiza una prueba de errores para asegurar de que la grabación ha sido exitosa Es gratuita	Funcionalidades limitadas El proceso de análisis no es tan eficiente
Emsa DiskCheck	Realiza un análisis de fondo en unidades de CD o DVD Realiza pruebas para determinar la velocidad y capacidad real del disco Informa cualquier error encontrado Es gratuito	Funcionalidades limitadas
DVDisaster	Crea un archivo de corrección de errores para evitar pérdidas de información en discos CD o DVD. Comprueba la velocidad de lectura de la unidad y la legibilidad del disco Restaura los posibles defectos a partir del archivo de corrección de errores. Es gratuito	Funcionalidades limitadas Requiere espacio en el disco para almacenar datos de recuperación

Fuente: Elaboración propia

Tabla 16: Criterios de selección de los programas para analizar estado de DVD

CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE PROGRAMA PARA ANALIZAR ESTADO DE DVD				
CRITERIOS	CDReader 3.0	VSO Inspector	Emsa DiskCheck	DVDisaster
Facilidad de uso de interfaz	3	3	3	3
Accesibilidad económica	3	3	3	3
Adaptación al desarrollo del caso	3	1	2	2
Software conocido y utilizado	3	2	2	1
TOTAL	12	9	10	9

Fuente: Elaboración propia

Comparando las características de los programas y teniendo en cuenta el cuadro de criterio, se optó por escoger el programa CDReader 3.0, debido a que es el que mejor se adecua a las necesidades del caso propuesto en nuestro proyecto.

Tabla 17: Programas para recuperar archivos en los discos dañados

PROGRAMAS PARA RECUPERAR ARCHIVOS DAÑADOS EN LOS DISCOS DVD		
PROGRAMAS	**VENTAJAS**	**DESVENTAJAS**
Unstoppable Copier	Permite leer archivos y directorios dañados sin mostrar un diálogo de error	No es infalible
	Recupera archivos de discos con daño físico	El tiempo de recuperación de datos es elevado
	No muestra ventanas y diálogos de confirmación y realiza todo el proceso de copia sin la intervención del usuario	
	Es capaz de copiar archivos del sistema o que estén en uso sin ningún problema.	
CD Data Recovery	Analiza todos los sectores del disco	No es infalible

	Recupera datos corruptos almacenados en CD o un DVD	El tiempo de recuperación de datos es elevado
	Ofrece un mecanismo para verificar la integridad de los datos	
	Recupera datos de discos ópticos dañados (CD, DVD, Blu-ray, HD-DVD)	No es infalible
IsoBuster	Crea imágenes ISO	El tiempo de recuperación de datos es elevado
	Permite rellenar los datos que faltan con ceros o valores aleatorio	Todas las funcionalidades del programa se obtienen al adquirir el programa completo
	También lee memorias flash	
	Analiza datos dañados debido al daño físico o por errores de programas	No es infalible
Recovery Toolbox for CD	Recupera datos dañados almacenados en discos CD/DVD	No recupera archivos de discos duros
	Ofrece control completo sobre el proceso de recuperación	
	Muestra un informe detallado sobre el proceso de recuperación de datos	

Fuente: Elaboración propia

Tabla 18: Criterios de selección de los programas parar recuperar archivos dañados CD/DVD

CUMPLIMIENTO DE CRITERIOS DE SELECCIÓN DE PROGRAMA PARA RECUPERAR ARCHIVOS ALMACENADOS EN CD/DVD DAÑADOS				
CRITERIOS	Unstoppable Copier	CD Data Recovery	IsoBuster	Recovery Toolbox for CD
Facilidad de uso de interfaz	3	3	3	3
Accesibilidad económica	3	3	2	3
Adaptación al desarrollo del caso	1	2	3	3
Software conocido y utilizado	1	2	2	3
TOTAL	8	10	10	12

Fuente: Elaboración propia

Comparando las características de los programas y teniendo en cuenta el cuadro de criterio, se optó por escoger el programa Recovery Toolbox for CD, debido a que es el que mejor se adecua a las necesidades del caso propuesto en nuestro proyecto y es el programa más conocido por los usuarios

Tabla 19: Valores para comparar programas

Lectura del cuadro comparativo	
3	Representa un alto grado de cumplimiento del criterio
2	Representa que el criterio se cumple parcialmente
1	Significa que el criterio no se satisface lo suficiente

Fuente: Elaboración propia

3.1.3. Aplicación de la metodología PURI para Datos

3.1.3.1. Descripción Del Caso N° 01

En un hecho delictivo, una persona denuncia en la comisaria que está siendo extorsionada por un individuo el cual ya tiene antecedentes policiales por los delitos de extorsión.

Tras un seguimiento, se detiene a la persona acusada de extorsión, a la cual se le incautó un ordenador portátil y dispositivos extraíbles de almacenamiento (USB, disco duro externo) para posteriormente realizar sus respectivos análisis.

Estos dispositivos poseen supuesta información personal de varios individuos como información de tarjeta de créditos, correos personales, cuentas bancarias, entre otros.

Objetivo: Analizar los dispositivos de almacenamiento realizando una descripción técnica de su contenido.

Acción Pericial: Realizar un análisis de los dispositivos de almacenamiento, manteniendo la integridad de los dispositivos, sin alterar su información.

- *Desarrollo de la Metodología*

3.1.3.2. Identificación

Para empezar con la aplicación de la metodología propuesta, se realizará el llenado del formulario FORM N° 001 – Ficha técnica de investigación, donde se detallará el incidente. (Ver Anexo 1 : Ficha técnica de Investigación).

En el formulario FORM N° 001, habrá unos campos donde se detallan ciertos datos del extorsionar, el cual nos permitió rastrearlo y ubicarlo.

A continuación, el investigador forense toma fotografías de todo lo encontrado en la casa del extorsionador, identificando los dispositivos de almacenamiento. Todo lo encontrado se registra en el formulario FORM N° 002 – Identificación de las evidencias. (Ver Anexo 2: Identificación de las evidencias).

Los investigadores forenses guardan todo el material encontrado que pueda servir como evidencia bajo su custodia para posteriormente realizar sus respectivos análisis.

Evidencia física:

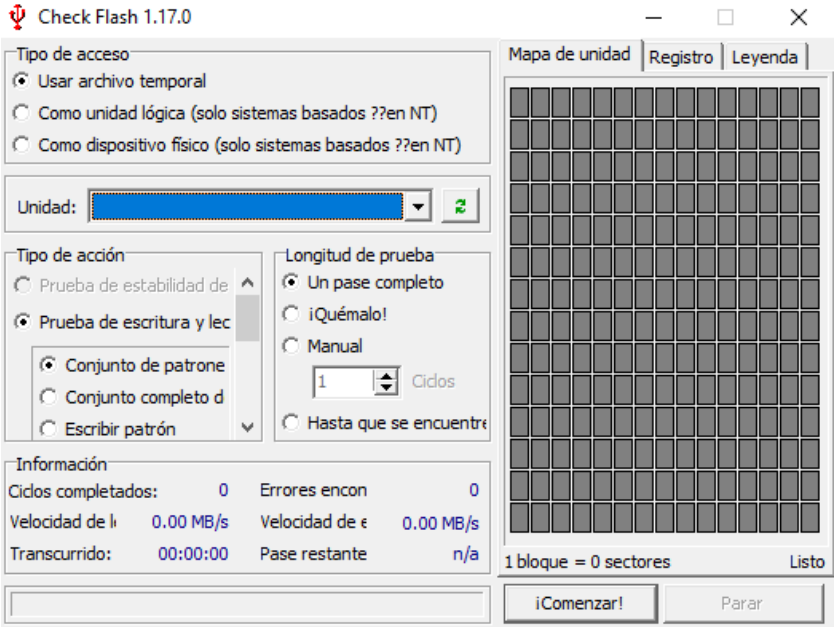
- Computadora portátil
- Celular
- Disco duro
- USB

3.1.3.3. Adquisición

En esta etapa el investigador forense extraerá la evidencia, el cual procederemos a llenar el formulario FORM N° 003 – Adquisición de la información (Ver Anexo 3: Adquisición de la Información), donde se analizará y se tendrá un control de lo obtenido en el dispositivo de almacenamiento externo USB.

Como primer paso verificaremos la integridad del USB y comprobaremos si la partición está corrupta o encriptada utilizando el programa Check Flash, el cual se muestra a continuación:

Ilustración 7: Interfaz del programa Check Flash



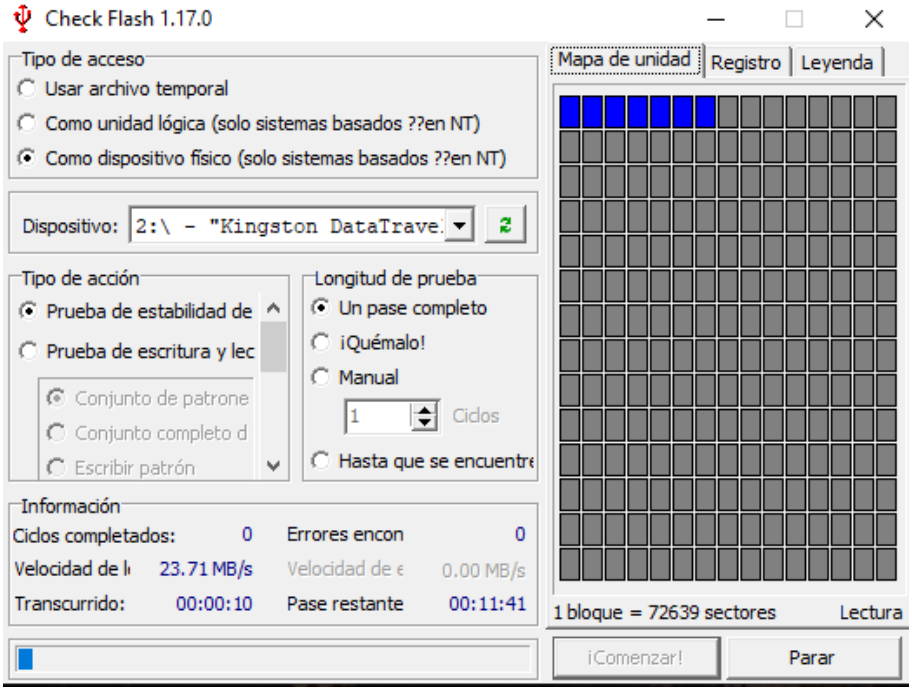
Fuente: Elaboración propia

- Para realizar el proceso de verificación, señalamos la opción “como dispositivo físico” esto opción nos permitirá seleccionar el dispositivo a analizar, en este caso el USB que lleva por nombre “Kingston DataTraveler 2.0 USB Device”.

- La acción a realizar será de solo lectura, esto nos permitirá mantener la integridad del contenido.

- La longitud de prueba será de pase completo, esto nos permitirá analizar el dispositivo de inicio a fin.

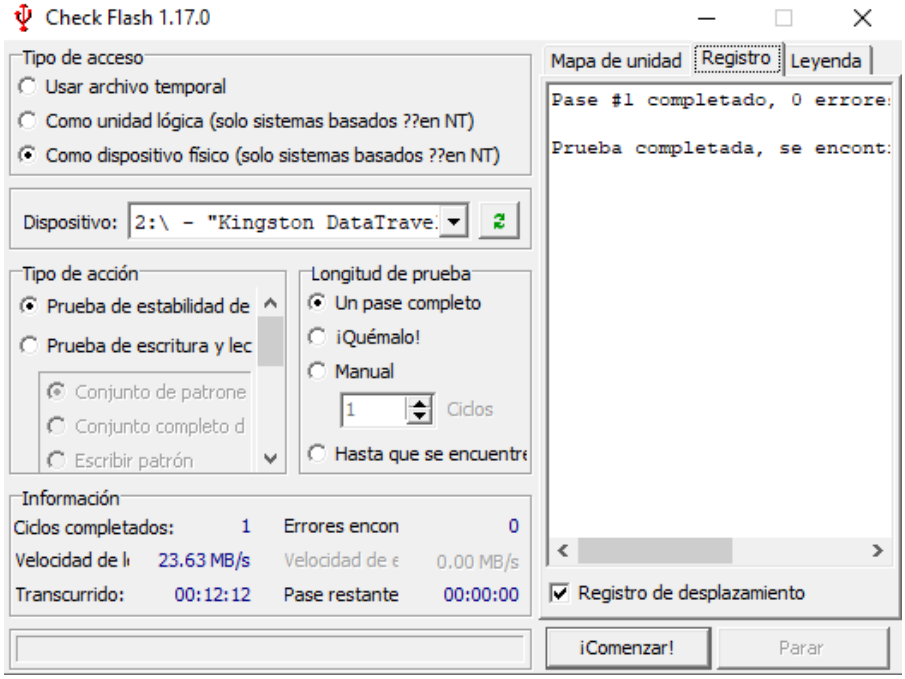
Ilustración 8: Análisis del dispositivo USB



Fuente: Elaboración propia

Una vez terminado el proceso de verificación, se mostrará en el cuadro de registro el resultado del análisis. En este caso se muestra que el USB no contiene errores y está libre de cualquier encriptación.

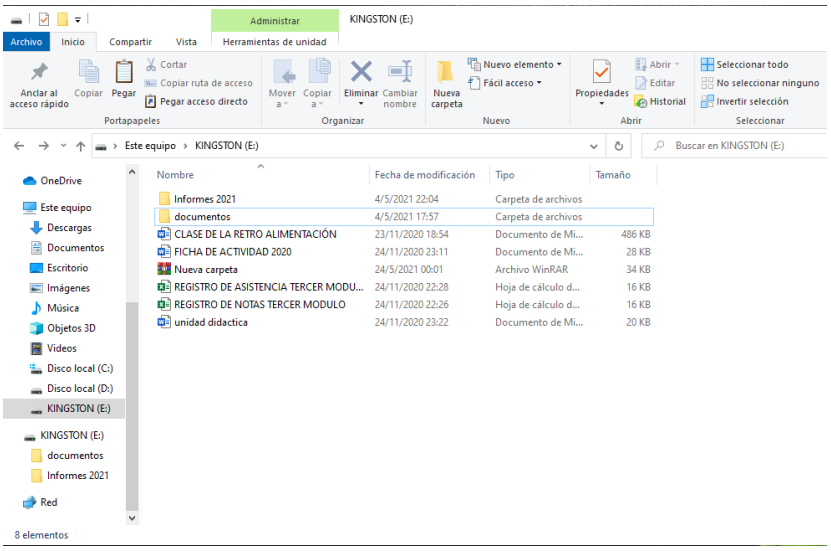
Ilustración 9: Resultado del Análisis del dispositivo USB



Fuente: Elaboración propia

Después de comprobar el estado del USB, visualizamos su contenido. A simple vista encontramos carpetas, documentos en formato Word, Excel y un archivo RAR que lleva por nombre “Nueva carpeta”.

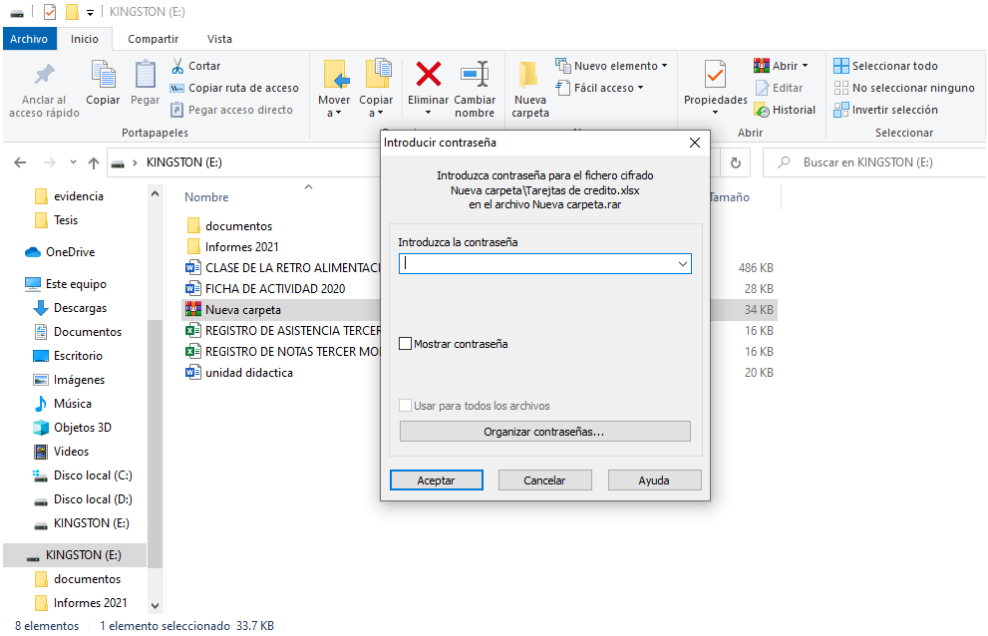
Ilustración 10: Archivos del dispositivo USB



Fuente: Elaboración Propia

Al momento de querer extraer la información comprimida en el archivo RAR, se muestra una ventana emergente con el mensaje “introduzca la contraseña”.

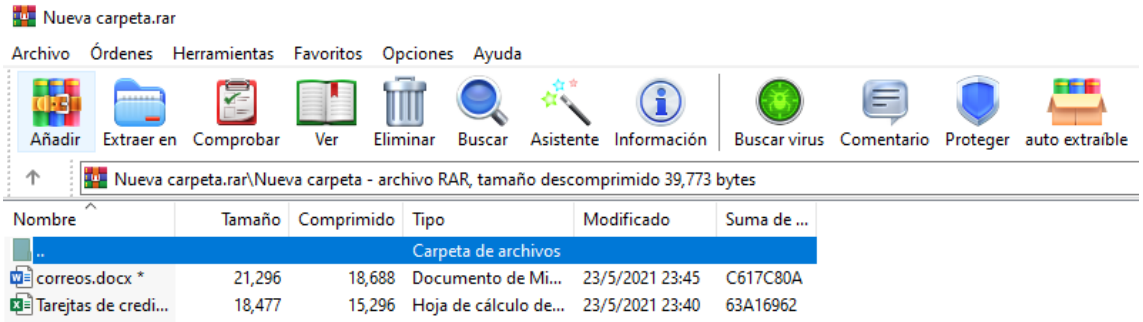
Ilustración 11: Cuadro de diálogo para ingresar la clave



Fuente: Elaboración propia

El programa WinRAR nos permite previsualizar su contenido, pero sin poder abrir sus documentos. Podemos ver que dentro de la carpeta comprimida encontramos dos archivos que llevan por nombre: correos (formato .docx) y tarjetas de crédito (formato .xlsx), el cual puede contener evidencia importante.

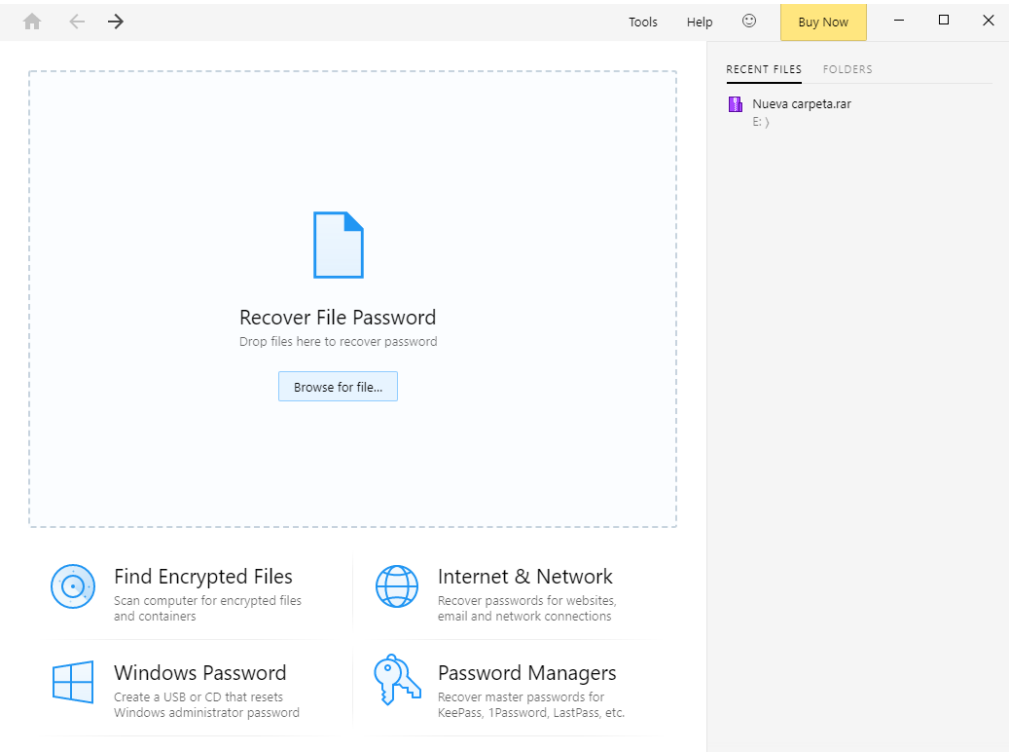
Ilustración 12: Vista previa de archivos



Fuente: Elaboración propia

Para poder descifrar la contraseña de la carpeta comprimida “Nueva carpeta”, utilizaremos el programa Passware Kit, el cual se muestra a continuación:

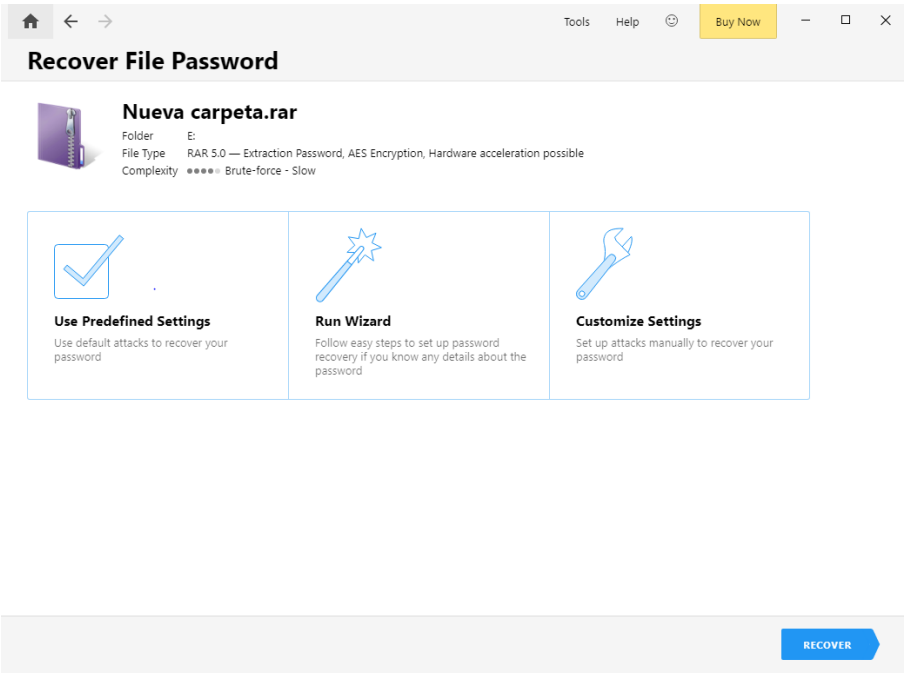
Ilustración 13: Interfaz del programa Passware Kit



Fuente: Elaboración propia

- En la pestaña “Browse for file” buscaremos la ubicación de archivo, en este caso se encuentra en KINGSTON (E:) y seleccionamos el archivo RAR.
- Luego escogeremos la opción “Use Predefined Setting” y le damos en “RECOVER”.

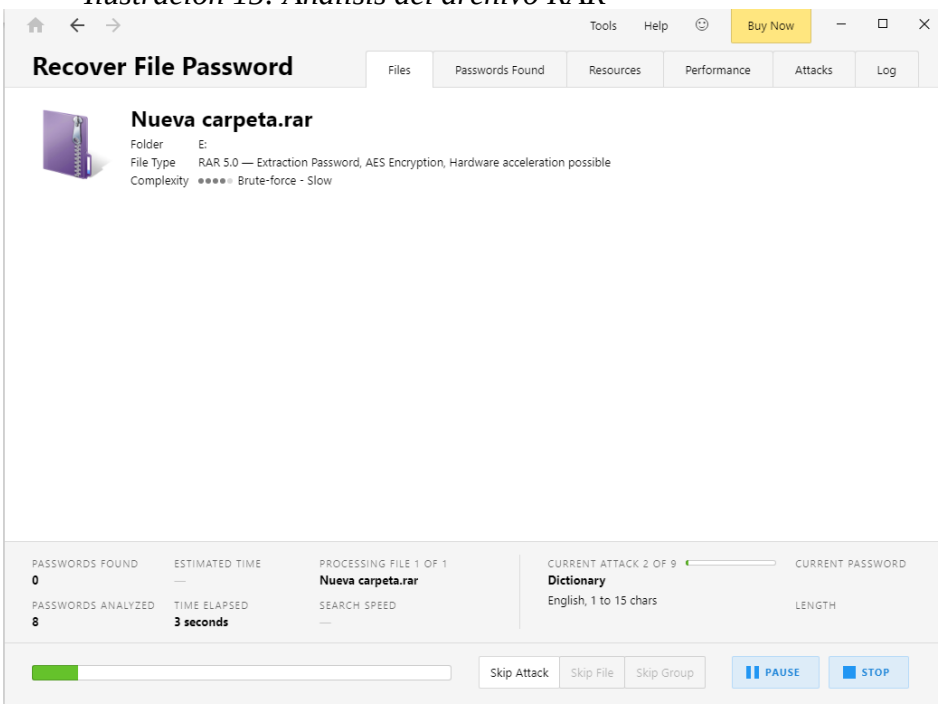
Ilustración 14: Ubicación del archivo RAR



Fuente: Elaboración propia

- El programa empezará a realizar el proceso de descifrado de la carpeta.

Ilustración 15: Análisis del archivo RAR

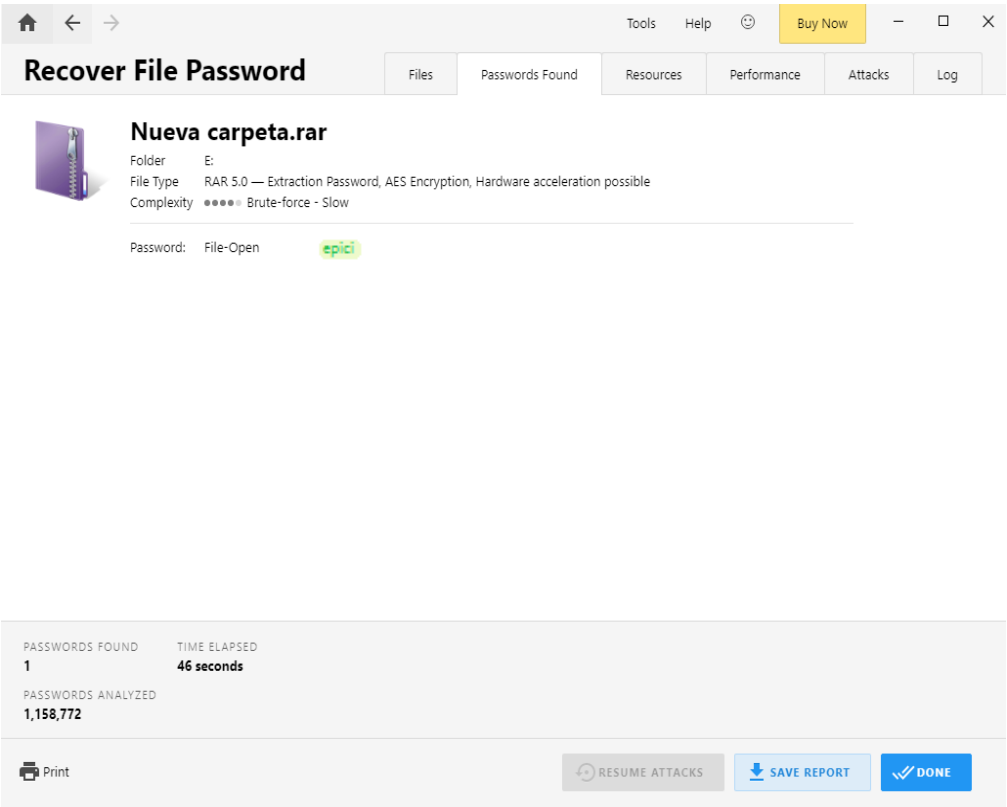


Fuente: Elaboración propia

Cuando termine la carga, se nos mostrara una ventana con la contraseña del archivo RAR, el cual nos muestra que es “epici”.

El tiempo de espera para que el programa descifre la contraseña, dependerá de la complejidad de la misma, debido a que el programa buscará todas las combinaciones posibles: letras mayúsculas, letras minúsculas, números, símbolos.

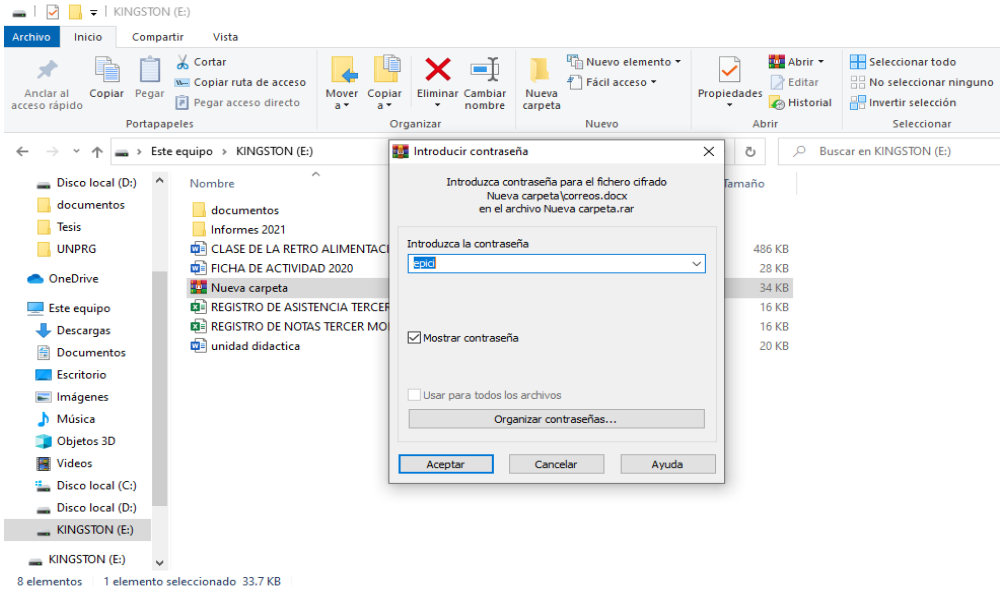
Ilustración 16 : Resultado del descifrado



Fuente: Elaboración propia

- A continuación, extraeremos la carpeta contenedora con la contraseña y visualizaremos su contenido.

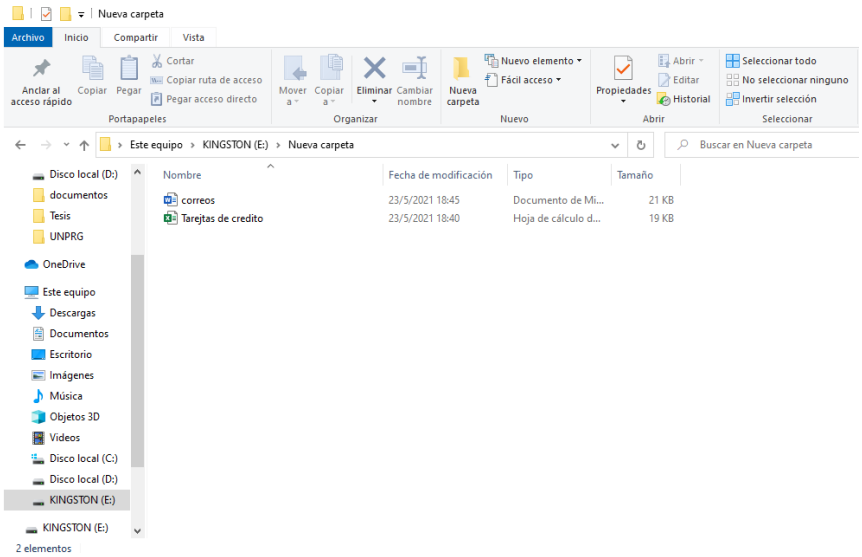
Ilustración 17: Cuadro de diálogo con contraseña



Fuente: Elaboración propia

- Podemos ver los archivos que se mostraban anteriormente. A continuación, procederemos a revisar cada uno de los documentos.

Ilustración 18: Visualización de contenido de "Nueva Carpeta"



Fuente: Elaboración propia

- Analizamos el primer archivo que lleva por nombre "correos" cuyo tipo de formato es Word (.docx).

- Podemos apreciar que en su contenido nos muestra una lista de correos y contraseñas pertenecientes a varios usuarios con diferentes cargos. El documento especifica que dichos correos son de uso privado y no se permite su uso sin autorización

Ilustración 19 : Contenido del archivo Word "correos"

49	kimbery_sanderson@outlook.com	mVSPxD04Y9s0Rqz	Abogado
50	ethelyn_david@aol.com	LjXeY_OTDz7Z5nA	Licenciado
51	mona_bowes@hotmail.com	TyzfIqDOX8JVpmT	Gerente
52	graham_boyd@yandex.com	TBPn8yRKaH92bVO	Asesor Comercial
53	wanetta_lawson@zohomail.com	FQfffPMLqNjR0de	Administrador
54	floretta_ryan@aol.com	HTTf26UMrS1Mayw	Licenciado
55	andera_lyons@mail.com	6_cNAR23xgexMt4	Empresario
56	vaughn_penn@mail.com	4dwlDEDrnitIcv_	Gerente
57	kelley_ferreira@hotmail.com	ZgCl3FVLGVRsIjB	Asesor Comercial
58	merlin_grainger@yandex.com	7veWDNkl3chx_ET	Administrador
59	valda_moseley@protonmail.com	fCovcrdYpgtIicm	Licenciado
60	hans_reader@outlook.com	HJpbiN7yRWKlmor	Empresario
61	wei_arnold@hotmail.com	ASWz7FX8iZw9UEB	Abogado
62	angelina_campbell@yandex.com	LH6n68tvJAmRwUH	Licenciado
63	shanel_gordon@gmail.com	KGJY8bX09yEnJhj	Gerente
64	kayleigh_samuels@yandex.com	wFJ1kzoUQHuj7uI	Asesor Comercial
65	shondra_davie@yahoo.com	6T7y_WledEfONht	Administrador
66	jovan_mclaughlin@mail.com	LhI_gwQYjeNg09U	Licenciado
67	sherman_handley@mail.com	ThiKmQgIpvgBZ59	Empresario
68	darnell_derrick@protonmail.com	f_268VHx4gbjqEB	Gerente
69	sunshine_hayes@hotmail.com	2x4yK5STfH1gRnP	Asesor Comercial
70	rosalia_hampton@yahoo.com	NQ1XGqPoBfrEXQ7	Administrador

NOTA: Estos correos empresariales son únicos y privados, no se permite su distribución sin autorización, en caso contrario se tomará todas las medidas de ley. Atte: La Gerencia

Fuente: Elaboración propia

- Analizamos el segundo documento que lleva por nombre "tarjetas de crédito" cuyo tipo de formato es Excel (.xlsx).

- Podemos apreciar que en su contenido se encuentran 4 hojas que llevan por nombre VISA, MASTERCARD, DINNERS Y AMERICA EXPRESS.

- Cada hoja nos muestra una lista de información completa de tarjetas de crédito de diferentes personas.

Ilustración 20: Contenido del archivo Excel "Tarjetas de crédito"

1)		
MARCA DE TARJETA	: VISA	
NÚMERO DE TARJETA	: 4500072535905521	
BANCO	: BANCO RIPLEY S.A.	
NOMBRE	: Christian Karlsen	
DIRECCIÓN	: Tabar 3790	
PAÍS	: PERU	
DINERO	: $584	
CVV/CVV2	: 455	
FECHA DE CADUCIDAD	: 04/2024	
PIN DE TARJETA	: 9235	
2)		
MARCA DE TARJETA	: VISA	
NÚMERO DE TARJETA	: 4824217404744233	
BANCO	: BANCO RIPLEY S.A.	
NOMBRE	: Daniel Myllri	
DIRECCIÓN	: R Conselheiro Joo Cunha 104	
PAÍS	: PERU	
DINERO	: $646	
CVV/CVV2	: 818	
FECHA DE CADUCIDAD	: 08/2022	
PIN DE TARJETA	: 4131	
3)		
MARCA DE TARJETA	: VISA	
NÚMERO DE TARJETA	: 4824214383378414	
BANCO	: BANCO RIPLEY S.A.	
NOMBRE	: Johannes Chiagoziem	
DIRECCIÓN	: C/ Libertad 4	
PAÍS	: PERU	
DINERO		
CVV/CVV2	: 887	
FECHA DE CADUCIDAD	: 04/2021	
PIN DE TARJETA	: 8855	

Fuente: Elaboración propia

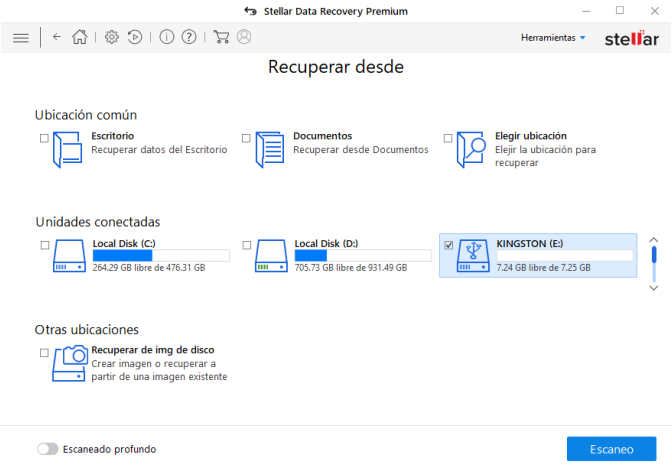
A continuación, utilizaremos el programa Stellar Data Recovery, este programa nos permitirá recuperar archivos que hayan sido eliminados del USB.

Ilustración 21: Interfaz del programa Stellar Data Recovery

Fuente: Elaboración propia

- Marcada la opción “Todo”, daremos clic en siguiente y seleccionaremos el dispositivo a analizar, en este caso será la unidad “KINGSTON (E:)”, por último, le damos en “Escaneo”.

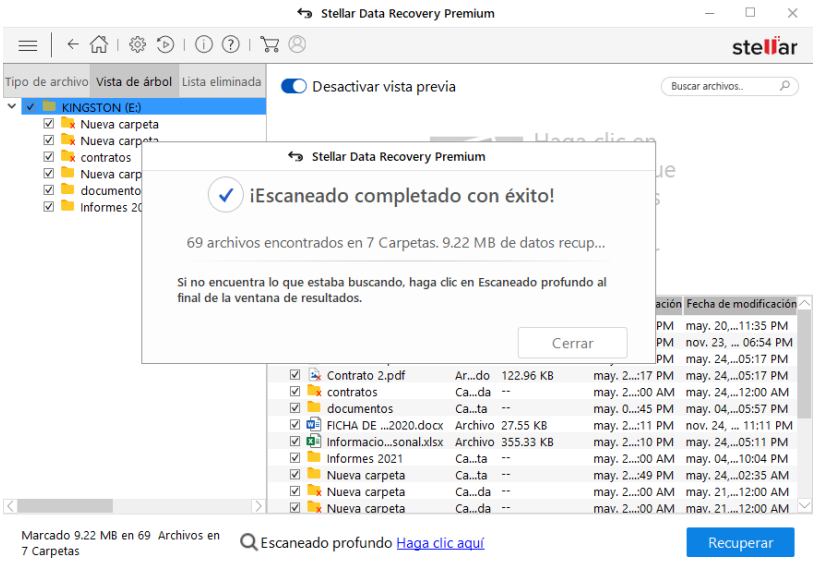
Ilustración 22: Selección del dispositivo a analizar



Fuente: Elaboración propia

- Una vez que se haya escaneado todo el USB, nos aparecerá la siguiente ventana con un resumen de la cantidad de archivos encontrados.

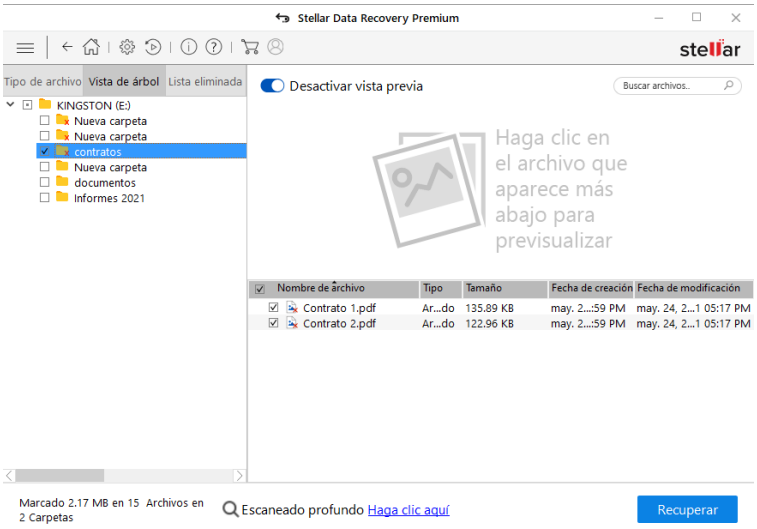
Ilustración 23: Resumen de los archivos encontrados



Fuente: Elaboración propia

- Navegando por el USB, encontramos una carpeta que lleva por nombre “contratos”, el cual contiene dos archivos que tienen por nombre “Contrato 1” y “Contrato 2”.

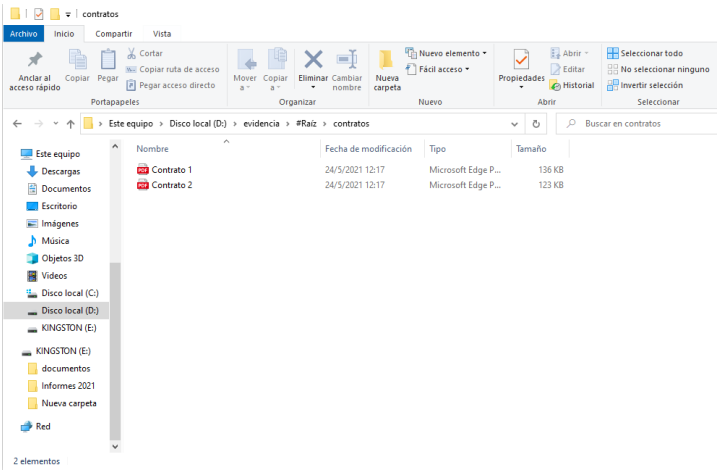
Ilustración 24: Visualización de archivos eliminados



Fuente: Elaboración propia

- A continuación, procederemos a recuperar los dos archivos, la ruta a almacenar será en el Disco local D, en una carpeta que llevará por nombre “evidencia”, los archivos por defecto se almacenan en una carpeta con nombre “#Raiz”.

Ilustración 25: Archivos eliminados recuperados



Fuente: Elaboración propia

- Analizando los dos documentos que se encuentran en formato PDF, visualizamos que son contratos de afiliación de bancos, el cual cuenta con las firmas tanto del gerente del banco como de los representantes.

Ilustración 26: Contenido de contrato 2

Scotiabank

CONTRATO DE AFILIACION AL SERVICIO DE PAGO DE APORTES PREVISIONALES VIA EL PORTAL DE AFPNET

Conste por el presente documento el contrato de afiliación al servicio de pago de aportes previsionales vía el portal de AFPnet (en adelante, el "Contrato") que celebran de una parte, **SCOTIABANK PERÚ S.A.A.**, con Registro Único de Contribuyente Nº 20100043140, con domicilio en Av. Dionisio Derteano 102, Distrito de San Isidro, Provincia y Departamento de Lima, debidamente representado por los apoderados cuyos datos constan al final de este documento, a quien en adelante se le denominará el "BANCO"; y de la otra parte, el "CLIENTE", cuyos datos, conjuntamente con los de sus representantes se indican al final del presente documento, bajo los términos y condiciones siguientes:

PRIMERO: ANTECEDENTES

1.1 El BANCO es una empresa del sistema financiero organizada de acuerdo a las leyes de la República del Perú, que se rige por sus estatutos, la Ley Nº 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y demás disposiciones establecidas por la Superintendencia de Banca y Seguros que le resultan aplicables.

Fuente: (scotiabank, s.f.)

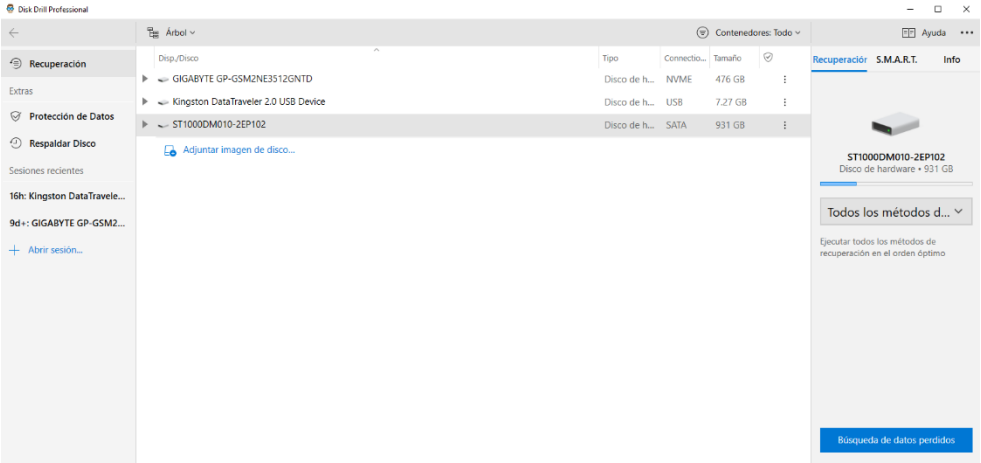
Ilustración 27: Firmas del contrato 2

EL BANCO	**CLIENTE 1**
EL BANCO	**CLIENTE 2**
Razón Social: SCOTIABANK PERÚ S.A.A. RUC: 20100043140 Domicilio : Calle Las Vegas, Mz. A32 - Lt. 21 Urb. Primavera Representante 1: Jacinto Sánchez DNI N° 40057187	Razón Social: SCOTIABANK RUC: 20100043140 Domicilio: Saenz Peña 025 - Bolognesi Representante 2: Hector Carballo DNI N°14789652
Poderes inscritos en la Partida Electrónica N° 11008578 del Registro de Personas Jurídicas de Lima	Poderes inscritos en la Partida Electrónica N° del Registro de Personas Jurídicas de

Fuente: (scotiabank, s.f.)

Para recuperar archivos ocultos, utilizaremos el programa Disk Drill, el cual se muestra a continuación:

Ilustración 28: Interfaz del programa Disk Drill



Fuente: Elaboración propia

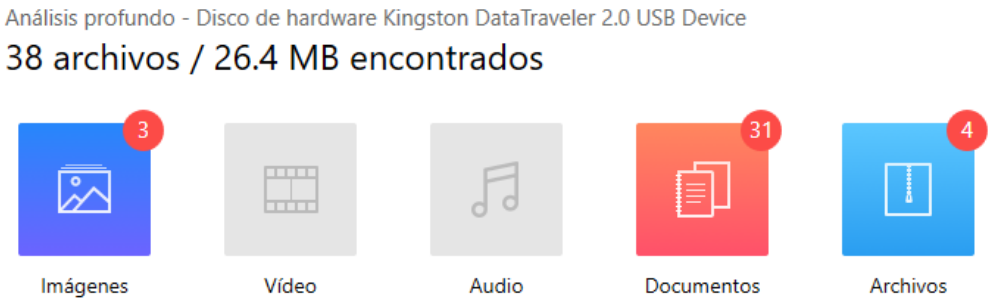
- Seleccionamos el disco a analizar, en este caso será la partición que lleva por nombre "Kingston DataTraveler 2.0 USB Device", seleccionamos la pestaña "Todos los métodos de recuperación" y escogemos la opción "Análisis profundo"

Ilustración 29: Selección de dispositivo a analizar

Fuente: Elaboración Propia

- Una vez terminada el análisis, nos muestra un resumen de la cantidad de archivos encontrados en el USB.

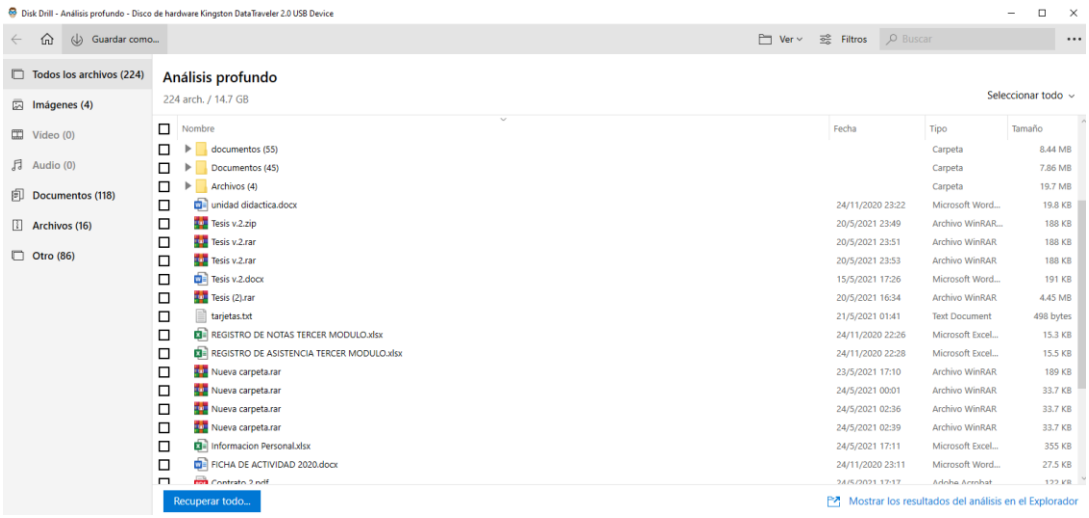
Ilustración 30: Cantidad de archivos encontrados en el USB



Fuente: Elaboración propia

- Podemos apreciar que, a través del programa, el USB contiene más archivos que su contenido original a simple vista, en el cual nos llama la atención un archivo que lleva por nombre "Información Personal", el cual procederemos a extraer.

Ilustración 31: Visualización del contenido USB a través del programa Disk Drill

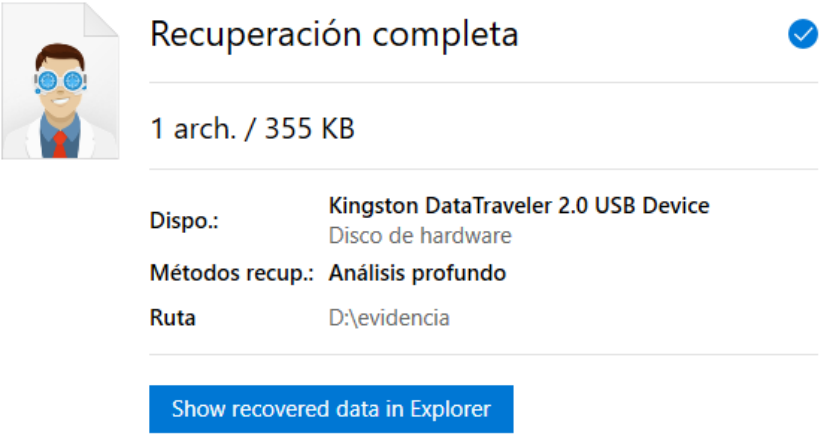


Fuente: Elaboración propia

- Para recuperar el archivo, seleccionamos la casilla y daremos clic en "Recuperar Todo".

- A continuación, escogeremos la ruta donde deseamos que se extraiga, en este caso será en el Disco local D, en la carpeta "evidencia"

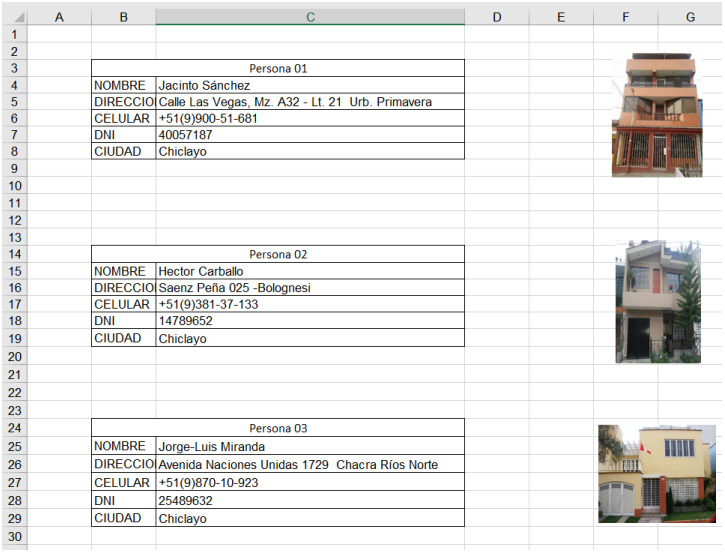
Ilustración 32: Ruta de recuperación de archivos



Fuente: Elaboración propia

- Como paso final, analizaremos el archivo extraído.
- Podemos ver que el contenido del archivo consta de datos personal de varias personas con imágenes de sus domicilios.

Ilustración 33: Contenido del archivo Excel "Información personal"



Persona 01	
NOMBRE	Jacinto Sánchez
DIRECCIO	Calle Las Vegas, Mz. A32 - Lt. 21 Urb. Primavera
CELULAR	+51(9)900-51-681
DNI	40057187
CIUDAD	Chiclayo
Persona 02	
NOMBRE	Hector Carballo
DIRECCIO	Saenz Peña 025 -Bolognesi
CELULAR	+51(9)381-37-133
DNI	14789652
CIUDAD	Chiclayo
Persona 03	
NOMBRE	Jorge-Luis Miranda
DIRECCIO	Avenida Naciones Unidas 1729 Chacra Ríos Norte
CELULAR	+51(9)870-10-923
DNI	25489632
CIUDAD	Chiclayo

Fuente: Elaboración propia

- El nombre de Jacinto Sánchez figura en el contrato 2 y es el nombre de la persona denunciante.

3.1.3.4. Análisis

Una vez concluida la fase de adquisición procederemos a analizar toda la evidencia obtenida. Para ello se llenará el formulario FORM N° 7 – Análisis de la evidencia (Ver Anexo 5: Análisis de la evidencia)

Paso 1

Analizamos la integridad del dispositivo USB incautado para comprobar si el estado del dispositivo esta corrupto o encriptado, este análisis se realizó utilizando el programa "Check Flash", el cual mostro como resultado que el USB no tiene errores y está libre de cualquier cifrado.

Paso 2

Revisando el contenido del USB a simple vista, se puede apreciar un archivo RAR que

ANÁLISIS DE LA EVIDENCIA	**FORM N° 007** **Fecha: 02/05/2021**
N° de Expediente:	EXP001
Analista	Erick Casas Villar
Cargo	Analista
Al realizar el análisis del dispositivo USB con los programas Disk drill, Stellar Data Recovery, Passware Kit, Check Flash, se recuperaron los siguientes archivos: Un archivo RAR "Nueva Carpeta" con contraseña (se logró desencriptar) Dos archivos eliminados en formato PDF: "Contrato1" y "Contrato2" (se logró recuperar) Un archivo oculto en formato Excel: "Información personal" (se logró recuperar)	

lleva por nombre "Nueva carpeta", el cual está protegido por una contraseña. Para poder obtener la contraseña, utilizamos el programa "Passware Kit", después de un tiempo determinado, se muestra la contraseña, teniendo esta por nombre "epici".

Dentro de la carpera se encontró dos archivos formato office, “correos(.docx)” y “tarjetas de crédito(.xlsx)”.

Paso 3

Para verificar si el USB ha tenido archivos eliminados, utilizamos el programa “Stellar Data Recovery”, el cual nos permite recuperar los archivos. Una vez escaneado el dispositivo, encontramos una carpeta con nombre “contratos” la cual contiene dos archivos PDF.

Paso 4

Utilizando el programa “Disk Drill” podremos recuperar archivos que estén ocultos en el USB, a través de un análisis profundo. Una vez terminado el proceso de análisis, encontramos un archivo en formato Excel(.xlsx) que lleva por nombre “Información Personal”.

3.1.3.5. Presentación

Una vez interpretada toda la evidencia obtenida, procederemos a realizar el informe final

INFORME FINAL	**FORM N° 007**
	FECHAS: 05/05/2021

N° de Expediente: EXP001

- *Precedente*

Descripción del incidente

En un hecho delictivo, una persona denuncia en la comisaria que está siendo extorsionada por un individuo el cual ya tiene antecedentes policiales por los delitos de extorsión.

Tras un seguimiento, se detiene a la persona acusada de extorsión, a la cual se le incautó un ordenador portátil y dispositivos extraíbles de almacenamiento (USB, disco duro externo) para posteriormente realizar sus respectivos análisis.

Estos dispositivos poseen supuesta información personal de varios individuos como información de tarjeta de créditos, correos personales, cuentas bancarias, entre otros.

Objetivo

Analizar el dispositivo de almacenamiento USB, realizando una descripción técnica de su contenido.

- *Tareas Realizadas*

Descripción de la evidencia

En la siguiente tabla, nombraremos los archivos encontrados en el dispositivo USB tras los diferentes análisis.

- *Archivo RAR "Nueva carpeta" con contraseña*

- Se encontró un documento Word (correos)
- Se encontró un documento Excel (tarjetas de credito)

- *Archivos eliminados*

- Se encontró dos PDF con nombres "contrato 1" y "contrato2"

- *Archivos ocultos*

- Se encontró un archivo Excel con nombre "Información personal"

Descripción de las herramientas utilizadas

En la siguiente tabla, se menciona los programas utilizados para el análisis del USB

- *Check Flash*

Programa utilizado para analizar el estado del USB.

- *Passware Kit*

Programa utilizado para descifrar archivos RAR con contraseña.

- *Stellar Data Recovery*

Programa utilizado para recuperar archivos eliminados del USB.

- *Disk Drill*

Programa utilizado para recuperar archivos ocultos del USB.

Descripción de la información obtenida

- Archivo Word ("correos") encontrado en la carpeta RAR, en este documento se encontró una lista de direcciones de correos electrónicos confidenciales de varios usuarios con diferentes cargos, pertenecientes a un consorcio. En la nota del documento específica, que los correos no deben ser distribuidos ni utilizados sin la autorización de la propia empresa.
- Archivo Excel ("Tarjetas de crédito") encontrado en la carpeta RAR, en este documento se encontró una lista con información completa de tarjeta de créditos, esto incluye: Marca de tarjeta, N° de tarjeta, banco, nombre del titular, dirección, país, saldo, CVV, fecha de caducidad, PIN.
- Archivo PDF ("contrato1", "contrato2") recuperados de los archivos eliminados del USB cuyos contenidos eran contratos bancarios, los cuales contenían las firmas del banco y de los representantes.
- Archivo Excel ("Información personal"), recuperado de los archivos ocultos del USB, se encontró diferentes tipos de datos como: Nombre, DNI, Dirección, Celular y Ciudad, incluyendo fotos referenciales de sus viviendas o negocios.

- *Resultado final*

Teniendo en cuenta la evidencia obtenida y analizada, podemos afirmar lo siguiente:

- El dispositivo USB fue utilizado para almacenar información confidencial y privadas de personas y de una corporación para cometer sus delitos de extorsión.
- Durante el proceso de investigación se pudo encontrar archivos formato RAR con contraseñas, documentos eliminados y ocultos.

- Después de revisar la información, podemos detectar que el nombre Jacinto Sánchez que aparece en el archivo Excel como referencia la imagen Ilustración 33: Contenido del archivo Excel "Información personal", está vinculado a los contratos recuperados de los archivos eliminados como referencia la imagen Ilustración 27: Firmas del contrato 2.

Podemos concluir que se encontraron los datos de la persona denunciante que se utilizaban para extorsionarlo en la data recuperada del dispositivo USB. Esto está penado bajo la ley de Delitos Informáticos (LEY N° 30096) – Capítulo IV (Delitos Informáticos Contra La Intimidad Y El Secreto De Las Comunicaciones) – Artículo IV (Tráfico ilegal de datos), la cual indica que el uso indebido de datos sobre una persona natural o jurídica para extorsión está penado con privación de la libertad no mayor a cinco años.

Con esta aclaración, el proceso aplicado a través de la metodología PURI llegaría con éxito a su fin.

ANEXOS CASO 01

Anexo 01

Anexo 1 : Ficha técnica de investigación

FICHA TECNICA DE INVESTIGACIÓN		**FORM N° 001** **Fecha: 20/04/2021**
DETALLES DEL INCIDENTE		
Personal Encargado	Nombre:	José Santa Cruz
	DNI:	76854568
	Cargo:	Teniente
	Correo:	josesanta@hotmail.com
N° de Expediente:	EXP001	
Fecha del incidente:	13 de abril del 2021	
Descripción del incidente:	Una persona denuncia que está haciendo extorsionada por un individuo con la finalidad de obtener dinero.	
Persona responsable del acto delictivo	Nombre:	---
	DNI:	----
	Celular:	936784628
	Lugar de trabajo:	----
	Área de Trabajo:	----
Datos del denunciante	Nombre:	Jacinto Sánchez
	DNI:	40057187
	Celular:	+51 990051681

Fuente: Elaboración propia

Anexo 02

Anexo 2: Identificación de las evidencias

IDENTIFICACIÓN DE LAS EVIDENCIAS		**FORM N° 002** **Fecha: 22/04/2021**
DETALLES DE LA INTERVENCIÓN		
Personal Encargado	Nombre:	Erick Casas Villar
	DNI:	73541556
	Cargo:	Analistas
	Correo:	ejcv@gmail.com
N° de Expediente:	EXP001	
Fecha de la intervención:	22 de abril del 2021	
Lugar de intervención:	Domicilio del extorsionador (Mz.”C” Lte. 7 – Primavera)	
Persona intervenida	Nombre:	Juan Rodríguez
	DNI:	67656789
	Celular:	936784628
Objetos Incautados		
Objeto 01 **Código: OB001**	Equipo:	Laptop
	Modelo/Marca:	X55LB / ASUS
	Memoria:	8RAM
	Descripción del objeto:	Laptop ASUS de color plomo con carcasa negra y daño en Lector de disco.
	Análisis:	SI [ ] NO [X]

Objeto 02 **Código: OB002**	Equipo:	Disco Duro
	Modelo/Marca:	Toshiba
	Memoria:	1Terabyte
	Descripción del objeto:	Disco duro externo, color negro con velocidad 3.0
	Análisis:	No se analizará el dispositivo
Objeto 03 **Código: OB003**	Equipo:	Celular
	Modelo/Marca:	Motorola E5
	Memoria:	16RAM
	Descripción del objeto:	Celular smartphone Motorola negro gamma media.
	Análisis:	SI [ ] NO [X]
Objeto 04 **Código: OB004**	Equipo:	Memoria USB
	Modelo/Marca:	Kingston
	Memoria:	8GB
	Descripción del objeto:	Dispositivo USB color gris, con velocidad de transmisión 2.0
	Análisis:	SI [X] NO [ ]

Fuente: Elaboración propia

Anexo 03

Anexo 3: Adquisición de la Información

ADQUISICIÓN DE INFORMACIÓN	**FORM N° 003** **Fecha: 26/04/2021**
N° de Expediente:	EXP001
Equipo de Trabajo	
Jefe de Equipo:	Lorena Lluén Valiente
Analista:	Erick Casas Villar
Dispositivos a Analizar	
Código de Equipo:	OB004
Programas Utilizados:	Disk drill, Stellar Data Recovery, Passware Kit, Check Flash
Procedimiento:	Analizar el estado del dispositivo y lograr obtener la información encriptada, eliminada u oculta del USB
Información Obtenida:	Un archivo RAR con contraseña (se logró desencriptar) Un archivo eliminado Dos archivos ocultos

Fuente: Elaboración propia

Anexo 04

Anexo 4: Cadena de custodia

CADENA DE CUSTODIA				**FORM N° 004**	
CASO PROPUESTO N° 01					
N° de Expediente:	EXP001				
Nombre	**Cargo**	**Código del Equipo Manipulado**	**Observación**	**Fecha/Hora**	**Firma**
Erick Casas	Analista	OB004	Se logró recuperar la información del dispositivo	30/04/2021 3:00pm	

Fuente: Elaboración propia

Anexo 05

ANÁLISIS DE LA EVIDENCIA	**FORM N° 007**
	Fecha: 02/05/2021
N° de Expediente:	EXP001
Analista	Erick Casas Villar
Cargo	Analista
Al realizar el análisis del dispositivo USB con los programas Disk drill, Stellar Data Recovery, Passware Kit, Check Flash, se recuperaron los siguientes archivos: Un archivo RAR “Nueva Carpeta” con contraseña (se logró desencriptar) Dos archivos eliminados en formato PDF: “Contrato1” y “Contrato2” (se logró recuperar) Un archivo oculto en formato Excel: “Información personal” (se logró recuperar)	

Anexo 5: Análisis de la evidencia

Fuente: Elaboración Propia

Una vez realizado todos los procesos, podemos concluir que la aplicación de la informática forense con ayuda de la metodología PURI nos permitió obtener los datos que serán de suma importancia para la toma de decisiones en el ámbito judicial, el cual se obtuvo a través de los diferentes programas aplicados para la verificación del estado del dispositivo USB como también para la recuperación de datos eliminados, ocultos o encriptados.

3.1.4. Aplicación de la metodología PURI para Evidencias

3.1.4.1. Descripción del caso N° 02

Se produce un incidente en una institución dedicada al rubro de educación y certificación en tecnología de información.

Dicha empresa decide contratar servicios para investigar al jefe del área académica, por la supuesta venta ilegal de videos de las diferentes clases dictadas de manera virtual.

La institución sospecha que estos videos los estaba almacenando en DVD's, los cuales estaban camuflados en discos con los softwares utilizados por la institución.

Objetivo: Se contratan los servicios de investigación para obtener las pruebas necesarias para incriminar del jefe del área academia por la venta ilegal de los cursos.

Acción Pericial: Al visitar las instalaciones de la institución en presencia del jefe del área académica y los administrativos de la institución, se registró su espacio de trabajo tomando como evidencia 3 discos DVD's para su respectivo análisis.

- *Desarrollo de la Metodología*

3.1.4.2. Identificación

Para empezar con la aplicación de la metodología propuesta, se realizará el llenado del formulario FORM N° 001 – Ficha técnica de investigación, donde se detallará el incidente. (Ver Anexo 6: Ficha técnica de investigación).

El investigador forense toma fotografías de todo lo encontrado en el área de trabajo del acusado, identificando los discos DVD's. Todo lo encontrado se registra en el formulario FORM N° 002 – Identificación de las evidencias. (Ver Anexo 7: Identificación de las evidencias)

Los investigadores forenses guardan todo el material encontrado que pueda servir como evidencia bajo su custodia para posteriormente realizar sus respectivos análisis.

Evidencia física:

- Computadora portátil
- Memoria USB
- 3 CD/DVD
- Memoria Micro SD

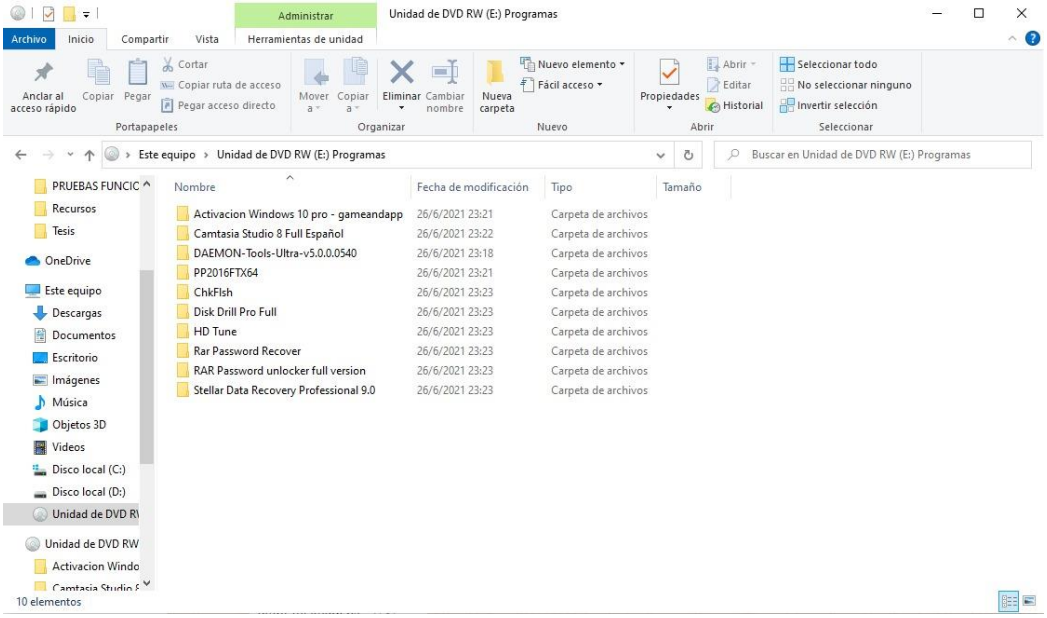
A continuación, se analizará la evidencia obtenida, el cual procederemos llenando el formulario FORM N° 005 – Recuperación de Información (Ver Anexo 8: Recuperación de la Información), donde se analizará y se tendrá un control de la información obtenida de los discos DVD's.

Ilustración 34: Evidencia fotográfica de los discos

Fuente: Elaboración propia

Procederemos a ver el contenido de los discos a simple vista. El primer disco que lleva por nombre "Programas" contiene instaladores de softwares.

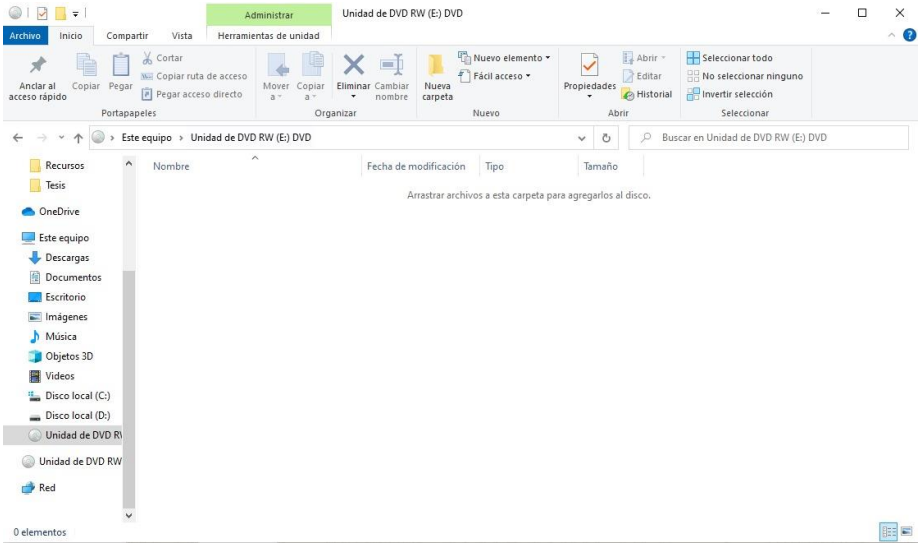
Ilustración 35 : Contenido del primer DVD "Programas"



Fuente: Elaboración propia

El segundo disco está completamente vacío

Ilustración 36: Contenido del segundo DVD



Fuente: Elaboración propia

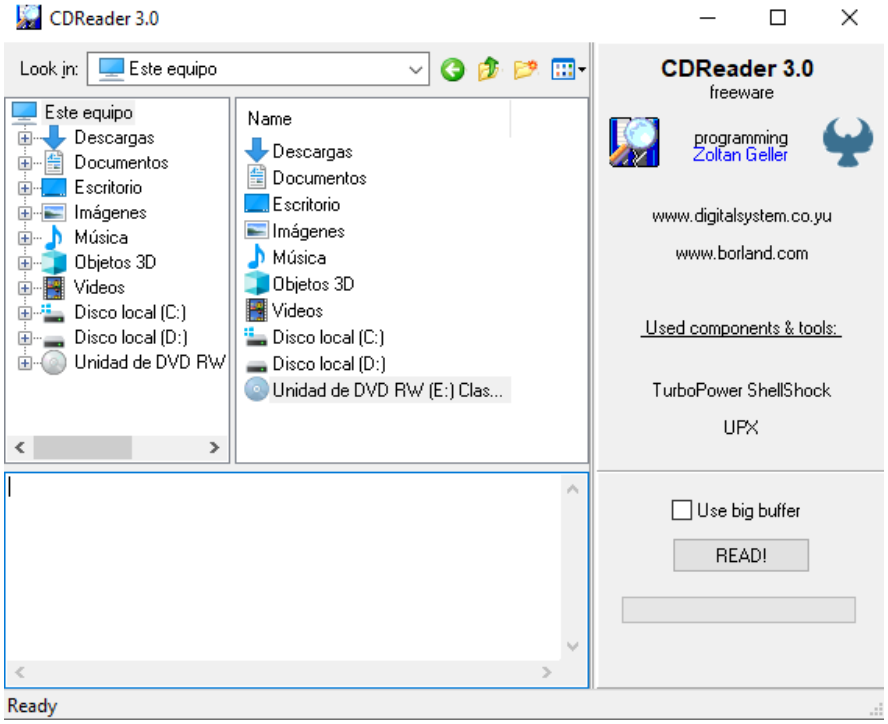
y el tercero se encuentra rayado, el cual se muestra a continuación.

Ilustración 37: Disco Rayado

Fuente: Elaboración propia

Como primer paso verificaremos la integridad interna del disco rayado, el cual se hará utilizando el programa "CDReader".

Ilustración 38: Interfaz del programa CDReader

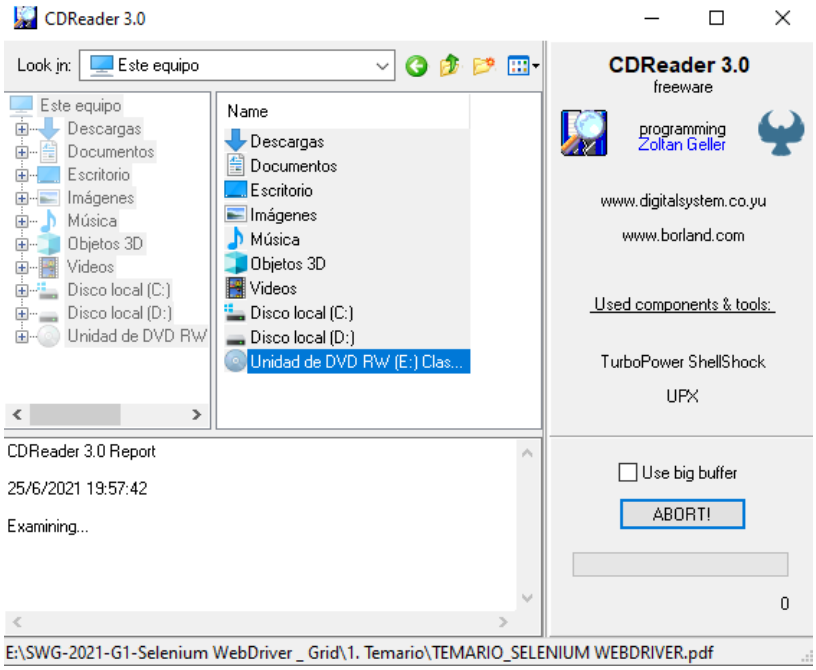


Fuente: Elaboración propia

- Al introducir el disco, se nos mostrará en la parte izquierda, el cual lleva por nombre "Unidad de DVD RW (E:) Clases Selenium".

- Lo seleccionamos y hacemos click en “READ!”, empezará el de análisis del disco.

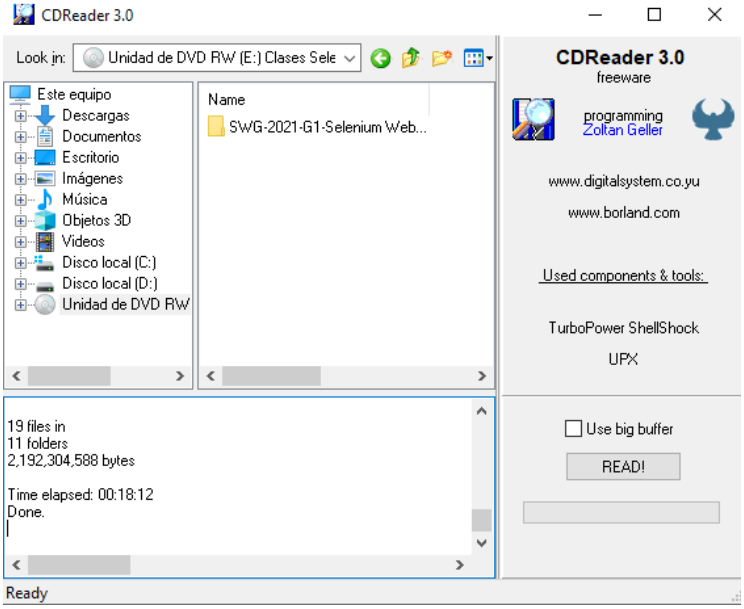
Ilustración 39: Selección de unidad a analizar



Fuente: Elaboración propia

- Una vez terminado el proceso de análisis del disco, se nos mostrara una ventana el resultado, el cual nos dice que contiene 19 archivos almacenados en 11 carpetas, cuyo tamaño total es 2.192 GB (2,192,304,588 bytes).

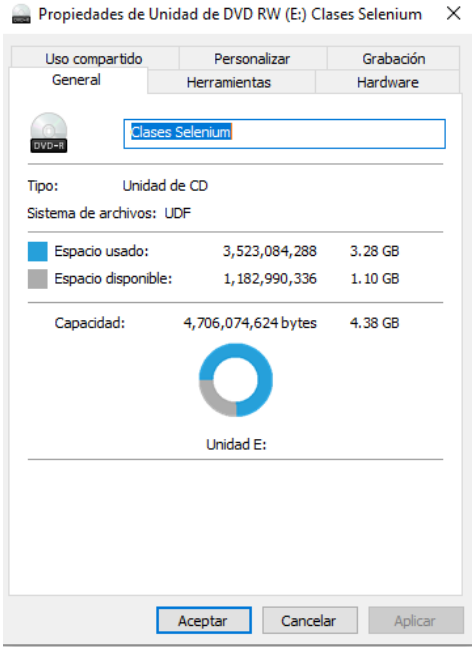
Ilustración 40: Resultado del análisis del DVD rayado



Fuente: Elaboración propia

- En conclusión, solo 2.192 GB puede ser recuperado del contenido total del disco que es 3.28 GB.

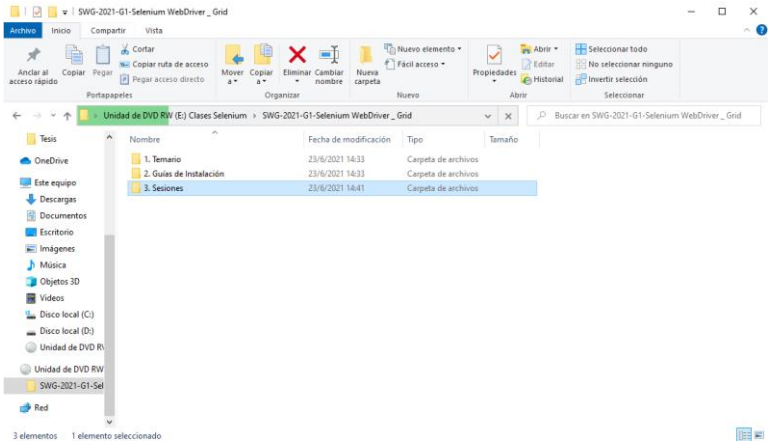
Ilustración 41: Espacio usado del disco rayado



Fuente: Elaboración propia

Después de analizar la integridad del disco, al querer visualizar su contenido, el explorador de archivos no nos permite abrir la información que se encuentran en las carpetas que se muestran en la imagen, por la misma condición en la que se encuentra el disco.

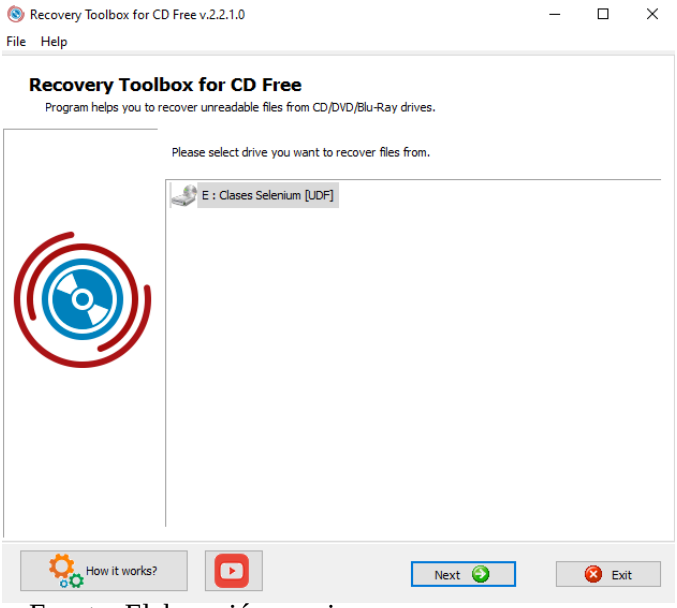
Ilustración 42: Contenido del disco rayado



Fuente: Elaboración propia

Para poder ver su contenido, utilizaremos el programa Recovery Toolbox for CD, el cual nos permitirá recuperar la información almacenada en el disco rayado.

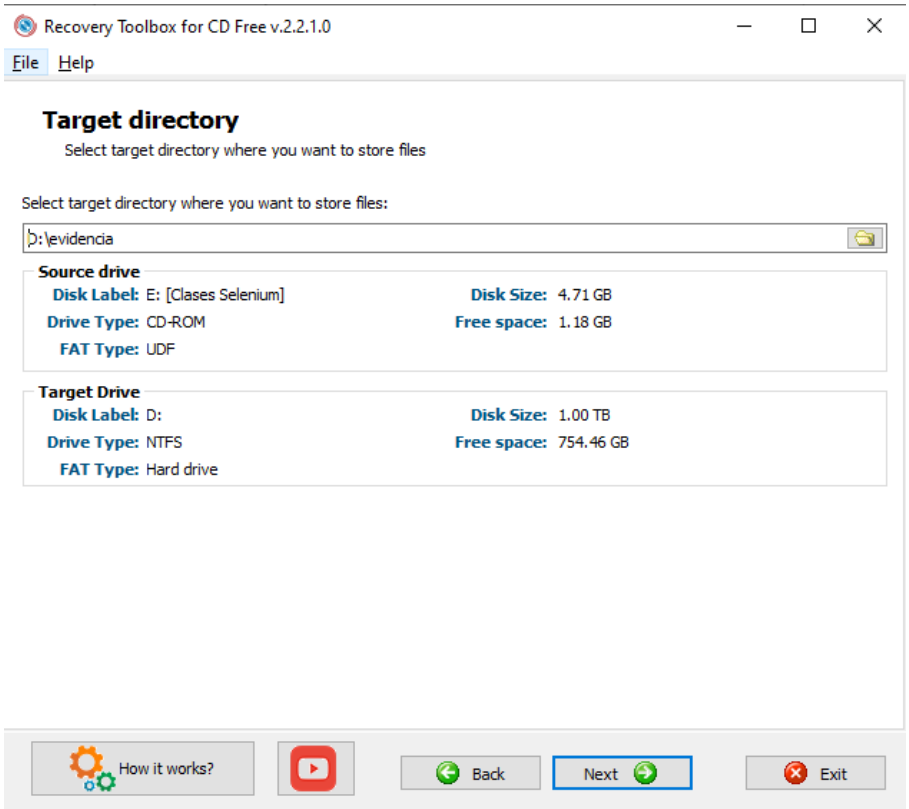
Ilustración 43: Interfaz del programa Recovery Toolbox for CD



Fuente: Elaboración propia

- Escogemos el disco a recuperar, en este caso será el disco que lleva por nombre "Clases Selenium", seleccionamos "Next" y nos aparecerá un cuadro en donde "Source drive (unidad de origen)" nos detalla la información del disco, el cual contiene: Disk label (etiqueta del disco), Drive type (tipo de unidad), FAT type (tipo de tabla de asignación de archivos), Disk size (tamaño del disco) y free space (espacio libre).
- Target Drive es el destino donde se almacenará la información, en este caso lo almacenaremos en la unidad D, en la carpeta "evidencia".

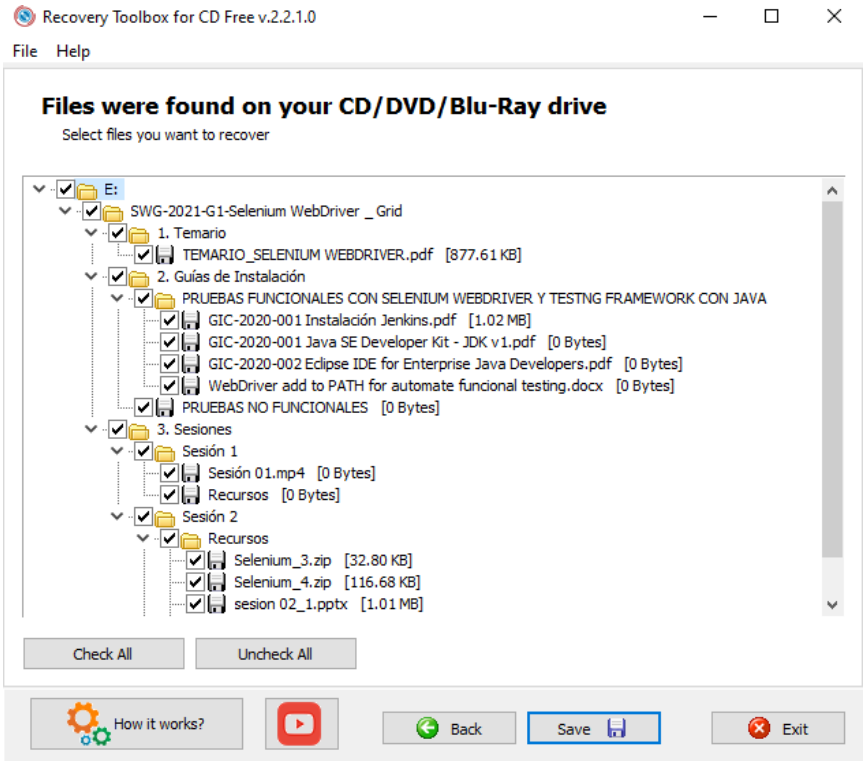
Ilustración 44: Ruta de destino para la información recuperada



Fuente Elaboración propia

- A continuación, nos mostrara todo el contenido del disco, seleccionamos todo y le damos en “Save”.
- Se puede apreciar que algunos archivos aparecen con 0 bytes, eso quiere decir que esos archivos no se pueden recuperar.

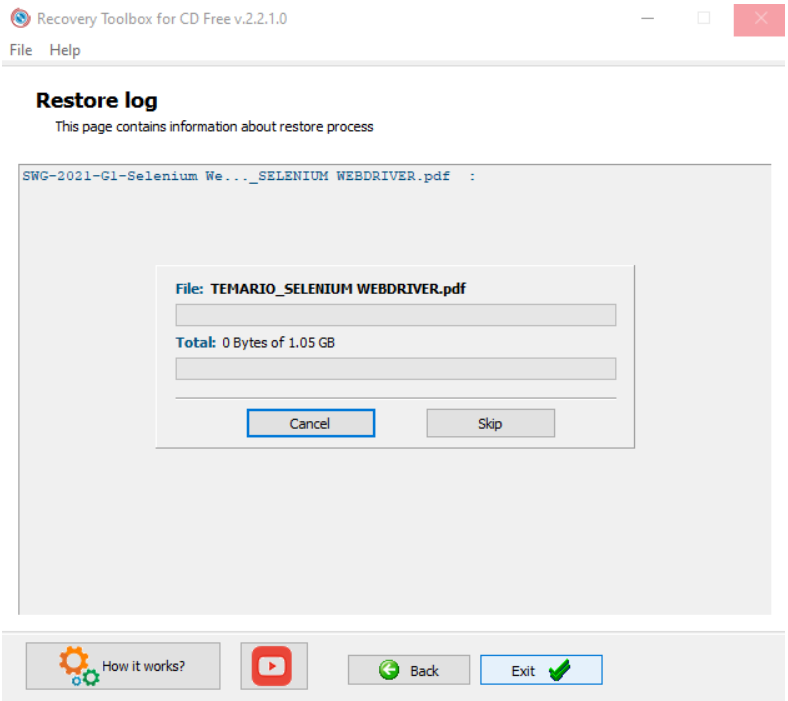
Ilustración 45: Interfaz de programa mostrando el contenido del disco



Fuente: Elaboración propia

- Nos aparece una ventana donde nos mostrará el proceso de restauración.

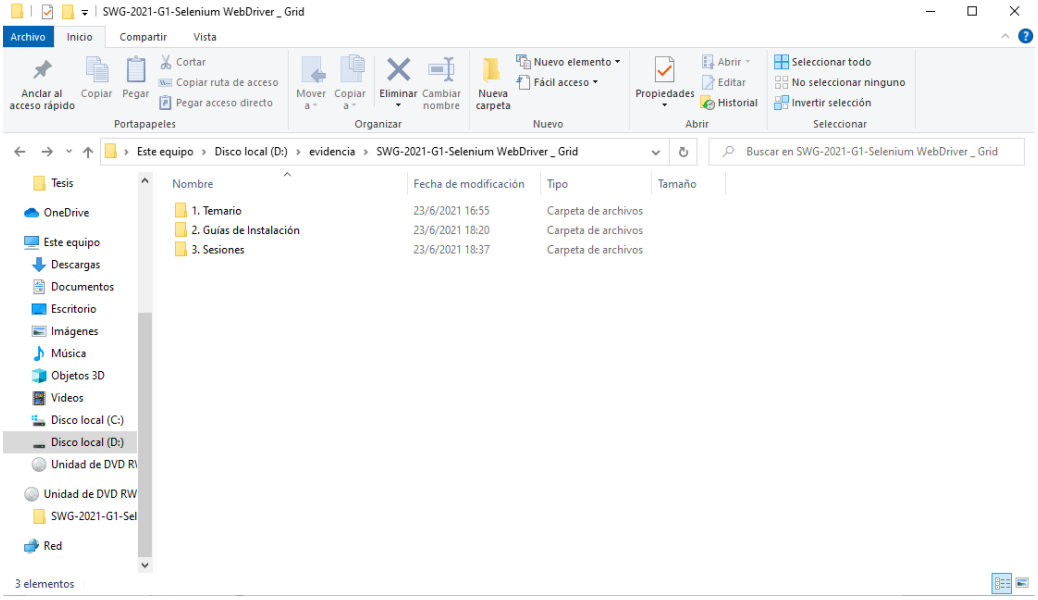
Ilustración 46: Interfaz de proceso de restauración



Fuente: Elaboración propia

- Una vez finalizada el proceso de recuperación, nos dirigiremos a la ruta donde se almacenó la información para visualizar su contenido.
- Un aproximado del 67% de todo el contenido del disco se puro recuperar.

Ilustración 47: Visualización del contenido recuperado



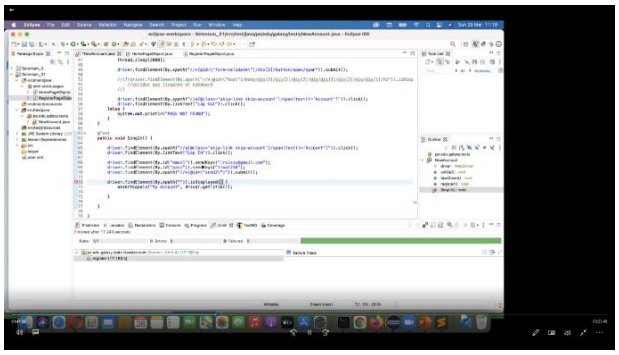
Fuente: Elaboración propia

- Al analizar el contenido de las carpetas, vemos varios archivos. A continuación, se muestran imágenes referenciales del temario y de un video de las sesiones.

Ilustración 49: Evidencia recuperado 1

Fuente: Elaboración propia

Ilustración 48: Evidencia recuperada



Fuente: Elaboración propia

- Se confirma que, en los discos encontrados, el disco rayado contiene archivos Word, PDF, PPT, archivos RAR y sesiones de video de las clases.

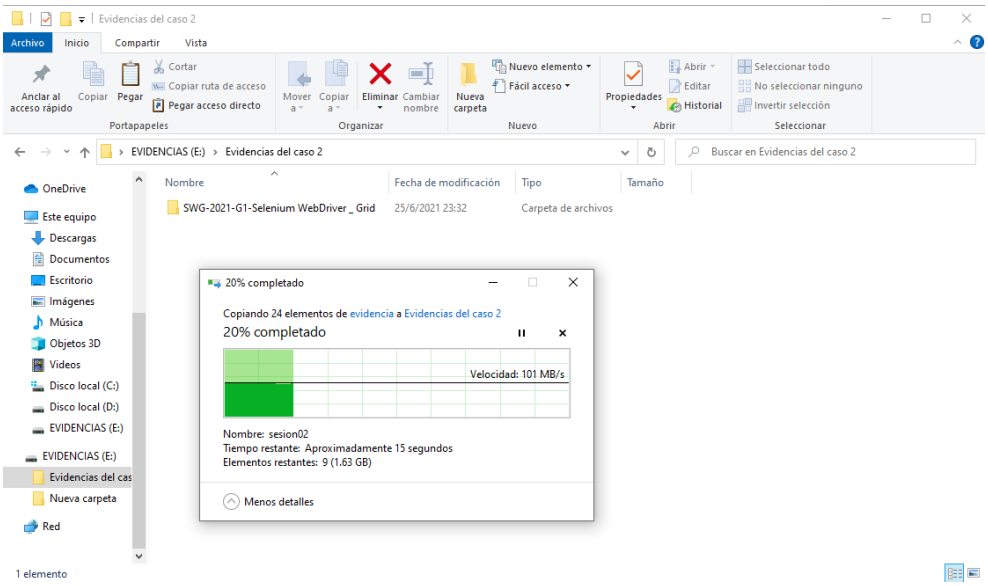
3.1.4.3. Preservación

En esta etapa se debe proteger toda la información recuperada por lo cual se procederá a realizar copias de seguridad, las cuales serán almacenadas en dispositivos extraíbles para mantener su integridad y posteriormente realizar su respectivo análisis.

Para este caso, toda la evidencia recuperada será almacenada en un disco duro externo de marca TOSHIBA con capacidad de 1 TB de almacenamiento, que lleva por nombre "EVIDENCIAS.

Solo en responsable forense debe tener acceso a la evidencia, registrándose en todo momento cada movimiento que se realice. Esto se hará llenando el formulario FORM N° 006 – PRESERVACIÓN (Ver Anexo 9: Preservación).

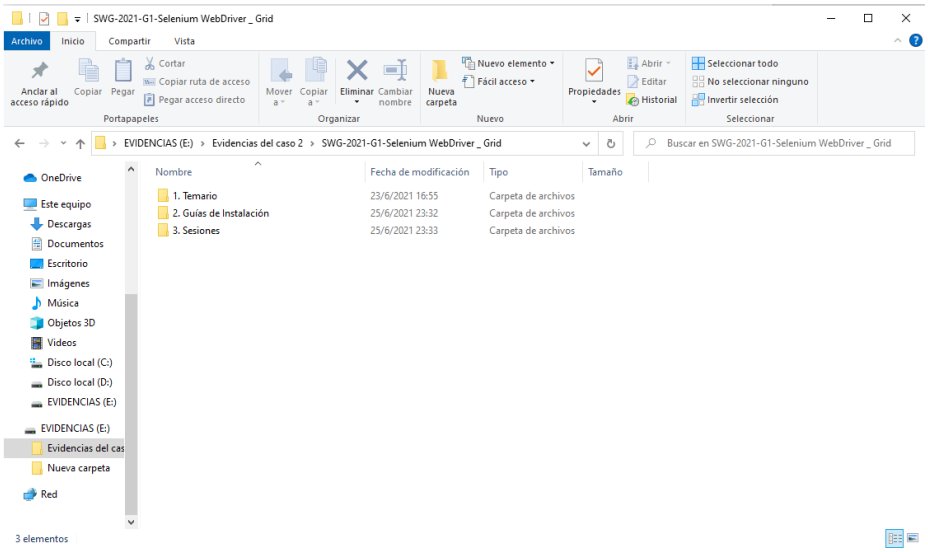
Ilustración 50: Copia de seguridad en disco duro



Fuente: Elaboración propia

Podemos confirmar que la información esta almacenada con éxito para posteriormente realizar su análisis.

Ilustración 51: Resultado de la copia de seguridad



Fuente: Elaboración propia

3.1.4.4. Análisis

Una vez realizada las copias de seguridad, procederemos a analizar la evidencia. Para ello se llenará el formulario FORM N° 7 – Análisis de la evidencia (Ver Anexo 10: Análisis de la Evidencia

<u>Paso 1</u>

Analizamos el contenido del primer disco que lleva nombre “Programas” el cual contiene instaladores de softwares utilizados por la institución.

Analizamos el contenido del segundo disco el cual se encuentra completamente vacío.

Al querer analizar el contenido del tercer disco, se puede apreciar que físicamente el disco se encuentra malas condiciones (rayado) por lo cual se requiere de programas para analizar su estado interno y su contenido.

<u>Paso 2</u>

Analizamos la integridad del disco DVD rayado que lleva por nombre “Clases Selenium” utilizando el programa “CDReader 3.0”, el cual nos mostró que contiene 19 archivos almacenados en 11 carpetas, cuyo tamaño total es 2.192 GB (2,192,304,588 bytes).

Paso 3

Para poder acceder a la información del disco rayado se utilizó el programa Recovery Toolbox for CD, el cual nos permitió recuperar aproximadamente el 67% de 3.28 GB, que es lo que contiene originalmente el disco.

Dentro de los archivos recuperados encontramos archivos PDF, Word, PPT, RAR y videos en formato mp4.

3.1.4.5. Presentación

Una vez interpretada toda la evidencia obtenida, procederemos a realizar el informe final.

INFORME FINAL	FORM N° 008
	FECHAS: 30/05/2021

N° de Expediente: EXP002

- *Precedente*

Descripción del incidente

Se produce un incidente en una institución dedicada al rubro de educación y certificación en tecnología de información.

Dicha empresa decide contratar servicios para investigar al jefe del área académica, por la supuesta venta ilegal de videos de las diferentes clases dictadas de manera virtual.

La institución sospecha que estos videos los estaba almacenando en DVD's, los cuales estaban camuflados en discos con los softwares utilizados por la institución.

Objetivo

Se contratan los servicios de investigación para obtener las pruebas necesarias para incriminar del jefe del área academia por la venta ilegal de los cursos.

- *Tareas Realizadas*

Descripción de la evidencia:

A continuación, nombraremos los archivos encontrados en los discos DVD tras los diferentes análisis.

- La primera carpeta que lleva por nombre “Temario”
- Se encontró un documento PDF
- La segunda carpeta que lleva por nombre “Guías de Instalación”.
- Se encontró una carpeta recuperada que contiene 3 archivos PDF y un Word.
- Se encontró una carpeta no recuperada
- La tercera carpeta que lleva por nombre “Sesiones”
- Se encontró 3 carpetas:
    - Sesión 1: un archivo no recuperado y un video
    - Sesión 2: una carpeta con 2 archivos RAR y 2 PDF, y un video
    - Sesión 3: una carpeta vacía y un video

Descripción de las herramientas utilizadas:

A continuación, se menciona los programas utilizados para el análisis del disco DVD:

- CDReader 3.0

Programa utilizado para analizar la integridad del DVD rayado.

- Recovery Toolbox for CD

Programa utilizado para recuperar información del disco rayado.

Descripción de la información obtenida

En la Carpeta “Temario” encontramos un archivo PDF con nombre “TEMARIO_SELENIUM WEBDRIVER”, el cual contiene los temas que se desarrollaran en cada sesión del curso.

- En la carpeta “Guías de Instalación” encontramos 2 archivos:

- El primer archivo es una carpeta que lleva por nombre “PRUEBAS FUNCIONALES CON SELENIUM WEBDRIVER Y TESTNG FRAMEWORK CON JAVA”, el cual contiene 3 archivos PDF y un archivo Word los cuales no fueron recuperados en su totalidad.
- El segundo archivo que lleva por nombre “PRUEBAS NO FUNCIONALES” no se logró recuperar su contenido.

  - En la carpeta “Sesiones” encontramos 3 carpetas:

- En la carpeta “Sesión 1” encontramos dos archivos que no se lograron recuperar su contenido.
- En la carpeta “Sesión 2” encontramos un video en formato mp4, el cual es la grabación del desarrollo de la clase, una carpeta que lleva por nombre “Recursos”, la cual contiene dos archivos RAR con códigos fuentes utilizados como ejemplos en las sesiones. Además, se encontraron dos archivos PPT con la explicación de las clases.

  - En la carpeta “Sesión 3” encontramos una carpeta vacía y un video en formato mp4, el cual es la grabación de una clase.

- *Resultado Final*

Teniendo en cuenta la evidencia obtenida y analizada, podemos afirmar lo siguiente:

- El disco DVD rayado con nombre “Clases Selenium” contiene archivos Word, PDF, PTT, RAR y videos de las clases dictadas por la institución.
- Podemos suponer que los archivos no recuperados en la carpeta “Guías de Instalación” contiene nombre y enlaces para la descarga de los programas utilizados en el desarrollo del curso.
- No se logró recuperar toda la información del disco debido al daño físico en la que se encontraba.

Podemos concluir que se logró obtener información del disco rayado que tenía como finalidad ser distribuida de manera no autorizada por la empresa, siendo esto para beneficio propio del acusado. Esto es considerado un delito menor, el cual está penado bajo la ley de Delitos Informáticos (LEY N° 30096) – Capítulo VII (Disposiciones Comunes) – Artículo X (Abuso de mecanismos y dispositivos informáticos), la cual indica que la venta, distribución o facilidad de programas o datos informáticos ilegalmente es penado ante la ley con una condena no mayor a 4 años y una multa de 90 días.

Con esta aclaración, el proceso aplicado a través de la metodología PURI llegaría con éxito a su fin.

ANEXOS DEL CASO 02

Anexo 6

Anexo 6: Ficha técnica de investigación

FICHA TÉCNICA DE INVESTIGACIÓN		**FORM N° 001** **Fecha: 14/05/2021**
DETALLES DEL INCIDENTE		
Personal Encargado	Nombre:	Enrique Castillo
	DNI:	7567876
	Cargo:	Suboficial
	Correo:	enrriquecast@hotmail.com
N° de Expediente:	EXP002	
Fecha del incidente:	13 de abril del 2021	
Descripción del incidente:	El gerente de una empresa dedicada el rubro de educación denuncia que un trabajador realiza ventas no autorizadas de cursos mediante DVD's.	
Persona responsable del acto delictivo	Nombre:	Juan Quiroz Valdiviezo
	DNI:	65897843
	Celular:	951371684
	Lugar de trabajo:	Capacitaciones Informáticas Oxford
	Área de Trabajo:	Oficina Académica
Datos del denunciante	Nombre:	Vladimir Campos Guerra
	DNI:	73589647
	Celular:	+51 967856478

Fuente: Elaboración propia

Anexo 7

Anexo 7: Identificación de las evidencias

IDENTIFICACIÓN DE LAS EVIDENCIAS		**FORM N° 002** **Fecha: 16/05/2021**
DETALLES DE LA INTERVENCIÓN		
Personal Encargado	Nombre:	Lorena Lluén Valiente
	DNI:	76475807
	Cargo:	Analista
	Correo:	Lluva@gmail.com
N° de Expediente:	EXP002	
Fecha de la intervención:	16 de mayo del 2021	
Lugar de intervención:	Domicilio del extorsionador (Mz.”C” Lte. 7 – Primavera)	
Persona intervenida	Nombre:	Juan Quiroz Valdiviezo
	DNI:	65897843
	Celular:	951371684
Objetos Incautados		
Objeto 01 **Código: OB001**	Equipo:	Laptop
	Modelo/Marca:	80KY/LENOVO
	Memoria:	4RAM
	Descripción del objeto:	Laptop LENOVO de color negra con carcasa negra y daño en la parte del cargador.
	Análisis:	SI [ ] NO [X]

Objeto 02 **Código: OB002**	Equipo:	Memoria USB
	Modelo/Marca:	SanDisk
	Memoria:	16 GB
	Descripción del objeto:	Memoria USB color Rojo y Negro 2.0
	Análisis:	SI [ ] NO [X]
Objeto 03 **Código: OB003**	Equipo:	DVD'S
	Modelo/Marca:	Max Plus
	Memoria:	4.38 GB
	Descripción del objeto:	3 discos DVD el cual uno se encuentra rayado en el área de grabación
	Análisis:	SI [X] NO [ ]
Objeto 04 **Código: OB004**	Equipo:	Memoria MicroSD
	Modelo/Marca:	Kingston
	Memoria:	16 GB
	Descripción del objeto:	Tarjeta SD color negro
	Análisis:	SI [ ] NO [X]

Fuente: Elaboración propia

Anexo 8

Anexo 8: Recuperación de la Información

RECUPERACIÓN DE INFORMACIÓN	**FORM N° 005** **Fecha: 20/05/2021**
N° de Expediente:	EXP002
Equipo de Trabajo	
Jefe de Equipo	Lorena Lluén Valiente
Analista	Erick Casas Villar
Dispositivos a Analizar	
Código de Equipo	OB003
Programas Utilizados	CDReader 3.0, Recovery Toolbox for CD
Procedimiento	Analizar el estado del dispositivo y recuperar la mayor cantidad información.
Información Obtenida	Tres carpetas contenedoras Archivos PDF, Archivos word, PPT, RAR, Videos MP4

Fuente: Elaboración Propia

Anexo 9

Anexo 9: Preservación

PRESERVACIÓN				**FORM N° 006** **Fecha: 22/05/2021**	
N° de Expediente:	EXP002				
Nombre	**Cargo**	**Dispositivo de Origen**	**Dispositivo de Respaldo**	**Fecha/Hora**	**Firma**
Lorena Lluén Valiente	Analista	DVD (Clases Selenium)	Disco Duro externo (Evidencia)	22/05 - 6:00pm	

Fuente: Elaboración propia

Anexo 10

Anexo 10: Análisis de la Evidencia

ANÁLISIS DE LA EVIDENCIA	**FORM N° 007**
	Fecha: 25/05/2021
Analista	Lorena Lluén Valiente
Cargo	Analista

Al realizar el análisis del dispositivo DVD rayado con los programas CDReader 3.0 y Recovery Toolbox for CD, se recuperaron los siguientes archivos:

Tres carpetas contenedoras

Carpeta 1. Temario: Contiene un archivo PDF con los temas que se desarrollará durante el curso

Carpeta 2. Guía de Instalación: Contiene una carpeta "PRUEBAS FUNCIONALES CON SELENIUM WEBDRIVER Y TESTNG FRAMEWORK CON JAVA" con tres archivos PDF y un Word que no se recuperaron con totalidad. El segundo archivo "PRUEBAS NO FUNCIONALES" no se logró recuperar

Carpeta 3. Sesiones: Encontramos tres carpetas, en la primera carpeta "Sesión 1" se encontró un archivo recursos y una video Sesión 01 (no se recuperó ningún archivo), en la segunda carpeta "Sesión 2" se encontró una carpeta "Recursos" con dos archivos RAR y dos archivos PPT referente a las clases y además un video de la Sesión 2 (Se recuperó toda la información), en la tercera capeta "Sesión 3" se encontró una carpeta "Recursos" (sin contenido) y un video de la Sesión 3 (se recuperó).

Fuente: Elaboración propia

Una vez realizado todos los procesos, podemos concluir que la aplicación de la informática forense con ayuda de la metodología PURI nos permitió obtener la evidencia necesaria que serán de suma importancia para la toma de decisiones en el ámbito judicial,

el cual se obtuvo a través de los diferentes programas aplicados para la verificación del estado del dispositivo óptico DVD, como también para la recuperación de archivos.

3.1.5. Propuesta económica del proyecto

Para la aplicación de la informática forense en la DIVINCRI de la ciudad de Chiclayo, se necesita realizar una inversión de hardware y software para poder realizar un correcto desarrollo de los casos de delitos informáticos. A continuación, se detallaron los costos en la siguiente tabla:

Tabla 20: Propuesta económica de Hardware

HARDWARE			
	Descripción	**Precio**	**Comentario**
Computadora de escritorio	S.O: Windows 10 Pro 64-bit Procesador: Intel Core i7-10700 CPU @ 2.90GHz (16 CPUs), ~2.9GHz RAM: 16 GB Almacenamiento: 1 TB HHD, 512 GB SSD	S/.5,000.00	Equipo utilizado para realizar las pruebas con los programas de recuperación y análisis de información
Laptop ASUS	S.O: Windows 10 Home 64-bit Procesador: --- RAM: 8 GB Almacenamiento: 1 TB HHD	S/.3,000.00	Equipo utilizado para realizar las pruebas con los programas de recuperación y análisis de información
Disco Duro Externo	Marca: Toshiba Interfaz: USB 3.0, 2.0 Almacenamiento: 1 TB	S/.130.00	Utilizado para almacenar evidencia digital.
USB	Marca: SanDisk Interfaz: USB 3.0, 2.0 Almacenamiento: 32 GB	S/.40.00	Utilizado para almacenar documentos e informes.
Lectora externa de CD/DVD	Marca: LG Interfaz: USB 3.0, 2.0	S/.120.00	Dispositivo utilizado para la lectura y escritura de discos CD/DVD
	Total	S/.8,290.00	

Fuente: Elaboración propia

La mayoría de los programas utilizados en el desarrollo de este proyecto son de licencia básica (versión gratuita), debido a que nos brindó las herramientas suficientes para poder obtener datos y evidencia digital. A continuación, se detallará los precios de los programas en sus versiones completas:

Tabla 21: Propuesta económica de software

SOFTWARE				
Programas	**Descripción**	**Sistema Operativo**	**Costo de licencia**	**Comentario**
Passware Kit Forensic	Desencripta archivos rar con contraseña	Windows y Mac	S/.5,027.16	Para el desarrollo del proyecto solo se requirió la licencia gratuita. Para una mejor funcionalidad del programa se requiere la compra del producto
Check Flash	Comprueba el estado de unidades flash USB.	Windows	Gratuita	
Stellar Data Recovery	Recupera cualquier tipo de información o archivo eliminado.	Windows y Mac	S/.784.00	Para el desarrollo del proyecto solo se requirió la licencia gratuita. Se recomienda la compra del producto, el cual brinda 3 licencias para 3 dispositivos diferentes por un año.
Disk Drill	Recupera cualquier tipo de archivo oculto como documentos, mensajes y archivos multimedia.	Windows, Linux y Mac	Gratuita	
CDReader	Verifica y comprueba el estado de los CD/DVD.	Windows	Gratuita	
Recovery Toolbox for CD	Recupera la mejor cantidad posible de información almacenada en CD, DVD o Blu-ray que estén dañados físicamente.	Windows	Gratuita	

Passware Kit Agent	Desencripta archivos rar con contraseña.	Linux	Gratuita	
F3	Código abierto que evalúa el estado de las memorias USB.	Mac	Gratuita	
CapacityTester	Prueba unidades USB o tarjeta de memoria para comprobar su integridad.	Linux	Gratuita	
Veeam Backup & Replication	Crea copias de seguridad (backup) y recupera todo tipo de información o archivo eliminado.	Linux	S/.320.89	Para una mejor funcionalidad del programa se requiere la compra del producto
R-Linux	Recupera archivos de manera rápida y confiable para la plataforma Linux.	Linux	Gratuita	
R-ESTUDIO	Recupera información completa almacenada en discos CD/DVD.	Windows, Mac y Linux	S/.717.98	Para una mejor funcionalidad del programa se requiere la compra del producto
	Total		S/.6,850.03	

Fuente: Elaboración propia

Tabla 22: Servicios

Servicios	Descripción	Costo
Internet	Costo anual (200mb) Alta velocidad.	S/. 1,800.00
OneDrive	Almacenamiento en la nube 2TB (anual).	S/.612.00
	Total	S/. 2,412.00

Fuente: Elaboración propia

Tabla 23: Costos y Presupuestos

Descripción	Costo
Software	S/.6,850.03
Hardware	S/.8,290.00
Servicios	S/. 2,412.00
Costo Total	17,552.3

Fuente: Elaboración propia

3.2. Discusión

Se elaboró satisfactoriamente la guía de procesos para la aplicación de la informática forense para la obtención de datos y evidencia digitales, sin comprometer la confidencialidad e integridad de las pruebas obtenidas que serán de utilidad la toma de decisiones en los casos de delitos informáticos.

La metodología PMI (Project Management Institute), utilizada en el artículo "Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana" (Proaño & Gavilanes, 2018), nos muestra los 5 procesos utilizados para la gestión de la evidencia digitales, las cuales son: identificar, obtener, extraer, custodiar e informar. Esta metodología es similar a la utilizada en el desarrollo de este proyecto (PURI), el cual nos brinda los pasos a utilizar para el tratamiento de la evidencia digital desde la identificación/extracción hasta la presentación del informe final.

Para la recuperación de datos y evidencia digital, Armilla, Panizzi, Etevoric, & Torres, (2019), plantean 7 etapas para el análisis y procesamiento de evidencia:

- Evaluación de escena, herramientas y equipamientos, dispositivos electrónicos: Estas etapas se comparan con la fase de identificación utilizada en el desarrollo de este proyecto de investigación, el cual es el inicio de toda investigación. Estas etapas especifican que después de evaluar la escena, se requiere el uso de herramientas y equipamientos que

permiten asegurar la integridad de la evidencia para cualquier tipo de dispositivo electrónico encontrado en la escena.

- Recolección, almacenamiento y transporte: Estas etapas se comparan con la fase de preservación utilizada en el desarrollo de este proyecto de investigación. Esta etapa resalta que se debe almacenar y registrar tanto la evidencia física como lógica, para así mantener su integridad y evitar cualquier tipo de perdida de información.
- Análisis: Esta etapa se compara con la fase de adquisición y análisis utilizada en el desarrollo de este proyecto de investigación. Esta etapa comprende las técnicas y herramientas utilizadas en la extracción de información para posteriormente realizar el análisis de su contenido, obteniendo la evidencia necesaria que certifique la culpabilidad del actor del crimen.
- Reporte: Esta etapa se compara con la fase de presentación utilizada en el desarrollo de este proyecto de investigación. En esta etapa se genera un reporte detallado de todo lo realizado en el desarrollo del caso para finalmente concluir si la persona acusada es culpable o no del acto delictivo.

En conclusión, la elaboración de guía de procesos ayuda a que los peritos se adapten cada vez más a los factores tecnológicos y a través de los diferentes programas y herramientas utilizados en el desarrollo del caso de estudio, permitan obtener datos y evidencias que serán de utilidad en la toma de decisiones.

Capítulo IV: Conclusiones

- Se elaboró la Guía de Procesos para la aplicación de la informática forense, por lo cual se tuvo que investigar diversas metodologías referentes a la recuperación de datos y evidencias digitales, en las cuales logramos diferenciar las ventajas y desventajas que ofrecen en cuanto a fase, procesos y facilidad de uso. La metodología que más se adaptó a la elaboración del proyecto según el criterio de selección fue la Metodología de PURI (Proceso Unificado de Recuperación de Información).
- Se utilizó diferentes programas para el desarrollo de los casos propuestos en este proyecto de investigación. Estos programas cumplían diferentes funciones, ya sea para verificar el estado de integridad del hardware como para recuperar información eliminada, oculta o no accesible por daños físicos en el dispositivo con la finalidad de obtener evidencia suficiente para poder obtener un resultado favorable en el proceso de investigación.
- Se desarrolló un procedimiento para el caso propuesto N° 01 utilizando 4 fases de la metodología PURI: Identificación, Adquisición, Análisis y Presentación, en el cual se explica paso a paso todo el proceso que se realizó en el hardware incautado teniendo como referencia la guía de procesos.
- Se desarrolló un procedimiento para el caso propuesto N° 02 utilizando 4 fases de la metodología PURI: Identificación, Preservación, Análisis y Presentación, en el cual se explica paso a paso todo el proceso que se realizó en el hardware incautado teniendo como referencia la guía de procesos.

- Para el desarrollo de la propuesta metodológica no se requiere de grandes inversiones de hardware y software, dado que muchas de las herramientas que se pueden utilizar son libres y gratuitas.

Capítulo V: Recomendaciones

- Se recomienda adquirir las licencias de los softwares en su versión completa para obtener mejores resultados más óptimos y confiables.
- Se recomienda adquirir servicios de almacenamiento en la nube para realizar backups de manera mensual de toda la información recuperada de los casos de delitos informáticos.
- Se recomienda capacitar al personal del área de delitos informáticos de la DIVINCRI sobre el uso de los diferentes programas y técnicas en la recuperación de datos y evidencia digital.

Bibliografía

AccessData. (2020). *accessdata.com*. Obtenido de exterro.com: https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager

Acurio, S. (2016). *Delitos Informáticos: Generalidades.* Obtenido de http://biblioteca.udgvirtual.udg.mx:8080/jspui/bitstream/123456789/599/1/Delitos%20Inform%C3%A1ticos.%20generalidades.pdf

Aguilera López , P. (2010). *Seguridad informática.* Madrid: Editorial Editex.

Anderson, D. (1997). *USB System Architecture.* MindShare, Inc.

Anonimo. (19 de Mayo de 2016). *Agencia Peruana de Noticias*. Obtenido de https://andina.pe/agencia/noticia-conoce-delitos-ciberneticos-son-los-mas-frecuentes-interactivo-667571.aspx

Areitio Bertolin, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Parainfo S.A.

Armilla, N., Panizzi, M., Etevoric, J., & Torres, L. (13 de Octubre de 2019). Buenas prácticas para la recolección de la evidencia. 2-8. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/63930/Documento_completo.pdf?sequence=1

Baca, G. (2016). *Introducción a la Seguridad Informática* (Vol. Primera Edición). México: Grupo Editorial Patria. Obtenido de https://books.google.com.pe/books?id=IhUhDgAAQBAJ&printsec=frontcover&dq=seguridad+informatica&hl=es-419&sa=X&ved=0ahUKEwjNtc7rjMPnAhUnIrkGHQAMAWkQ6AEIKDAA#v=onepage&q&f=true

Cacha Arana, C. M. (2019). *Peritaje Informático basado en una nueva metodología híbrida en 2M % J Ingenieros - Huaraz.* Grado de Ingeniero, Facultad de Ingenieía, Huaraz. Obtenido de http://repositorio.utp.edu.pe/bitstream/UTP/1008/1/Stevens%20Conde_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20Profesional_2017.pdf

Cartín, Q. (s.f.). *La diferenciación entre dato, información y conocimiento.* Obtenido de https://www.academia.edu/2767609/Dato_informacion_y_comocimiento

Cebrián Marín, D. (2015). *Sistemas de almacenamiento. IFCT0310.* Granada: IC Editorial.

Cherkes, M. (2017). *mikelab.kiev.ua*. Obtenido de http://mikelab.kiev.ua/index.php?page=PROGRAMS/chkflsh

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración* (Séptima Edición ed.). McGraw-Hill Interamericana.

Chicano Tejada, E. (2015). *Auditoría de seguridad informática. IFCT0109.* Málaga: IC Editorial.

Cleverfiles. (29 de Marzo de 2021). *cleverfiles.com*. Obtenido de https://www.cleverfiles.com/es/data-recovery-software.html

Colmenares, & Cruz. (2003). *Importancia de la Informática Forense.* Centro Universitario México AC, Ciudad de México. Obtenido de https://www.academia.edu/23975452/Informatica_forense

Corda, M. C., Viñas, M., & Coria, M. K. (s.f.). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su. *(Proyecto académico).* Universidad Nacional de La Plata, La Plata.

Crystal Dew World. (2021). *crystalmark.info*. Obtenido de https://crystalmark.info/en/software/crystaldiskinfo/

de la Cruz, F. (2017). *Aplicación de metodologías y herramientas de la informática forense para reducir el riesgo de la seguridad informática en la dirección nacional de comunicación y criminalística de la Policia Nacional del Perú - 2015.* Tesis para optener grado de maestria, Universidad Nacional Santiago Antunez de Mayolo, Escuela de PostGrado, Huaraz.

EFD Software. (2007). *efdsoftware.com*. Obtenido de hdtune.com: http://www.hdtune.com/

Ferro, J. (2020). *Investigación Criminal - Inspección Técnica en Criminología.* Obtenido de https://books.google.com.pe/books?id=6zHKDwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Ganivet Sánchez, J. (2017). *UF0926 - Diseño y organización del almacén.* Madrid: Editorial Elearning, S.L.

Garrido Buj, S., & Romero Cuadraro, M. (2019). *Fundamentos de gestión de empresas.* Madrid: Editorial Centro de Estudios Ramon Areces SA.

Gómez Vieites, Á. (2017). *Enciclopedia de la Seguridad Informática. 2ª edición.* Madrid: RA-MA.

Goméz, V. (2014). *Enciclopedia de la Seguridad Informática* (Vol. Segunda Edición (Actualizada)). Madrid: RA-NA. Obtenido de https://books.google.com.pe/books?id=Bq8-DwAAQBAJ&printsec=frontcover&dq=seguridad+informatica&hl=es-419&sa=X&ved=0ahUKEwjy29r1ocPnAhWxHLkGHU_dAs0Q6AEISDAE#v=onepage&q&f=false

Herrerías Rey, J. E. (2012). *El PC hardware y componentes.* Madrid: Anaya Multimedia.

Instituto Nacional de Ciberseguridad. (2016). Guía de almacenamiento seguro de la información. León, España. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

López Urrea, L. F. (2017). *INFORMÁTICA FORENSE* . Colombia: Shutterstock.

López, Amaya, & León. (2001). *Informática Forense: generalidades, aspectos tecnico y herramientas.* Bogotá. Obtenido de http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf

Marco Galindo, M. J., & Marco Simó, J. M. (2010). *Escaneando la informática.* Barcelona: Editorial UOC, S.L.

Martín, A. (2017). *Manual de Evidencia Digital* (Vol. Primera Edición). Independencia, Lima, Perú: Publimagen ABC sac. Obtenido de https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Oliva Haba, J. R., Martín Márquez, P. L., & Manjavacas Zarco, C. (2008). *Instalación y mantenimiento de equipos y sistemas informáticos.* Madrid: Paraninfo S.A.

Ortiz, E. (2019). *Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación Forense.* Obtenido de https://www.researchgate.net/publication/332786161_Evidencia_Digital_Fundamentos_aplicables_para_el_abordaje_de_la_Examinacion_Forense

Passware. (1998). *passware.com*. Obtenido de https://www.passware.com/kit-forensic/

Pérez Ríos, L., & Rodríguez Cabrera, J. (s.f.). Dispositivos de almacenamiento óptico. *(Trabajo de investigación).* Universidad de Las Palmas de Gran Canaria, Gran Canaria.

Picu, A. (21 de agosto de 2020). *endpointprotector.es*. Obtenido de https://www.endpointprotector.es/blog/que-son-las-amenazas-internas-y-como-puede-abordarlas/

Postigo Palacios, A. (2020). *Seguridad Informática.* Madrid: Ediciones Parinfo, SA.

Proaño, R., & Gavilanes, A. (30 de Marzo de 2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. 3-6. Obtenido de https://ingenieria.ute.edu.ec/enfoqueute/index.php/revista/article/view/229/201

Quizphe, G. X. (2015). *Metolología de la informática forense en la atención de delitos informáticos de cibergrooming.* Cuenca.

Ramírez, Z. (2008). *Sistema informático basado en algoritmos evolutivos para mejorar el proceso de identificación forense de evidencias digitales.* Proyecto de Investigación, Univesidad Católica Santo Toribio de Mogrovejo , Facultad de Ciencias, Chiclayo.

Rebollo, M. (2011). *Dispositivos de almacenamiento.* Universidad Politéctica de Valencia, Sistemas Informáticos y Computación, Valencia. Obtenido de https://riunet.upv.es/bitstream/handle/10251/13706/Dispositivos_de_almacenamiento.pdf

Recovery Toolbox Inc. (2003). *recoverytoolbox.com*. Obtenido de https://recoverytoolbox.com/es/cd.html

Roadkil. (17 de septiembre de 2010). *roadkil.net*. Obtenido de https://www.roadkil.net/program.php?ProgramID=29

Rodríguez, F., & Dómenech, A. (s.f.). La informática forense: El rastro digital del crimen.

Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., & Murillo Quimiz, Á. L. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* Pajan: Área de Innovación y Desarrollo S.L.

Rosa, O. (21 de Octubre de 2020). *El diario el cento del País* .

Ruiz Larrocha, E. (2017). *Nuevas tendencias en los sistemas de información.* Madrid: CENTRO DE ESTUDIO RAMÓN ÁCERES, S.A.

Salas, R. (2016). *Manejo y Validación de Evidencia Digital.* Universidad del Turabo, San Juan. Obtenido de https://www.academia.edu/19672138/MANEJO_Y_VALIDACION_DE_EVIDENCIA_DIGITAL

scotiabank. (s.f.). *scotiabank.* Obtenido de https://scotiabankfiles.azureedge.net/scotiabank-peru/PDFs/empresas/documentos/S1039.pdf?t=1600300800023

Softpedia. (2 de 10 de 2015). *Softpedia.com*. Obtenido de https://www.softpedia.com/get/System/Benchmarks/CDReader.shtml

Stellar. (2021). *stellarinfo.com*. Obtenido de https://www.stellarinfo.com/windows-data-recovery-professional.php?gclid=Cj0KCQjwhr2FBhDbARIsACjwLo1XBlSADp26NyoFpnxiSl7ZauWxzgPGxJ_FhJAGpuN_eXwGXeyUb_8aAoO8EALw_wcB

Tapia, P. (2017). *Implementación de metodología de análisis forense para la direción de tecnologías de información y comunicaciones de la armada del ecuador (DIRTIC).* Tesis para obtener grado de Maestría, Escuela Superior Politécnica del Litoral, Facultad de Ingeniería en Electricidad y Computación, Guayaquil.

Triana Fuentes, J. J., & Ballesteros Ricaurte, J. A. (s.f.). Evidencia forense digital en equipos de cómputo, redes y computación en la nube. *(Proyecto de investigación).* Universidad de Manizales, Manizales.

Vásquez Moctezuma, S. E. (2015). Tecnologías de almacenamiento de información en el ambiente digital. *e-Ciencias de la información*, 19.

Velázquez López, F. J., & Díaz Aguado, L. H. (2015). Cooperación en la formación entre Instituciones. *Monografía.* Instituto Nacional de Administración Pública, Madrid, España.

Viscano, Aide, & Baño. (s.f.). *Proceso Unificado de recuperación de información en SmartPhones.* Obtenido de http://www.ciiddi.org/congreso2014/images/documentos/proceso%20unificado%20de%20recuperacin%20de%20informacin%20en%20smartphones%20vizcaino.pdf

ANEXOS

Anexo 01: Ficha Técnica de Investigación

FICHA TÉCNICA DE INVESTIGACIÓN		***FORM N° 00 1***
		Fecha: 20/04/2021
DETALLES DEL INCIDENTE		
Personal Encargado	Nombre:	
	DNI:	
	Cargo:	
	Correo:	
N° de Expediente:		
Fecha del incidente:		
Descripción del incidente:		
Persona responsable del acto delictivo	Nombre:	
	DNI:	
	Celular:	
	Lugar de trabajo:	
	Área de Trabajo:	
Datos del denunciante	Nombre:	
	DNI:	
	Celular:	

Fuente: Elaboración Propia

Anexo 02: Identificación de las Evidencias

IDENTIFICACIÓN DE LAS EVIDENCIAS		***FORM N° 00 2***
		Fecha: ../../..
DETALLES DE LA INTERVENCIÓN		
Personal Encargado	Nombre:	
	DNI:	
	Cargo:	
	Correo:	
N° de Expediente:		
Fecha de la intervención:		
Lugar de intervención:		
Persona intervenida	Nombre:	
	DNI:	
	Celular:	
Objetos Incautados		
Objeto 01 **Código: OB001**	Equipo:	
	Modelo/Marca:	
	Memoria:	
	Descripción del objeto:	
	Análisis:	SI ☐ NO ☐

Fuente: Elaboración propia

Anexo 03: Adquisición de Información

ADQUISICIÓN DE INFORMACIÓN	***FORM N° 00 3***
	Fecha: ../../..
N° de Expediente:	
Equipo de Trabajo	
Jefe de Equipo	
Analista	
Dispositivos a Analizar	
Código de Equipo	
Programas Utilizados	
Procedimiento	
Información Obtenida	

Fuente: Elaboración propia

Anexo 04: Cadena de Custodia

CADENA DE CUSTODIA				***FORM N° 00 4***	
N° de Expediente:					
Nombre del Personal	Cargo	Código del Equipo Manipulado	Observación	Fecha/Hora	Firma

Fuente: Elaboración Propia

Anexo 05: Recuperación de Información

RECUPERACIÓN DE INFORMACIÓN	***FORM N° 00 5***
	Fecha: ../../..
N° de Expediente:	
Equipo de Trabajo	
Jefe de Equipo	
Analista	
Dispositivos a Analizar	
Código de Equipo	
Programas Utilizados	
Procedimiento	
Información Obtenida	

Fuente: Elaboración propia

Anexo 06: Preservación

PRESERVACIÓN				***FORM N° 00 6***	
				Fecha : ../../..	
N° de Expediente:					
Nombre del Personal	Cargo	Dispositivo de Origen	Dispositivo de Respaldo	Fecha/Hora	Firma

Fuente: Elaboración propia

Anexo 07: Análisis de la Evidencia

ANALISIS DE LA EVIDENCIA	***FORM N°007***
	Fecha : ../../..
N° de Expediente:	
Equipo de Trabajo	
Analista:	
Cargo:	

Fuente: Elaboración propia

Anexo 08: Informe Final

INFORME FINAL	*FORM N°008*
	FECHAS

N° de Expediente:

1. **PRECEDENTE**
    a. Descripción del incidente
    b. Objetivo
2. **TAREAS REALIZADAS**
    a. Descripción de la evidencia
    b. Descripción de las herramientas utilizadas
    c. Descripción de la información obtenida
3. **RESULTADO FINAL**
4. **REFERENCIAS**