OFICINA DE POSGRADO

Tema:

ANÁLISIS INFORMÁTICO FORENSE EN JUEGOS DE VIDEO EN LINEA Y SUS IMPLICACIONES CON DELITOS INFORMÁTICOS

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

Línea de Investigación:

PROTECCIÓN DE DATOS Y COMUNICACIÓN

Autor:

Andrea Fernanda Choto Tuquerres

Director:

Ing. Edgar Fernando Solís Acosta, Mg.

Ambato – Ecuador

Diciembre 2023

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ANDREA FERNANDA CHOTO TUQUERRES**, con cédula de ciudadanía **0605157023**, autor del trabajo de graduación intitulado: “ANÁLISIS INFORMÁTICO FORENSE EN JUEGOS DE VIDEO EN LINEA Y SUS IMPLICACIONES CON DELITOS INFORMÁTICOS”, previa a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD**, en la **OFICINA DE POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, diciembre 2023

Andrea Fernanda Choto Tuquerres

CC. 0605157023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

ANÁLISIS INFORMÁTICO FORENSE EN JUEGOS DE VIDEO EN LINEA Y SUS IMPLICACIONES CON DELITOS INFORMÁTICOS

Línea de Investigación:

Protección de datos y comunicación

Autor:

Andrea Fernanda Choto Tuquerres

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

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

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

Juan Carlos Acosta Teneda, P. PhD. f._____
OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villarroel, Dr. f._____
SECRETARIO GENERAL PUCESA

Ambato – Ecuador
Diciembre 2023

DEDICATORIA

El presente trabajo de titulación va dedicado primeramente a Dios por darme la oportunidad de cumplir con este objetivo.

A mi hijo en el cielo que ha sido mi inspiración para superarme cada día.

Finalmente dedico a mi familia que de una y otra manera han confiado en mí.

AGRADECIMIENTO

Agradezco a Dios por ser mi fortaleza en tiempos difíciles y darme sabiduría para culminar con las metas propuestas.

Así, también, agradezco a cada una de las personas que me apoyaron para alcanzar este objetivo, a mi hijo Mathias Andrés Pilatasig Choto (+) que su partida ha sido mi fuente de inspiración para seguir en mi preparación, a toda mi familia que han confiado en mí.

Finalmente, un agradecimiento a mis compañeros de estudio, y docentes por haber sido parte de mi proceso de formación.

RESUMEN

El presente trabajo de titulación permite identificar las vulnerabilidades que existe al hacer uso de los juegos de video y como estos implican en los delitos informáticos, la falta de conocimiento por parte de los usuarios de los videos juegos en línea es bajo relacionada con las buenas prácticas referentes a la seguridad en los datos que se comparten. Por lo tanto, es necesario realizar un análisis informático forense que permita conocer con exactitud, que datos se exponen en este tipo de juegos por parte de los usuarios. Esta investigación es importante porque permite tener conocimiento sobre las incidencias que tiene el compartir información en juegos en línea en la exposición a delitos informáticos. El objetivo de este trabajo es realizar un análisis informático forense en juegos de video en línea, que permita minimizar ataques con el propósito de adquirir información perteneciente a usuarios. Se aplica un proceso informático forense que consta de los siguientes pasos: identificación, preservación, análisis y presentación. La investigación es de campo, de tipo cuantitativa no experimental. Al finalizar el trabajo de investigación se espera mitigar los ataques informáticos al reducir la exposición de los usuarios a delitos informáticos que pueden presentarse en los juegos de video en línea.

Palabras claves: Análisis informático forense, video juegos en línea, delitos informáticos, vulnerabilidad, buenas prácticas en juegos de video, políticas en uso de video juegos.

ABSTRACT

The present titling work allows to identify the vulnerabilities that exist when using video games and how they imply in computer crimes, since the lack of knowledge on the part of the users of online video games is low related to the good practices regarding security in the data that is shared. Therefore, it is necessary to carry out a forensic computer analysis that allows to know exactly what data is being exposed in this type of games by users. This investigation is important because it allows us to have knowledge about the incidences that the sharing of information in online games has in computer crimes. The objective of this work is to carry out a forensic computer analysis in online video games, which allows minimizing attacks with the purpose of acquiring information belonging to users. A forensic computer process is applied that consists of the following steps: identification, preservation, analysis, and presentation. The research is field, of a quantitative non-experimental type. At the end of the research work, it is expected to mitigate computer attacks by reducing the exposure of users to computer crimes that can occur in online video games.

Keywords: Forensic computer analysis, online video games, computer crimes, vulnerability, good practices in video games, policies in use of video games.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE GRÁFICOS

ÍNDICE DE CUADROS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad los juegos de video en línea se han usado como un medio de entretenimiento, lo que implica la capacidad de utilizar el mismo para el cometimiento de actividades ilícitas y brinda un gran campo lleno de potenciales víctimas de ataques. Al hacer uso de estos juegos en línea los usuarios se ven obligados en compartir datos personales, en ciertos casos datos financieros, los mismos que son expuestos y utilizados por personas inescrupulosas. Se tiene como resultado la existencia de denuncias, que en ocasiones las personas afectadas toman la decisión de dejar pasar estos casos, por la falta de evidencias digitales y el número de trámites a realizar en este proceso, de la misma manera las personas que hacen uso de estas aplicaciones de entretenimiento son víctimas de mensajes ofensivos por no alcanzar las metas del juego. Adicionalmente existe desconocimiento por parte de los usuarios sobre los riesgos que existen al compartir datos, y las consecuencias que estos traen en un futuro, cuando los mismos son utilizados para otros fines.

Los usuarios no conocen sobre las seguridades que, se tiene al hacer uso de los juegos, el propósito del jugador es hacer uso de manera rápida el juego que se encuentra en el internet, y procede a instalar ciertos juegos de lugares no seguros e incluso sin leer las políticas que presenta para el uso del juego. Dentro de las políticas que se listan en ciertos juegos están: El acceso a la cámara, micrófono y demás documentos del equipo donde se va a instalar la aplicación de entretenimiento y en ciertos casos información de números de tarjetas de créditos o débitos para hacer el pago de este.

La falta de conocimiento de las seguridades en el uso de aplicaciones en internet, permite que los índices de delitos se hayan incrementado desde el año 2020 hasta el mes de Julio 2022 en 3183 delitos informáticos en Ecuador en las provincias Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay con más casos Pazan(2022). Esto permite que se generen amenazas las cuales devienen en un sinnúmero de delitos informáticos como: Phishing, grooming, engaños. Estas

amenazas, generan problemas como: robo de información, fraude a tarjetas de crédito, rapto, pornografía infantil (ya sea su producción o distribución). Los usuarios de juegos por lo general oscilan entre las edades de 35 a 44 años según la Asociación de Software de entretenimiento Duitama (2021), y se evidencia que en este grupo poblacional no hay una cultura que favorezca la protección de los datos, por lo tanto, se ven continuamente expuestos a delitos los mismos que para su solución requieren de una serie de procedimientos y denuncias que por su complejidad no siempre son aplicados.

En este contexto el problema de investigación es cómo se minimiza los niveles de delitos informáticos que se producen, por la falta de conocimiento sobre las seguridades que, se tiene que tomar en cuenta, en el manejo de los datos que se comparten en el uso de los juegos que se encuentran en internet.

Según la encuesta realizada por ESET, la industria de los videojuegos continúa expandiéndose y la evolución, sobre todo en algunos sectores, como son las plataformas de videojuego en la nube que tuvieron un gran crecimiento y que proyectan también un importante aumento en las ganancias. Asimismo, el número de nuevos gamers crece de manera sostenida desde 2015. Pero este crecimiento y expansión también atrae cada vez más a actores maliciosos, incluso a los grupos sofisticados como Lazarus, que robó cerca de 625 millones en criptomonedas de Axie Infinity. Todo esto muestra lo importante que es que la comunidad gamer adquiera hábitos seguros a la hora de jugar y esto es algo que se construye, porque lamentablemente la actividad de los cibercriminales es una constante.

El objetivo de este proyecto de desarrollo es determinar vulnerabilidades relacionadas con los delitos informáticos en video juegos en línea. Con esto se logrará la generación de políticas de buenas prácticas de acceso a video juegos con el propósito de asegurar la información del usuario. La investigación es de campo, de tipo cuantitativa no experimental. Esta investigación es importante realizarlo, no existe un análisis forense que permita tener conocimiento sobre las incidencias que se presentan al hacer uso de las aplicaciones de entretenimiento.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

En el presente capítulo, se analizan conceptos importantes que ayudan a comprender los procedimientos y pasos que conlleva realizar el análisis forense informático a un equipo utilizado para juegos en línea.

1.1 Estado de arte

En la actualidad se afirma que no existen trabajos relacionados con el análisis forense aplicado a los videojuegos en línea, por lo cual en esta investigación se va a realizar el proceso de análisis para determinar las vulnerabilidades existentes.

Actualmente se revisan investigaciones en videojuegos en consolas, por el autor Córdova (2018) en el cual presentan su versión de una metodología preliminar para el análisis forense de la información contenida en consolas *Xbox One*, son estas investigaciones dirigidas a video juegos en consola en específico. Para aplicar una metodología de Análisis Forenses basada en normativa legal ecuatoriana para el desarrollo en video juegos en línea se va a realizar a partir de UNE: 71506-3:2013, se encuentra una metodología aplicable al proyecto por lo que cuenta con los parámetros que garantizan los resultados requeridos, esta norma está dentro de las normas más aceptadas por peritos informáticos, así como la normativa legal requerida para dar validez a la Evidencia Digital.

Aunque existan estudios y ponencias sobre el Análisis Forense, se evidencia que no existe una metodología general aplicable a los videojuegos en línea, lo que dificulta que en el país se cuente con el conocimiento necesario y tampoco herramientas para realizar esta clase de Análisis Forense.

1.2 ANÁLISIS INFORMÁTICO FORENSE

Informática forense

Se define como “Una ciencia del área de la computación que ha surgido recientemente debido a la necesidad de entender los acontecimientos ocurridos

durante un evento o incidente relacionado con la seguridad informática en el cual ésta ha sido vulnerada por un atacante con el fin de afectar a dicho sistema ya sea en la modificación, destrucción, o robo de la información, por mencionar algunas acciones que afecta la integridad, confidencialidad o disponibilidad de un sistema, o el conjunto de ellos" (Guevara ,2018).

Con base a la definición anterior, la informática forense se describe como el análisis de datos digitales, los mismos que se les relaciona con delitos y el estudio de evidencias en casos judiciales.

Importancia de la informática Forense

La informática forense tiene por objetivo responder las siguientes preguntas: ¿cómo sucedió? ¿Cuáles fueron los activos informáticos vulnerados y comprometidos? ¿Cuáles fueron las causas? ¿Quién y cómo se ejecutó la vulnerabilidad? y ¿Qué información fue vulnerada? El ámbito de trabajo es post-mortem, lo que quiere decir que se realiza cuando ya ha pasado el incidente, asimismo es esencial para la resolución de conflictos en procesos judiciales en donde estén relacionados dispositivos de procesamiento y/o almacenamiento digital. (Gálvez, 2021)

Según Ealde (2021), el análisis forense informático tiene muchas utilidades. Más aun al tener en cuenta el aumento de las *ciber* amenazas para empresas y usuarios como consecuencia del mayor uso de la tecnología que se realiza en la actualidad en todos los niveles. Dentro de las actividades en las que son aplicadas las actividades en la informática forense se detallan a continuación:

Aportar evidencias en procesos judiciales: En casos de manipulación de discos duros, robo de datos o ataques de malware, el análisis forense sirve como una prueba esencial en un proceso judicial.

Ciberseguros: Los seguros ante ataques informáticos son cada vez más frecuentes. En este sentido, cuando se produce una brecha de seguridad es

necesario que un perito recopile evidencias para ver si ha de aplicarse o no el seguro. Es similar a lo que ocurre en la peritación de seguros de automóviles.

Predecir y prevenir ciberdelitos. Finalmente, la informática forense sirve para la predicción y prevención de ciberataques.

Tipos de Análisis Forenses

De acuerdo con la teoría, existen dos tipos de análisis forense general que dependen del estado en el que se encuentre el elemento que se prueba, a saber, el análisis en frío y el análisis caliente, como su nombre lo indica, el estado en frío se da porque el dispositivo se encuentra apagado y cuando el aparato o dispositivo está encendido o en un estado en reposo es el estado caliente (Cordova, 2018).

Análisis Forense en caliente

El análisis caliente se refiere a un tipo de análisis realizado cuando los equipos, dispositivos o componentes electrónicos de investigación están encendidos o en reposo mientras la policía recopila pruebas durante la fase de allanamiento.

Este procedimiento generalmente se realiza en computadoras y teléfonos inteligentes, debido a que el análisis antes mencionado tiene un software y generalmente implica revisar la información almacenada en la computadora, depende de la gravedad del delito que se investiga, no hay necesidad de romper contraseñas o sistemas de seguridad, que tienen diferentes métodos, como el análisis de la memoria no volátil o la memoria RAM.

Es importante que la evidencia se recolecte en orden de mayor a menor volatilidad de la información. Una secuencia de fluctuaciones es parte del período de tiempo en el que se dispone de cierta información, por lo que es necesario recopilar información que permanecerá por menos tiempo, es decir, información que fluctúa más (Cordova, 2018).

Análisis Forense en frio

El análisis realizado cuando la máquina, el dispositivo o los investigadores están apagados mientras la policía recopila pruebas durante la fase de búsqueda se denomina análisis forense en frío. Este procedimiento requiere más experiencia en el ámbito forense, se realiza una serie de pasos para no dañar la evidencia original y evitar que sea manipulada, lo que a su vez requiere de un software especializado para procesar la evidencia y obtener la información pertinente. Sirve como prueba digital incriminatoria.

Previo a la realización de procedimientos de análisis forense en frío, se asegura la integridad de la evidencia al realizar los pasos previamente requeridos por el buscador, y se siguen y aplican los procedimientos de cadena de custodia, la evidencia es recibida tal cual. Encontrado en una escena del crimen. No abra el dispositivo, siempre está cerrado, la evidencia es alterada si se abre.

Como regla general, no se utiliza la evidencia original respaldada por el repositorio, sino una copia de baja calidad, a menudo llamada imagen forense; al hacer una copia, utilice medios forenses limpios y utilice herramientas de software especiales para asegurarse de que la evidencia no se contamine (Cordova, 2018).

Herramientas para el Análisis Forense

Para el proceso de análisis forense se utilizan herramientas para descubrir evidencia digital. Las herramientas más comunes que son utilizadas para este proceso son las siguientes:

FTK Imager

Es una herramienta de vista previa de datos e imágenes que le permite examinar archivos y carpetas en discos duros locales, unidades de red, unidades de CD/DVD y ver imágenes forenses o el contenido de volcados de memoria.

Con FTK *Imager*, también se codifica archivos SHA1 o MD5, exportar archivos y carpetas de imágenes forenses al disco, ver y restaurar archivos que se han eliminado de la Papelera de reciclaje (a menos que se hayan sobrescrito sus bloques de datos) e instalar *Forensic*. Programa imágenes para ver su contenido en el Explorador de Windows. (Grupo Atico34, 2022)

Autopsy

Es una herramienta que ayuda en el análisis de evidencias digitales, esta herramienta es utilizada como principal para el desarrollo de análisis forense.
Autopsie como herramienta independiente, se considera una herramienta robusta para admitir todo tipo de casos, existen módulos adicionales para requisitos específicos. (Basis Technology, 2022)

OSForensics

OSForensics permite recuperar rápidamente evidencia forense de su computadora mediante la indexación y búsqueda de archivos de alto rendimiento. Identifica archivos y actividades sospechosos mediante la comparación de hash mediante la comparación de firmas de disco, correo electrónico, memoria y datos binarios. Administra sus investigaciones digitales y crea informes a partir de los datos forenses recopilados. (www.osforensics.com, 2018)

Estándares y metodologías para el Análisis Forense.

Actualmente, el análisis forense ofrece varios métodos propuestos por diversos autores y entidades, dentro de estas se tiene las siguientes:

- ISO 27037
- UNE: 71506-3:2013
- Metodología del Departamento de Justicia (DOJ) de los Estado Unidos.

ISO 27037

La Organización Internacional de Normalización (ISO) en el estándar ISO/IEC 27037 sirve principalmente como guía para la identificación, recopilación, adquisición y preservación de evidencia digital, no tiene un proceso de análisis de evidencia. Otro punto que sustenta este estándar es que el alcance global del estándar de seguridad informática ISO 27000 define los dispositivos y funciones que se utilizan en él, por ejemplo (dispositivos de almacenamiento masivo, teléfonos inteligentes, GPS, computadoras en red, etc.).

Sistemas de videovigilancia, etc.) El objetivo de lo anterior es siempre preservar la integridad de la prueba y utilizar métodos aceptables para promover su admisibilidad en cualquier procedimiento judicial. (Servicio de Acreditación Ecuatoriano, 2018)

Metodología del Departamento de Justicia (DOJ) de los Estado Unidos.

El modelo del DOJ (Eloff et al., 2008) no hace distinción entre los métodos forenses aplicados a computadores o a algún otro dispositivo electrónico. Intenta construir un modelo general para aplicarlo a la mayoría de los dispositivos electrónicos.

UNE: 71506-3:2013

Según la norma **UNE: 71506-3:2013**, el análisis forense se divide en cinco fases son estas: Fase de Preservación, Fase de Adquisición, Fase de Documentación, Fase de Análisis y la Fase de Presentación, a continuación, se detalla un resumen de cada fase:

Fase de Preservación: La prioridad es asegurar la integridad de la evidencia original en la escena del delito, es decir, en esta fase el Perito Informático se asegura y toma las medidas pertinentes para demostrar que no se realizaron

modificaciones, alteraciones o destrucción sobre dicha información para que pase a ser definida como evidencia.

Fase de Adquisición: Consiste en crear una imagen o clonado a bajo nivel de los datos originales del medio de almacenamiento.

Fase de Documentación: En esta etapa se documentará el procedimiento al completo, desde que se inicia el análisis, hasta que se envía el informe pericial al solicitante. Se documentarán todos los procesos llevados a cabo y las herramientas que se utilizaron, al seguir una secuencia temporal definida. En la cadena de custodia quedarán reflejados todos los pasos llevados a cabo durante el manejo de las evidencias.

Fase de Análisis: Una vez que el proceso de almacenar la Imagen Forense fue documentado correctamente, comienza la fase de análisis, donde el Perito Informático utilizara todo su conocimiento con el objetivo de hallar huellas de la información que requiere encontrar.

Fase de Presentación: Con esta fase se culmina el Análisis Forense y como resultado se obtendrá el informe final pericial con los resultados de todas las fases antes descritas.

1.3 JUEGOS DE VIDEO EN LÍNEA

Definiciones de Video Juegos

Se define como “Juegos electrónicos en los que están involucradas una o más personas que interactúan entre sí, es decir, es todo tipo de juego digital interactivo que su base principal es entretener y divertir por un lapso prolongado, se utilizan soportes de interfaz como los ordenadores, las videoconsolas, las consolas portátiles o máquinas recreativas" (Rodríguez, 2022).

Juegos en línea

Los juegos en línea describen cualquier videojuego que ofrece interacción en línea con otros jugadores, lo que distingue al juego es el nivel de interactividad que ofrece, la cantidad de información que comparten los jugadores y el número de personas con las que interactúan son dos factores clave que se consideran. (Internet Matters, 2023)

Cuadro 1. Tipos de juegos de video.

Clasificación	Descripción
Videojuego multijugador.	Dos o más jugadores interactúan simultáneamente, Este acceso suele ser en tiempo real o por turnos.
Videojuego de rol multijugador masivo en línea.	Los videojuegos de rol en línea competitivos presentan un estilo de juego profesional, y desempeñan roles en grupo o en solitario.
Videojuego de rol en línea competitivo.	Juego de rol que permite a miles de jugadores ingresar simultáneamente a un mundo virtual e interactuar entre sí a través de Internet.
Juegos en la nube.	Juegos en línea, que son almacenados en los servidores de la compañía de juegos y son transmitidos directamente a las computadoras con acceso al servidor a través del cliente. (es.wikipedia.org, 2021)

Fuente: elaboración propia

Juegos de video en línea más usados

Según el estudio realizado por Cejas (2022) se tiene como los juegos más usados para la plataforma PC: Dota2, *Call of Duty*, *Fortnite* y Fifa.

Peligros de juego de video en línea

Según AO Kaspersky Lab (2022) dentro de los peligros que se han dado al hacer uso de los juegos de video en línea, se tiene como:

Ciberacoso

Algunos jugadores aprovechan el cambio de identidad, para interactuar con personas de diferentes edades y condición social. Hay varias formas habituales de ciberacoso, directamente mensajes hirientes y dañinos a los jugadores, o enviar spam con comentarios despectivos sobre sus víctimas a canales de chat mundiales.

Generalmente, los jugadores antiguos utilizan los videojuegos para atraer y manipular víctimas más jóvenes. El resultado final son mensajes inapropiados, conversaciones mediante webcam o incluso encuentros en persona que llevan a la explotación sexual. Los juegos online dan la oportunidad a los usuarios de crear una especie de experiencia online compartida. Después de realizar un juego o una partida así llamada en los juegos los usuarios más antiguos crean un vínculo con los jugadores inexpertos o que recién inician y establecen un conjunto de experiencias comunes que conducen a más preguntas personales.

En muchos casos estos usuarios tienen la capacidad de consentimiento para adquirir más información personal e incluso chantajes en adquirir más experiencia a cambio de diferentes propuestas.

Usar el anonimato de los jugadores y los avatares para permitirles a los usuarios crear un alter ego o una versión ficticia de sí mismos es parte de la diversión. Sin embargo, también permite a los usuarios intimidar, acosar y, en ocasiones, molestar a otros jugadores.

Es difícil enjuiciar a los jugadores por acosar a otros o usar el juego para acosarlos de forma anónima. Algunos jugadores usan el juego para acosar a otros u obtener su información personal, como nombres de usuario y contraseñas. Incluso publicar información personal en línea que usan una táctica conocida como *doxeo*. El *doxeo* revela información no solo sobre los niños, sino también sobre sus padres, y puede convertirlos en víctimas de intimidación y acoso.

Los jugadores a menudo usan las redes sociales y las comunidades de juegos en línea para comunicarse con otros usuarios, obtener consejos y trucos, compartir estrategias, formar equipos y conectarse mientras juegan o ven jugar a otros. Estos tipos de comunidades en línea también son lugares donde los ciberdelincuentes causan daño.

Por ejemplo, publicar enlaces que parecen estar relacionados con un juego pero que en realidad son virus informáticos o malware (*software* diseñado para afectar, dañar u obtener acceso a una computadora). También ser lugares donde los depredadores intentan acercarse a los niños. (Departamento de Salud y Servicios Humanos de los Estados Unidos, 2021)

Problemas de privacidad

Al hacer uso de los juegos en línea se realizan todo tipo de conversaciones, de las que se adquieren informaciones personales.

Información personal que se deja en consolas y ordenadores de sobremesa
Otro peligro de los juegos *online* proviene de los propios ordenadores. Cuando han perdido su utilidad, los usuarios desechan estos equipos o las venden y a menudo no se percatan en eliminar los archivos e información personal, lo que, a su vez, pone en riesgo la información personal que es netamente es privada.

Es de gran importancia eliminar toda la información que, se tiene en los ordenadores, *tablets* a un estado de fábrica en el mejor de los casos, depende del tipo de dispositivo se utilizan las herramientas necesarias para la eliminación de la información. Además, algunos dispositivos incluyen zonas de almacenamiento que no se ven afectadas por las funciones de borrado del dispositivo. En el caso de ordenadores de escritorio o portátil, no confiar simplemente en la función de eliminado general sino realizar un proceso de formateo, estos no eliminarán los datos de la unidad.

Costos de juego en línea

Algunos juegos *online* utilizan el modelo gratis a ciertos módulos del juego, pero requieren de un pago para acceder a otras partes del juego. Existen juegos que requieren de un pago para que sea de uso libre de publicidad, estos pagos se los desarrolla mediante pagos en recargas o descuentos por tarjetas de crédito, débito, para hacer uso de varios módulos o tener más puntos en el juego.

En la mayoría de los casos, estos juegos requieren una tarjeta de crédito para registrarse y empezar a jugar, y el cargo se produce automáticamente si los usuarios deciden comprar nuevos artículos o servicios.

En la mayoría de los casos, estos juegos requieren una tarjeta de crédito para registrarse y empezar a jugar, y el cargo se produce automáticamente si los usuarios deciden comprar nuevos artículos o servicios. Existen usuarios menores de edad que sin adquirir autorización hacen uso de estos documentos sin saber el problema que los llevara como facturas con valores altos e incluso el robo de claves.

Malware

El programa maligno funciona en segundo plano, por lo que las víctimas no sospechan que su juego online es la fuente. Las aplicaciones parecieran legítimas o hacerse pasar por aplicaciones legítimas. Por lo tanto, es importante leer los comentarios, investigar a los desarrolladores y asegurarse de que cualquier aplicación es segura antes de descargar y se descarga aplicaciones procedentes de fuentes fiables. El dedicar tiempo necesario para instalar un analizador de antimalware, es importante a fin de que se revise periódicamente todos los dispositivos de uso.

Los ciberdelincuentes utilizan títulos de videojuegos populares y el atractivo del contenido gratuito para atraer a los usuarios y engañarlos para que descarguen software infectado con programa maligno. Esto lo hacen a través de publicaciones en redes sociales o mensajes directos, correos electrónicos de *phishing* o incluso

clasificaciones en motores de búsqueda o archivos *torrent*. El malware a menudo está diseñado para eludir los filtros de seguridad tradicionales, o los usuarios necesitarían desactivar el software *antimalware* por completo. También suelen pedir demasiados permisos de conducir.

El programa maligno también puede ocultarse en *mods*, es decir, otros archivos necesarios para seguir en el proceso de juego. En junio de 2021, se reveló que más de 3 millones de PC habían sido pirateadas por troyanos durante un período de dos años, distribuido principalmente a través de software y juegos pirateados, el programa maligno robó más de 1 millón de direcciones de correo electrónico únicas y 26 millones de credenciales de inicio de sesión, entre otras cosas. (Muncaster, 2022)

Adicional existen los siguientes problemas al hacer uso de los juegos de video:

Robo de dinero virtual en videojuegos

Los videojuegos tienen activos muy valiosos, como la moneda virtual o los *tokens*, o el árbol *Bodhi* que se usa en la realidad virtual. La codicia de los jugadores expertos en informática puede llevarlos a manipular las cuentas de otros jugadores para robar sus recursos, moneda virtual o, como se sabe, usar las tarjetas de crédito asociadas a sus cuentas para comprar bienes o servicios en videojuegos para ayudar a otros jugadores (ilegalmente). (Juan, 2021)

Comunicación en el uso de los juegos de video

Con el apogeo de los juegos multijugador, las personas pueden comunicarse con otras personas desconocidas mientras juegan. Este elemento social es a menudo lo que hace que los videojuegos tengan mayor nivel de interés para cada usuario y proporcionan beneficios sociales. Con el uso de los chats en línea se da la problemática de ataques verbales, es esto un problema en la sociedad por daños psicológicos que esto causa.

Según el artículo publicado por AO Kaspersky Lab (2023) se tienen los siguientes peligros de los juegos en línea:

El robo de identidad

Los ciberdelincuentes recopilan información de identificación personal para crear perfiles de posibles víctimas. Uno de los peligros potenciales de jugar juegos en línea con extraños es la función de chat que te permite hablar con otros jugadores. Los delincuentes usarían el chat para recopilar información confidencial, como su nombre, número de teléfono y dirección. Por eso es tan importante ser consciente de la información que compartes mientras juegas.

Correo electrónico de *phishing*

Los correos electrónicos de *phishing* o los enlaces de *phishing* distribuidos a través de chats de juegos en línea es otra forma en que los piratas informáticos engañan a las personas para que instalen malware de juegos en sus computadoras. Por ejemplo, parecer que un correo electrónico o chat proviene de una fuente legítima, lo que le solicita que descargue contenido adicional o visite una página de destino.

De hecho, estos correos electrónicos son falsos y maliciosos.

Filtración de datos

Los piratas informáticos atacan directamente a los editores de juegos. Si logran acceder a los sistemas de un editor, roba una gran cantidad de información, desde el código fuente de los juegos hasta la información personal almacenada en las cuentas de los usuarios. Un ejemplo famoso es la violación de datos de *Zynga*, donde un grupo de piratas informáticos robó información de inicio de sesión (nombres de usuario, contraseñas y direcciones de correo electrónico) para los juegos *Draw Something y Words With Friends*. Más de 172 millones de cuentas se vieron afectadas, lo que la convirtió en una de las filtraciones de datos más grandes de todos los tiempos.

Industria de los videojuegos y el alto riesgo de seguridad

Según ciberseguridad.com (2023) menciona que muchos juegos y foros de juegos tienen sitios web mal protegidos. Una empresa que crea un juego o un foro comienza con un presupuesto pequeño y simplemente no piensa en la seguridad porque no cree que sea necesaria. También elegir un servidor web que no cobre altas tarifas de seguridad. Alternativamente, es posible que las empresas de juegos no implementen medidas de seguridad muy simples, al comprar e instalar un certificado SSL o usar FTP para proteger su sitio web de ataques DDoS.

Grooming

Este tipo de ciberdelito incluye la violencia contra menores de edad por los adultos quienes se ganan la confianza con fines sexuales (Seguros Sura, 2019).

Windows como sistema operativo en juegos de video

Cuando se trata de PC para juegos, *Steam* está en la cima gracias a las encuestas de usuarios de hardware y software. En la plataforma de *Valve*, casi el 30 por ciento de los jugadores usan Windows 11 y ese número continúa en crecimiento cada mes. El 28,42% de los usuarios de *Steam* utilizan el nuevo sistema operativo, y este número crece (aunque muy lentamente) en la plataforma durante varios meses. Si se suma todo esto a nuevas unidades pres montados y portátiles que ya cuentan con este sistema básico, ayuda a escalar. Esto aumentaría significativamente entre el año 2024 y 2025. (Lerner, 2023)

Windows 11

Windows 11 es un sistema operativo de cliente construido sobre la base de *Windows* 10; *Windows* 11 ofrece innovaciones centradas en la productividad del usuario final y diseñado para admitir el lugar de trabajo híbrido actual. Se conserva su contribución a la gestión de dispositivos y actualizaciones. Las características de seguridad de la aplicación ayudan a evitar la ejecución de código

malintencionado o no deseado, ponen en cuarentena archivos de Office que no son de confianza y protegen contra sitios de *phishing* o programa maligno. (Mestew, 2023)

Windows 11 incluye funciones para juegos y videojuegos en los últimos modelos de PC. Como tal, necesitas una buena máquina para ejecutar los juegos más exigentes. *Windows* 11 hace que las máquinas se destaquen y sobresalgan en términos de gráficos, velocidad de juego, conectividad a Internet. *Microsoft* trae algunas de las funciones que se encuentran en las consolas *Xbox Series* X y Series S a *Windows* 11. El objetivo final, ejecutar videojuegos en la PC en las mejores condiciones. (Lópezlee, 2022)

Permisos de aplicaciones al ser instaladas

Según Microsoft (2023) las aplicaciones o juegos de Microsoft Store están diseñados para aprovechar ciertas funciones de hardware o software en su dispositivo *Windows*.

La aplicación tiene la capacidad de leer o escribir todos los archivos (incluidos documentos, imágenes y música) y configuraciones de registro que permiten que la aplicación realice cambios en la configuración del computador. Se usa cualquier dispositivo externo (como cámaras, micrófonos o impresoras) conectado a su dispositivo o parte de él sin previo aviso. También tiene acceso a la ubicación y usar las funciones de la plataforma, como el historial de ubicaciones, el diagnóstico de aplicaciones.

Descripción de funciones que se utiliza en las aplicaciones:

Información de la cuenta: Accede a cualquiera de la información de la cuenta.

Permitir elevación: Permite que la aplicación se ejecute con privilegios de administrador sin preguntar primero al usuario.

Diagnóstico de aplicaciones: Obtiene información de diagnóstico sobre otras aplicaciones en ejecución.

Bluetooth: Activa la conexión Bluetooth entre el dispositivo y otros dispositivos.

Calendario: Accede a los calendarios.

Historial de llamadas: Historial de acceso de llamadas telefónicas realizadas en el dispositivo, en *Skype* u otras aplicaciones de telefonía.

Contactos: Accede a los contactos, contactos o aplicaciones de libreta de direcciones.

Acciones de instalación personalizadas: Instala *software* adicional.

Correo electrónico: Accede a correo electrónico y a la información de la cuenta.

Reconocimiento facial: Activa y usa cualquier hardware de reconocimiento facial.

Sistema de archivos: Accede a los archivos y carpetas a los que tiene acceso y lee o escribe en todos sus archivos (incluidos documentos, imágenes y música).

Lector de huellas digitales: Activa y usa cualquier *hardware* del lector de huellas digitales.

Servicios del sistema local: Instala un servicio en el equipo que se ejecuta con privilegios máximos.

Ubicación: Activa y usa el GPS, Accede a los datos de ubicación Mapas y otras aplicaciones de ubicación.

Mensajería: Accede a los mensajes instantáneos e información de cuenta.

Micrófono: Se activa y usa el micrófono en el dispositivo.

Aplicación modificable: Habilita al usuario para modificar la aplicación.

Movimiento: Usa el acelerómetro u otra característica de detección de movimiento en el dispositivo.

Música biblioteca: Accede a cualquier archivo de música desde la Música de su dispositivo.

Comunicaciones de campo cercanas: Usa las conexiones de comunicaciones de campo cercano (NFC) entre el dispositivo y otros dispositivos.

Notificaciones: Accede a las notificaciones que se encuentran en el centro de acciones.

Servicios empaquetados: Instala un servicio en el equipo.

Corrección de compatibilidad de redirección de escritura de paquete: Permite que la aplicación cree, modifique o elimine archivos en la carpeta de instalación de la aplicación.

Biblioteca de imágenes: Accede a cualquier archivo de imagen desde la biblioteca de imágenes del dispositivo.

Tareas: Accede a su lista de tareas *Outlook* y otras aplicaciones de seguimiento de tareas.

Recursos no virtualizados: Escribe entradas del Registro y archivos que no se limpien al desinstalar.

Biblioteca de vídeo: Accede a cualquier archivo de vídeo desde la biblioteca de vídeo del dispositivo.

Reconocimiento de voz: Activa y usa cualquier hardware de reconocimiento de voz.

Cámara web: Usa la cámara en el dispositivo.

***WiFi*:** Usa conexiones *WiFi* entre el dispositivo, Internet y otros dispositivos.

Conexiones cableadas: Usa las conexiones cableadas, incluidas las comunicaciones Ethernet, USB y Serial entre el dispositivo, Internet y otros dispositivos.

1.4 DELITOS INFORMÁTICOS

Delitos Informáticos

Un delito informático es considerado a toda aquella acción perjudicial, que se da por vías informáticas o que tiene como objetivo destruir y dañar información en computadores, medios electrónicos y redes de Internet.

Los tipos de delitos informáticos presentes hoy en día se tiene: Delitos en contra de la confidencialidad, la integridad y la disponibilidad de los datos (Córdova, 2018).

La Organización de las Naciones Unidas (ONU), reconoce los delitos informáticos de acuerdo con una clasificación, esta se divide en secciones de acuerdo con el acto cometido. (Miguel, 2008)

Tipos de Delitos informáticos de acuerdo con la ONU

a) Fraudes cometidos mediante manipulación de computadoras.
    - Manipulación de los datos de entrada
    - La manipulación de programas
    - Manipulación de los datos de salida
    - Fraude efectuado por manipulación informática

b) Falsificaciones informáticas.
    - Como objeto
    - Como instrumento

c) Daños o modificaciones de programas o datos computarizados
    - Sabotaje informático
        - Virus
        - Gusanos
    - Bomba lógica o cronológica
        - Acceso no autorizado a servicios y sistemas informáticos
    - Piratas informáticos o hackers
        - Reproducción no autorizada de programas informáticos de protección legal

Además, existen otro tipo de delitos que se tipifican en función de la conducta, como:

a) Directamente contra los propios sistemas
    - Acceso no autorizado.
    - Destrucción de datos.
    - Infracción al *copyright* de bases de datos.
    - Interceptación de correo electrónico.
    - Estafas electrónicas.
    - Transferencias de fondos.

b) A través de la red de Internet
    - Espionaje.
    - Terrorismo.
    - Narcotráfico.
    - Tráfico de armas.
    - Proselitismo de sectas.
    - Propaganda de grupos extremistas

Normativa Legal en el Ecuador

Código Orgánico Integral Penal

COIP: Delitos Informáticos en Ecuador, Registro Oficial 180, 10-Feb-2014 “Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas**.” (Asamblea Nacional, 2014)**

Delitos contra la integridad sexual y reproductiva

Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos

Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. - La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.

Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años. La persona que suplanta la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.

Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos

Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. - La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales*, blogs, fotoblogs*, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años, será sancionada con pena privativa de libertad de siete a diez años.

Delitos contra el derecho a la intimidad y privacidad personal y familiar
Violación a la intimidad

Art. 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley

Intercepción ilegal de datos

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

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Tipos de delitos informáticos más cometidos en el Ecuador

Según (Redacción Seguridad, 2022) existen Cinco de estas categorías delictivas ocurren con mayor frecuencia en el país.

Estos incluyen: fraude en línea, invasión de la privacidad, acceso no autorizado a los sistemas informáticos, ataques a la integridad de los sistemas informáticos y apropiación indebida fraudulenta por medios electrónicos. Este último es el más común. Se configura cuando una persona utiliza de manera fraudulenta un sistema informático o una red electrónica para defraudar bienes ajenos, transferir dinero o bienes sin consentimiento en perjuicio de otro. Según el artículo 190 del Código Integral Penal (CPC), la pena es de prisión de uno a tres años. En concreto, la policía realizó 38 operativos para combatir estos delitos en dos años y medio.

Además, policías uniformados arrestaron a 39 personas sospechosas de cometer delitos cibernéticos durante este período. Por ejemplo, otra pandilla que se especializaba en fraudes en línea fue arrestada en 2021. Según las denuncias contra la organización, las víctimas perderán unos 100.000 dólares. La investigación reveló que tres personas recolectaron dinero de la estafa y lo depositaron en la cuenta del líder de la pandilla. Según un informe de inteligencia, las pandillas que roban dinero electrónicamente ganan entre $6,000 y $9,000 al mes.

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1 Caracterización de la Institución

En el presente proyecto es necesario realizar una investigación de campo, se va a recabar información de un grupo de jugadores, así mismo se va a adquirir una imagen forense sin alterar ningún dato para realizar el análisis informático forense y así analizar e identificar si, existe información relevante que esté relacionado con los delitos informáticos, cabe mencionar que para el presente proyecto no se va a considerar el cálculo de población y muestra para el estudio.

2.2 Metodología de Investigación

El proyecto de desarrollo es de tipo cuantitativa, se tiene las siguientes fases de investigación:

1. Recolección de datos, los mismos que se obtienen por medio del análisis forense al computador del que se van a adquirir la imagen forense.
2. Los datos recolectados de la imagen forense adquirida se van a realizar un análisis del resultado obtenido en la herramienta *Autopsy*.
3. Después de realizar el análisis se procede a sacar los resultados, estos son indicados que fueron vulnerados al hacer uso de los diferentes juegos en cada computador, este resultado se plasma en un informe.

En este proyecto se maneja el tipo de investigación no experimental, se basa en datos que no son manipulados, y la información que se obtiene en cada imagen forense no va a ser manipulado es en su estado real. Al contar con un computador que son analizados, es necesario realizar una investigación de campo, donde se procede a extraer una copia bit a bit de los equipos, para identificar procesos anormales en dichos equipos.

Técnicas y herramientas

La entrevista es una herramienta que se utiliza para recolectar los datos y mediante el uso de esta en la presente investigación ayuda a determinar los juegos más usados y de esta manera seleccionar uno, es este el que se va a analizar, esta entrevista se realiza a un grupo de jugadores, que tienen una experiencia amplia en el uso de los juegos de video en línea; además, se hace uso de una investigación bibliográfica para conocer sobre los juegos más utilizados y como estos implican vulnerabilidades.

Después de realizar una investigación sobre las diferentes herramientas especializadas que se utilizan para un análisis forense, para el desarrollo del presente trabajo se selecciona a *Autopsy* como una herramienta que permite realizar un análisis de evidencias obtenidas y FTK *Forensic Toolkit* que a través de sus utilidades permite realizar el proceso de extracción de una copia *bit* y a *bit* de la información almacenada.

Cuadro 2. Herramientas para la investigación.

Herramientas de análisis forense	**Descripción**	**Utilización**
Estación de trabajo forense	Windows 11	Estación de trabajo forense
FTK Imager 4.3.1.0	Visor de imágenes forenses/datos	Imágenes, hash, visualización de datos
Autopsy 4.17.0	Visor de imágenes forenses y analizador de datos forenses	análisis, visualización de datos

Fuente: elaboración propia

2.3 Metodología de Desarrollo

El análisis forense, se realiza a un computador que al momento es utilizado para distracción en el uso de juegos de video en línea y uso personal, este equipo es incautado para su análisis y de esta manera se determina los procesos que se realizan en el uso de juegos de video y así verifica si existe riesgos de filtración de información o la existencia de vulnerabilidades.

Para el análisis forense existen varias metodologías, de las cuales las más utilizadas por peritos informáticos son:

- UNE: 71505-3:2013
- ISO 27037
- Metodología del Departamento de Justicia (DOJ) de los Estado Unidos.

Cuadro 3. Comparación metodologías análisis forense.

No	**Metodología**	**Evaluación por fases del Análisis Forense**				
		Preservación	Adquisición	Documentación	Análisis	Presentación
1	UNE: 71505-3:2013	X	X	x	X	x
2	ISO 27037	X	x	x		x
3	DOJ	X	X		X	x

Fuente: elaboración propia

Para determinar el juego a analizar se realiza una entrevista, dado como resultado el juego más usado entre el grupo de 10 estudiantes universitarios, que se realizó la misma.

Después de realizar una investigación sobre los juegos de video más usados en la actualidad, se seleccionaron 10 juegos más destacados, de estos juegos se procedió a seleccionar los 3 primeros.

Para seleccionar el juego de estudio se procede a realizar una entrevista a 10 personas que hacen uso de los juegos más populares; De este proceso se determinó a Dota2 como el más utilizado de entre los jugadores.

Dota2

Dota2 es un videojuego de estrategia en tiempo real multijugador en línea entregado por la plataforma *Steam* con su subdivisión Valve *Corporation*.
Son considerados el fenómeno de la comunidad *gamer* llamados los juegos MOBA (*Multiplayer Online Battle* Arena) o DOTA 2 (*Defense of the Ancients*) necesita de gran comunicación y trabajo en equipo para lograr la victoria, además, la variedad de héroes la complejidad de las habilidades e infinidad de estrategias aseguran cada una de las partidas como únicas **(Sánchez & Torres, 2014)**.

Tabla 1. Juegos más usados.

Clasificación	Nombre Juego	Características
1	Dota2	Juego en equipos de 5 personas.
2	*Call of Duty*	Juego individual, en dúos, en tríos y en escuadrón.
3	*Fortnite*	Juego permite hasta a 100 personas participar juntas en una partida

Fuente: AO Kaspersky Lab (2022)

La norma UNE 71506/2013 es una norma que se ha elaborado para definir el proceso aseguir en el análisis forense en la gestión de evidencias electrónicas.
Según la norma UNE 71506/2013 está compuesta de las siguientes fases:

1. Preservación

En esta fase se pretende mantener en todo momento la validez y confiabilidad de las evidencias originales. Los peritos informáticos que realicen el primer contacto con las evidencias almacenarían éstas en los soportes adecuados, llevar la indumentaria adecuada para evitar descargas electrostáticas, usar soportes aislados para evitar interferencias externas y almacenar dichas evidencias de forma segura hasta el final del proceso pericial.

2. Adquisición

Durante la fase de adquisición se realiza un clonado a bajo nivel de los datos

originales, se sigue una serie de precauciones antes de adquirir dichos datos si el lugar del incidente está delimitado físicamente. Es importante el propio estado en el que se encuentran los sistemas, puesto que el proceso de adquisición no es el mismo si los sistemas están apagados que si están encendidos, en los que cualquier acción comprometería la integridad de las evidencias.

3. Documentación

En esta etapa se documentará el procedimiento al completo, desde que se inicia el análisis, hasta que se envía el informe pericial al solicitante. Se documentarán todos los procesos llevados a cabo y las herramientas que se utilizaron, se sigue una secuencia temporal definida. En la cadena de custodia quedarán reflejados todos los pasos llevados a cabo durante el manejo de las evidencias.

4. Análisis

Durante esta fase de análisis se van a llevar a cabo una serie de procesos y tareas que intentarán dar respuesta a preguntas relacionadas al evento que motivó la investigación. En términos generales, las acciones y procesos que van a llevarse a cabo durante esta fase son:

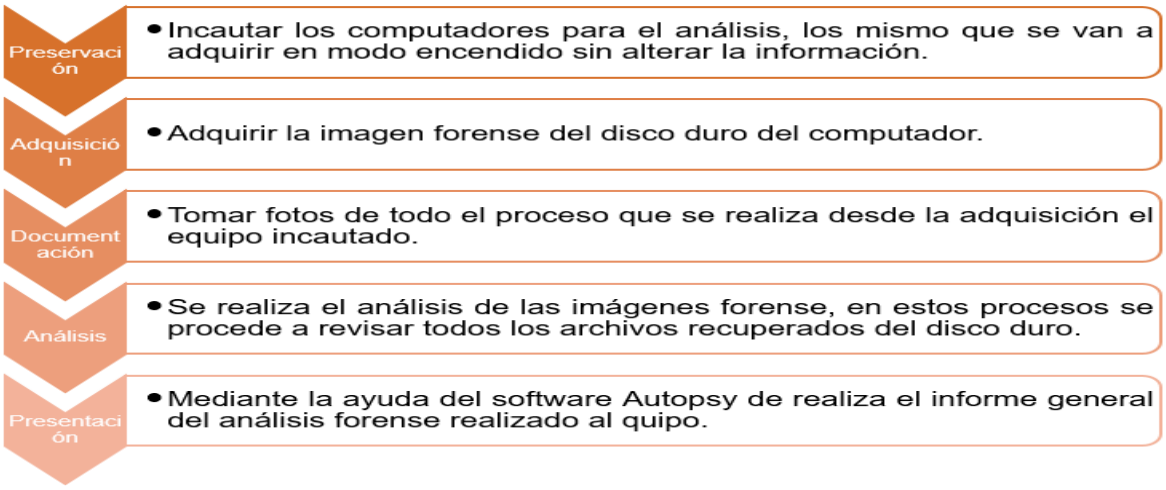
- Recuperación de ficheros borrados.
- Estudio de las particiones y sistemas de archivos.
- El estudio del sistema operativo.
- Estudio de la seguridad implementada en el sistema Análisis. detallado de los datos obtenidos.

5. Presentación

Durante la última fase se escribe un informe pericial con toda la información obtenida a lo largo del proceso de análisis. Dicho informe se escribe con un lenguaje inteligible para un público no técnico. Cuando el informe está finalizado, éste es remitido al organismo solicitante, junto al documento de control de

evidencias, para aportar una mayor trazabilidad al proceso. Al saber de las fases que contiene la norma UNE 71506/2013, se considera las siguientes actividades en el presente proyecto:

Figura 1. Generación de la cadena de custodia

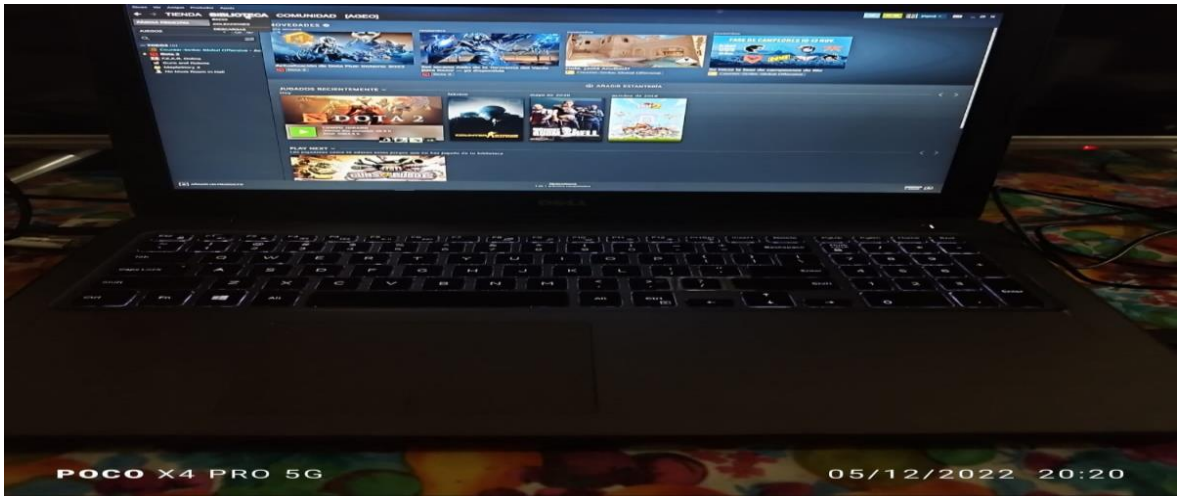


Fuente: elaboración propia

ETAPA I PRESERVACIÓN

En este primer paso se realiza la incautación del equipo de cómputo, para lo cual se procede a solicitar el computador al usuario, sin alterar el estado en el que se encuentra el computador.

Figura 2. Equipo del equipo de cómputo



Fuente: elaboración propia

ETAPA II ADQUISICIÓN

En esta etapa se recaba toda la información posible, se captura el tráfico de red, se hace un volcado de memoria RAM, así como, también, se capturan procesos, que se ejecutan en el equipo atacado para establecer una línea de tiempo e identificar cuáles son las vulnerabilidades encontradas y, para el presente caso de estudio, se hace únicamente una copia bit a bit del disco duro del equipo incautado, para esto existen herramientas especializadas que permiten ejecutar este proceso; en la presente investigación, se realiza una copia con la herramienta FTK *Imager* para obtener una imagen física a través de los pasos que se detalla a continuación:

1. Descarga de la herramienta FTK
2. Con el equipo encendido se procede a ejecutar el programa FTK, para obtener la imagen forense del disco duro del equipo.
3. Se procede a obtener la imagen de la memoria RAM, mediante el uso del programa FTK *Imager*.

ETAPA III DOCUMENTACIÓN

En esta fase se procede a documentar el proceso mediante la captura de pantalla de cada paso realizado en el análisis forense del equipo, a continuación, se muestra todo el proceso realizado:

1. Incautación del equipo
   El equipo se encuentra encendido el momento que se procede a incautarlo.

Figura 3. Incautación del equipo de cómputo

Fuente: elaboración propia

2. Descarga de herramientas forense

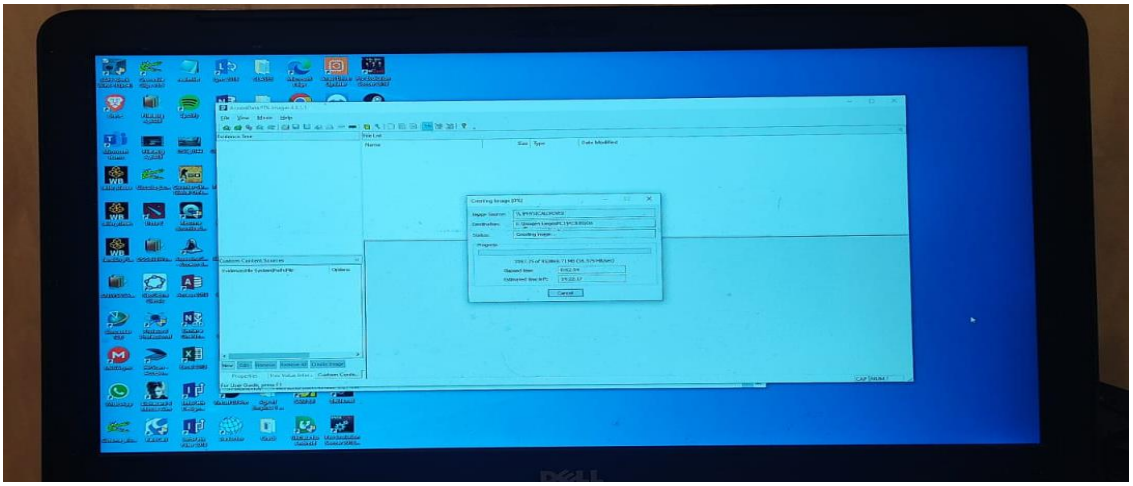
   La herramienta se encuentra en el siguiente enlace para la descarga: https://accessdata.com/product-download/ftk-imager-version-4-3-1-1

3. Obtiene imagen forense del disco duro

   Una vez identificado el disco a copiar, es importante, tener en cuenta que para la copia, se realiza en un disco externo con mínimo el doble de capacidad del disco origen.

   Se procede a ejecutar el programa FTK *imager*

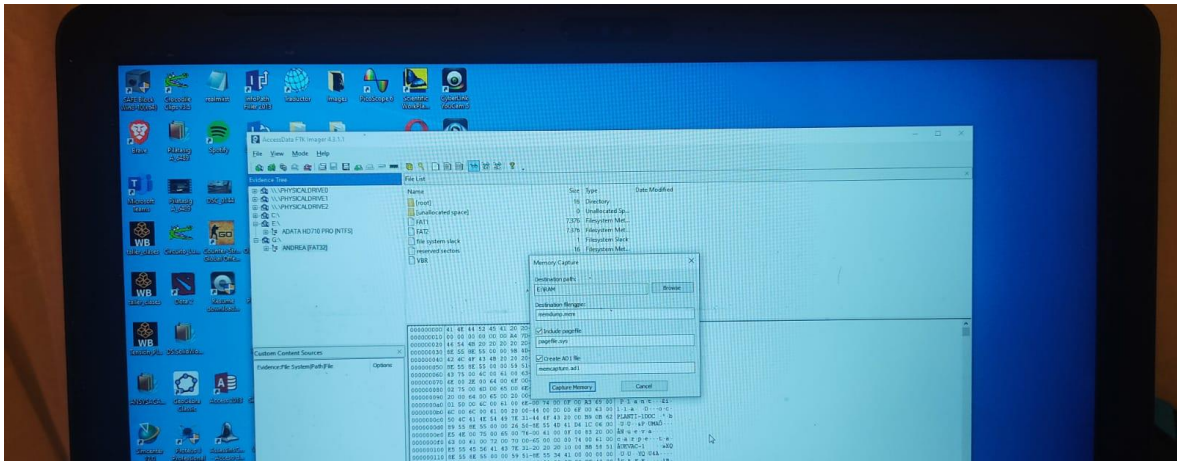
Figura 4. Obtención de la imagen forense disco duro



Fuente: elaboración propia

4. Obtiene imagen forense de la memoria RAM como se muestra en la figura 5

Figura 5. Obtención de la imagen forense RAM



Fuente: elaboración propia

ETAPA IV ANÁLISIS

Se procede a realizar el análisis de la imagen que se obtuvo, para esto se hace uso de la herramienta *Autopsy*.

1. Disco duro

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

2. Instalación y ejecución, como, se observa en la Figura 6.

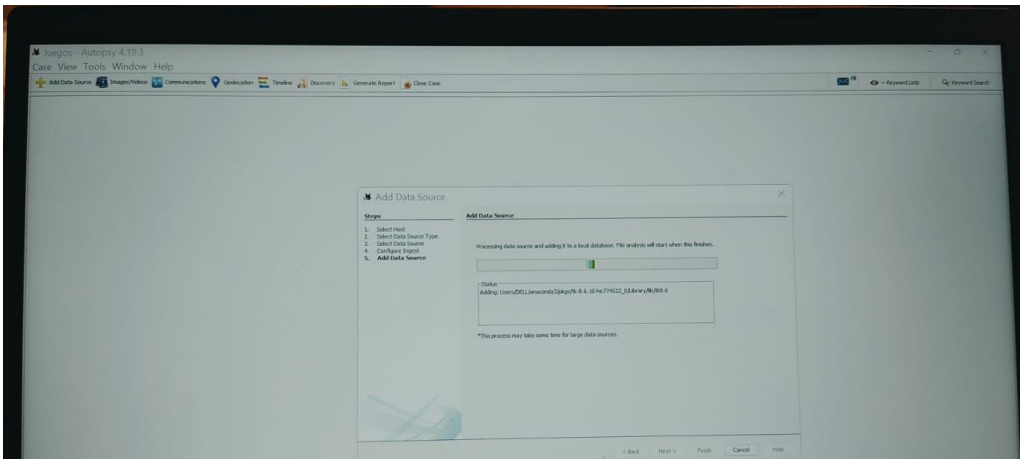
Figura 6. Carga de la imagen forense disco duro

Fuente: elaboración propia

3. Se ejecuta la aplicación de *Autopsy*, y se crea el caso, se carga la imagen forense del disco duro.

4. Una vez seleccionado los diferentes módulos para buscar información, estos procesos, se ejecutan en segundo plano y proporcionan resultados en tiempo real, como se ve en la figura 7:

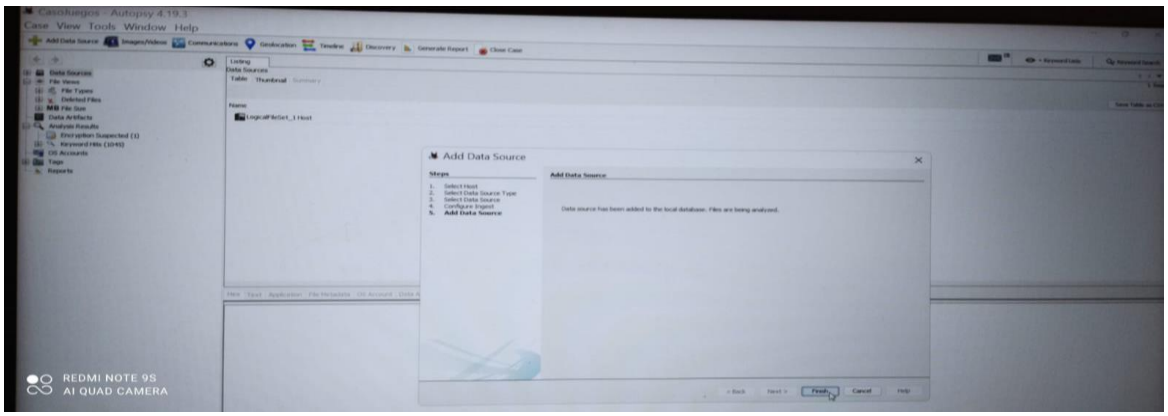
Figura 7. Carga de la imagen forense disco duro



Fuente: elaboración propia

5. Se carga la imagen forense de la memoria RAM, como se visualiza en la figura 8

Figura 8. Carga de la imagen forense de la RAM



Fuente: elaboración propia

6. Como siguiente y último paso en esta etapa, el investigador busca indicios para establecer causas y brechas de seguridad.

ETAPA V

Presentación

En esta etapa se realiza la presentación del informe pericial, el mismo que se va a detallar en el capítulo III, en el que se indica todos los hallazgos del equipo incautado.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1 Informe Forense

El desarrollo del siguiente apartado se documenta de acuerdo con el Anexo 4. Formato informe Consejo de la Judicatura, sin embargo, al tratarse de un tema de investigación, se realizan ajustes y, se omiten detalles en los datos generales por situación educativa, esto con el objetivo de preservar la integridad en la información de la persona que realiza el presente proyecto. (Judicatura, 2020)

"INFORME PERICIAL"

DATOS GENERALES

No. de Proceso	**001**
Nombre y Apellido de la o el Perito	**Andrea Fernanda Choto Tuquerres**

PARTE DE ANTECEDENTES

En la presente investigación se ha considerado un equipo de cómputo, que se utiliza para juegos de video, por lo tanto, se realiza un AFI para determinar cuál o cuáles son las vulnerabilidades que existen y las que se explotan en un futuro por hacer uso de juegos de video.

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

PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE

En la Figura 9, muestra el equipo de cómputo de la marca DELL, cuenta con un disco duro de 1 TB de capacidad en almacenamiento, información, que se obtiene del acta entrega recepción suscrita conforme el formato establecido en el Anexo 2.

Formato acta entrega recepción, la metodología de investigación, que se aplica en el presente caso, se detalla en el epígrafe 2.2 y 2.3 del capítulo anterior.

Figura 9. Equipo de cómputo DELL

Fuente: elaboración propia

PARTE DE CONCLUSIONES

Las conclusiones correspondientes al análisis forense se reflejan en el apartado de conclusiones del presente proyecto.

PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO

Se valida la cadena de custodia, que se observa en la Figura 10; se concluye que la copia *bit* a *bit* entregada para el análisis coincide con la información original del equipo incautado.

Figura 10. Verificación cadena de custodia

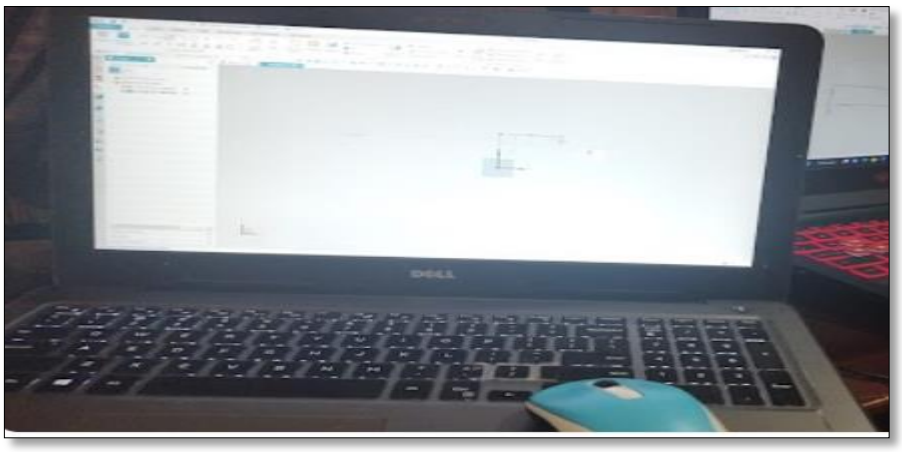
```
 MD5 checksum:     195de603b56c5046fc071e302a0174cc
 SHA1 checksum:    100c003cfdbe6f1af2ecd7d20ed54aded19112f0

Image Information:
 Acquisition started:    Tue Dec  6 09:30:43 2023
 Acquisition finished:   Tue Dec  6 18:24:30 2023
```

Fuente: elaboración propia

Para la ejecución del análisis forense, se recibe un computador el lunes 05 de diciembre de 2022. De dicho equipo se procede a extraer la imagen del disco duro interno (ver Tabla 5) para efectuar una copia origen-destino (clonación espejo bloque a bloque) mediante un procedimiento técnico de cómputo forense, con el fin de preservar la evidencia original sin contaminarla y obtener una fiel copia de la misma.

Figura 11. Procedimiento de adquisición de imágenes forenses del disco auditado.



Fuente: elaboración propia

El disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB se encuentra operativo al momento de obtener la imagen forense utilizada para realizar este análisis, se observa en la tabla 5.

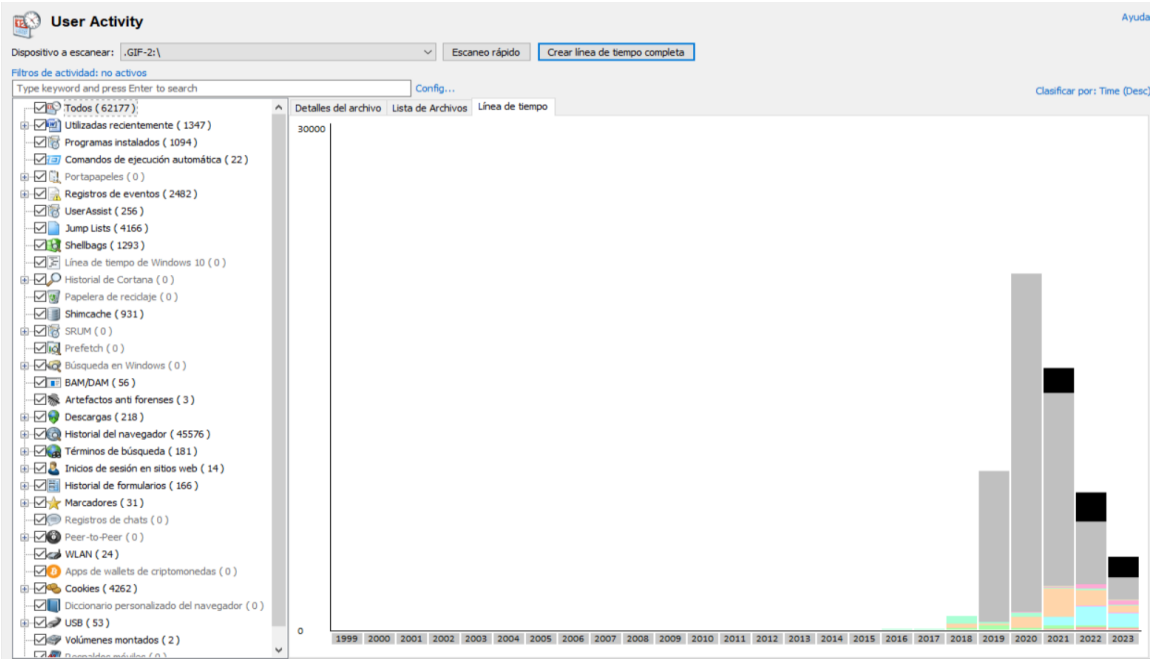
Tabla 2. Disco duro interno del equipo auditado.

Marca:	**TOSHIBA**
Modelo:	**MQ01ABD100**
Tecnología:	**IDE**
Capacidad:	**953869 MB**
Número de Serie:	**X77HTZOMT**
Salud del disco:	**Normal**

Fuente: elaboración propia

El mencionado disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB registra en la línea de tiempo como última fecha de operatividad el 05/12/2022 a las 20h00:00, se visualiza en la Figura 12.

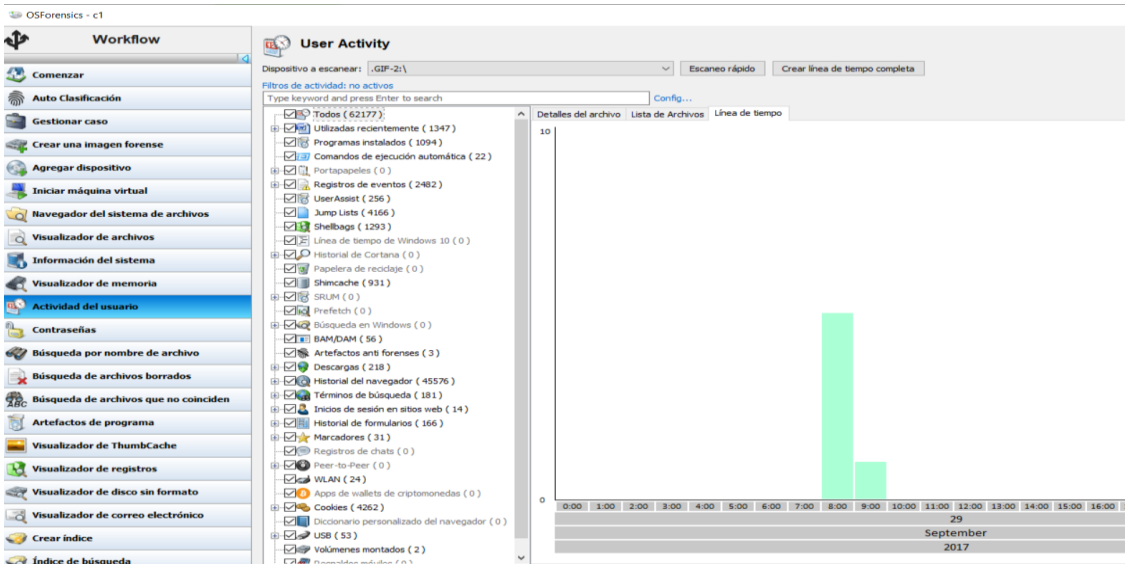
Figura 12. Línea de tiempo.



Fuente: elaboración propia

El sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB es Microsoft Windows 10 y en su línea de tiempo denota fecha de creación 29/09/2017 a las 03h45:11 (hora local), es el nombre del computador (*hostname*) DELL, se visualiza en la imagen 13.

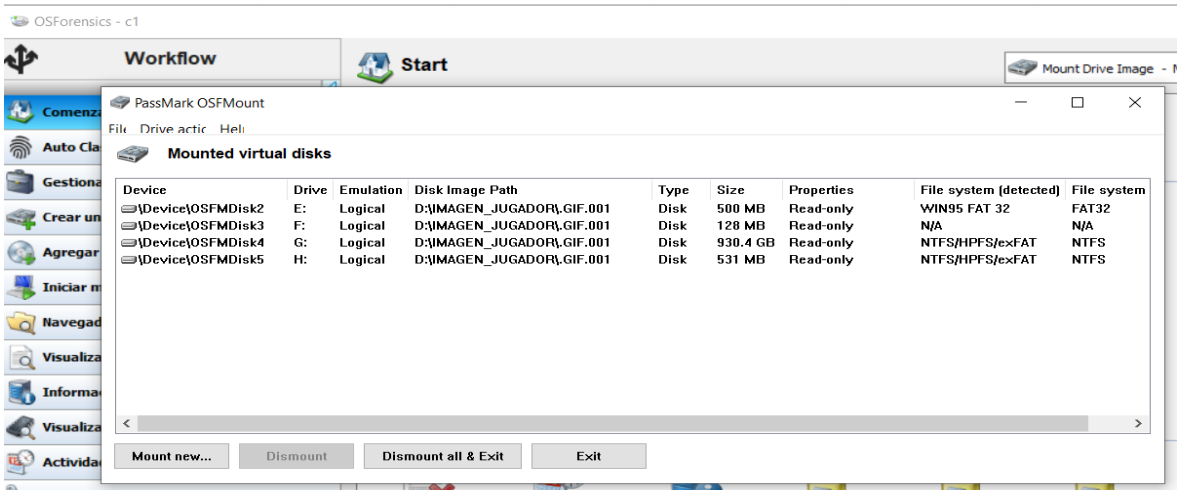
Figura 13. Línea de tiempo Instalación del sistema.



Fuente: elaboración propia

El sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, se encuentran cuatro particiones: Partición 0 500.0MB (WIN95 FAT32), Partición 1 100.00MB (NTFS/HPFS/exFAT), Partición 2 128.0MB (*Empty partition*), Partición 3 930GB (NTFS/HPFS/exFAT) y Partición 4 531MB (NTFS/HPFS/exFAT), que se visualizan en la figura 14.

Figura 14. Mapeo de particiones de disco auditado en *OSForensics*.



Fuente: elaboración propia

En el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, se registran cuatro cuentas de usuario, ver en la tabla 6.

Tabla 3. Cuentas de usuario existentes.

Username [ID]	***Administrator [500]***
Full Name	
Description	*Built-in account for administering the computer/domain*
Password Hint	
Account Created	*N/A*
Last Login	sábado*, 23 de* diciembre *de 2017, 22:50:50*
Password Reset	*Never*
Password Fail Date	*N/A*
Password Fail Count	*0 (reset after correct login)*
Login Count	*4*
Notes	**Password never expires**
Username [ID]	***Guest [501]***
Full Name	
Description	*Built-in account for guest access to the computer/domain*
Password Hint	
Account Created	jueves, 27 de mayo de 2021, 12:01:38 *(can be inaccurate if registry permissions have been updated)*
Last Login	*Never*
Password Reset	*Never*
Password Fail Date	*N/A*
Password Fail Count	*0 (reset after correct login)*
Login Count	*0*
Notes	**Password never expires**
Username [ID]	***DefaultAccount [503]***
Full Name	
Description	*A user account managed by the system.*
Password Hint	
Account Created	viernes, 16 de diciembre de 2022*,* 11:29:09 *(can be inaccurate if registry permissions have been updated)*
Last Login	*Never*
Password Reset	*Never*
Password Fail Date	*N/A*
Password Fail Count	*0 (reset after correct login)*
Login Count	*0*
Notes	**Password never expires**
Username [ID]	***WDAGUtilityAccount [504]***
Full Name	
Description	*A user account managed and used by the system for Windows Defender Application Guard scenarios.*
Password Hint	

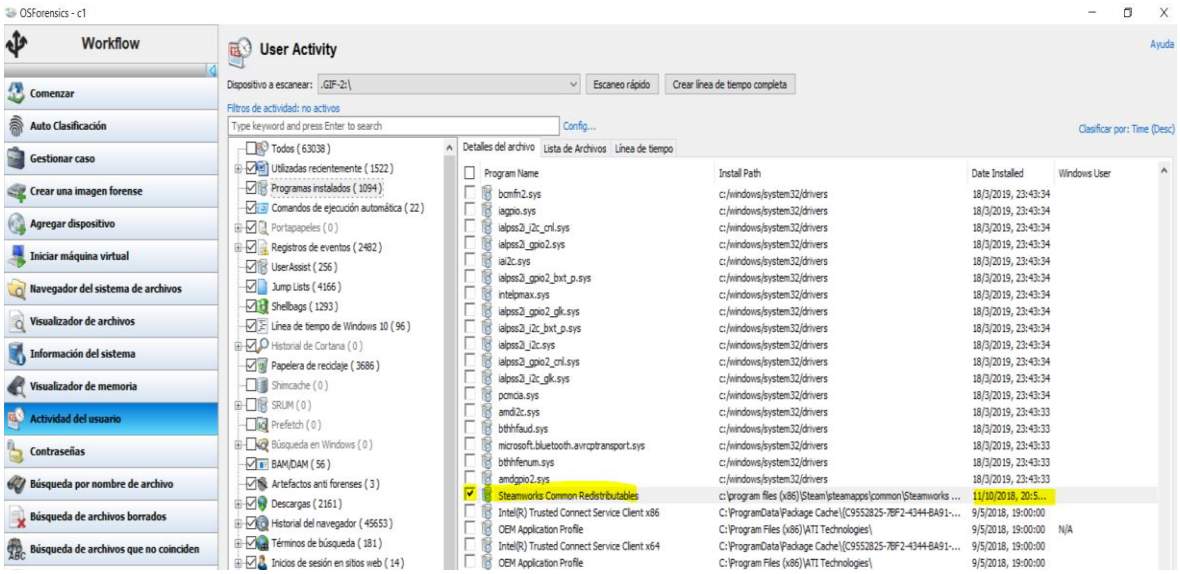
Account Created	jueves, 27 de mayo de 2021, 12:01:38 *(can be inaccurate if registry permissions have been updated)*
Last Login	*Never*
Password Reset	sábado, 23 de diciembre de 2017, 22:14:20
Password Fail Date	*N/A*
Password Fail Count	*0 (reset after correct login)*
Login Count	*0*
Notes	
Username [ID]	***DELL [1001]***
Full Name	
Description	
Password Hint	
Account Created	jueves, 27 de mayo de 2021, 12:01:38 *(can be inaccurate if registry permissions have been updated)*
Password Reset	*Never*
Password Fail Date	*N/A*
Password Fail Count	*0 (reset after correct login)*
Login Count	*3903*
Notes	**Password never expires**
Username [ID]	***ASPNET [1003]***
Full Name	*ASP.NET Machine Account*
Description	*Account used for running the ASP.NET worker process (aspnet_wp.exe)*
Password Hint	
Account Created	jueves, 27 de mayo de 2021, 12:01:38 *(can be inaccurate if registry permissions have been updated)*
Last Login	*Never*
Password Reset	viernes, 16 de diciembre de 2022, 11:29:09
Password Fail Date	*N/A*
Password Fail Count	*0 (reset after correct login)*
Login Count	*0*
Notes	**Password never expires**

Fuente: elaboración propia

En el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, la cuenta utilizada por defecto corresponde al usuario denominado **dell**.

En el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB se registra el programa *Steam* a partir del 11-10-2018 21:09:03, ver figura 15.

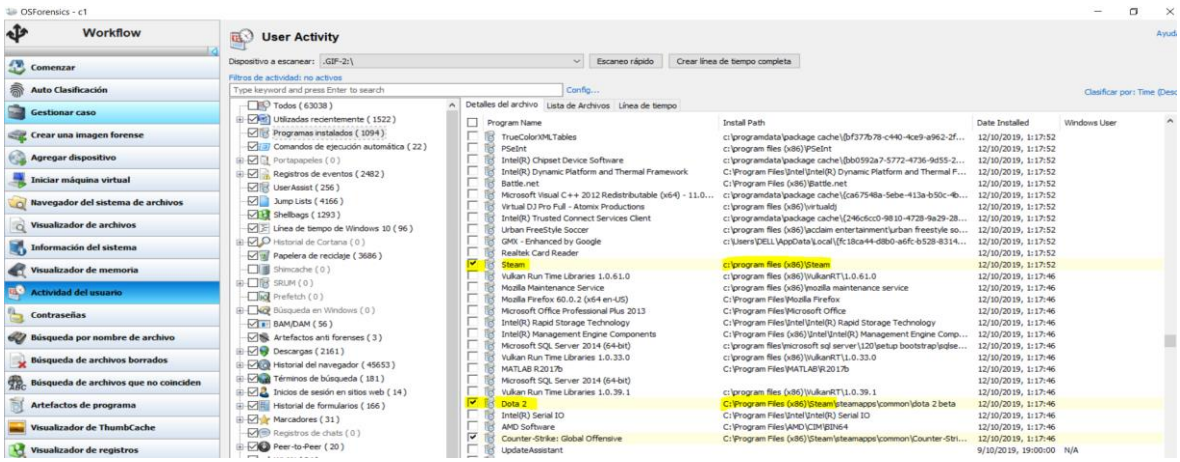
Figura 15. Instalación de aplicación para juegos.



Fuente: elaboración propia

En el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB se registra el programa Dota2 a partir del 11-06-2021 17:42:10, ver figura 16.

Figura 16. Instalación de Dota 2.

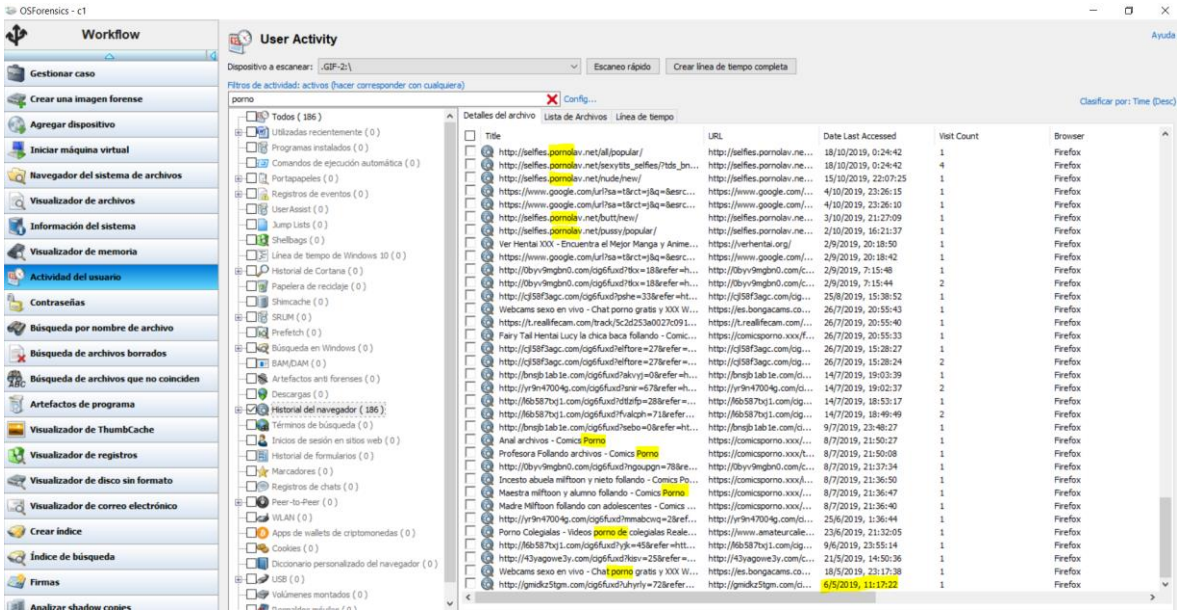


Fuente: elaboración propia

Que la información recabada de los archivos de historia y caché de los navegadores instalados en el sistema operativo del disco duro interno marca *TOSHIBA*, modelo

MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, denota conexiones a los sitios webs: https://cumshots.com/t5/index.php?t=Ex-popunder-ES-LQ, http://pornojuegosgratis.com/, https://www.juegosporno.xxx/, estos registros se han realizado desde la fecha 06-05-2019 11:17:22, ver figura 17.

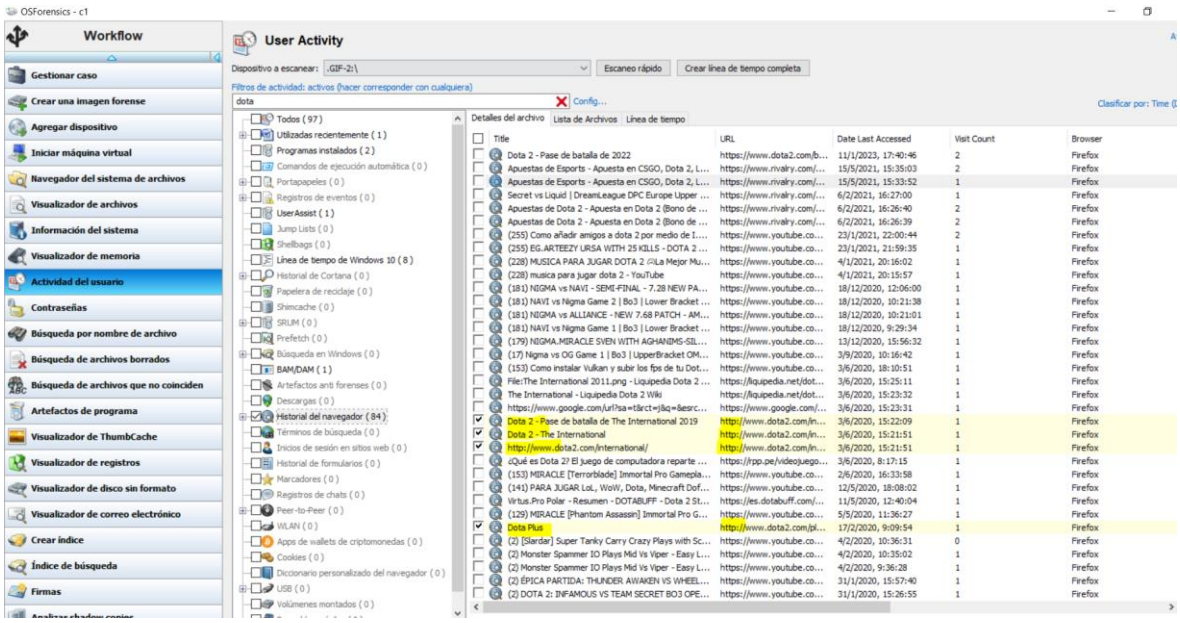
Figura 17. Navegación desde el año 2019.



Fuente: elaboración propia

Que como resultado de la búsqueda del texto dota en la imagen forense del disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, se halla evidencia de búsquedas a las siguientes páginas web: http://www.dota2.com/international2019/battlepass/, http://www.dota2.com/international/overview/, http://www.dota2.com/international/ , http://www.dota2.com/plus?l=spanish, misma que se transmite desde el computador analizado a través de la red local y hacia Internet en texto plano, es decir sin cifrar, hacia dichas páginas web puesto que el protocolo utilizado por las mismas es HTTP el cual no utiliza inscripción, ver figura 18.

Figura 18. Navegación de usuario por palabra de búsqueda dota sitios no seguros.



Fuente: elaboración propia

Que la dirección IP registrada por Windows en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, es una dirección IP privada perteneciente a la red interna donde se encuentra conectado el computador auditado. Dicha dirección IP es 192.168.1.6/26 y se obtiene de forma automática por el adaptador de red Ethernet de dicho computador a través del protocolo DHCP, ver tabla 7.

Tabla 4. Información de la red.

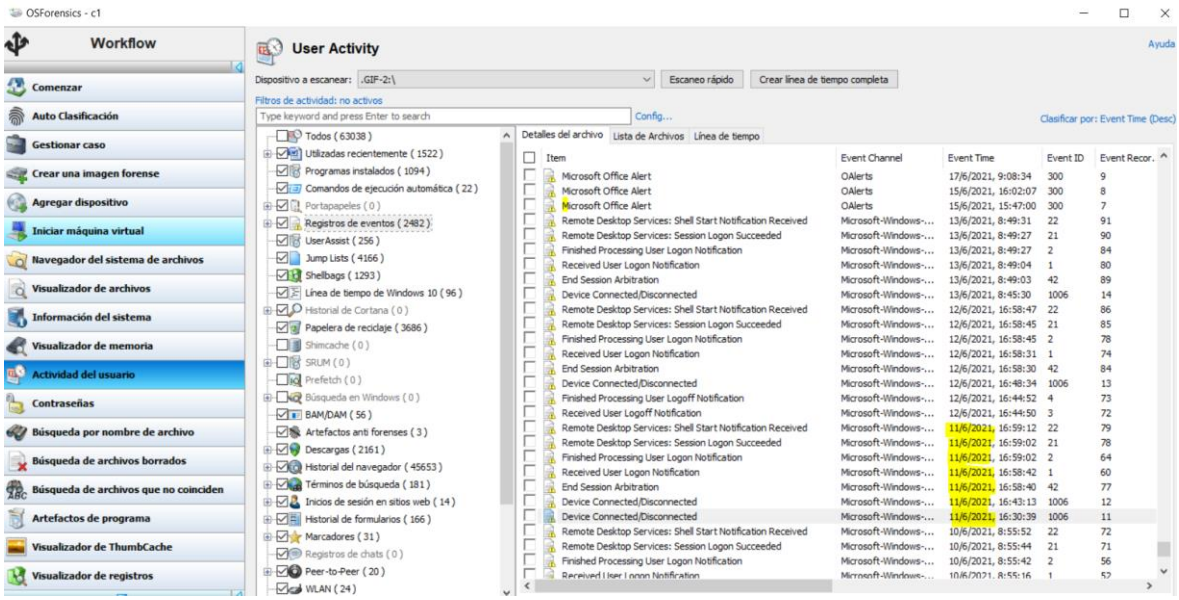
Network GUID	{befa380e-9e19-49a9-a45b-efffc6befcdb}
Network Name	*Ethernet*
IP (using DHCP)	192.168.1.6 (Yes)
DHCP Server	192.168.1.1
DHCP Name Server	192.168.1.1

Fuente: elaboración propia

Que la puerta de enlace o *gateway* asignado al adaptador de red del computador auditado corresponde a la IP 192.168.1.1, ver tabla 7.

Que el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, no registra actividades que alerten el sistema en las fechas en las que se instalaron el programa Dota2, ver figura 19.

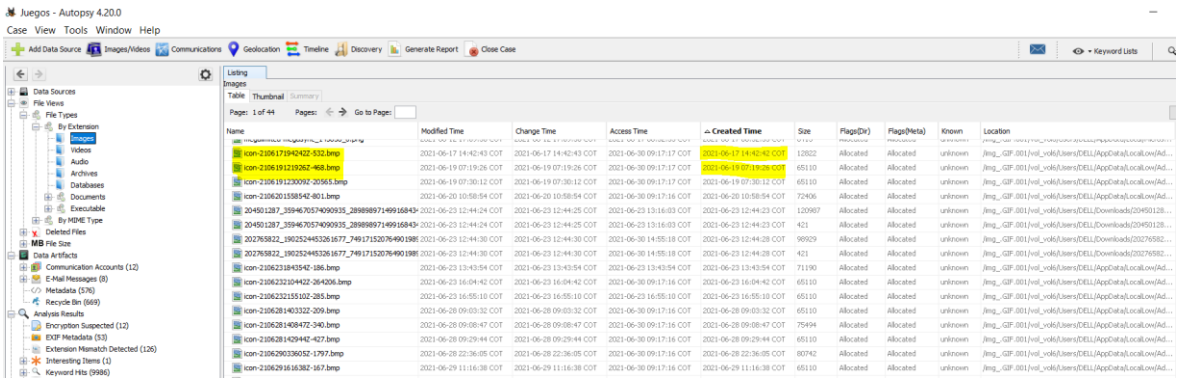
Figura 19. Registro de Eventos a partir de la instalación del juego.



Fuente: elaboración propia

Que el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, registra fotografías de pornografía a partir de la fecha 17-06-2021, ver figura 20.

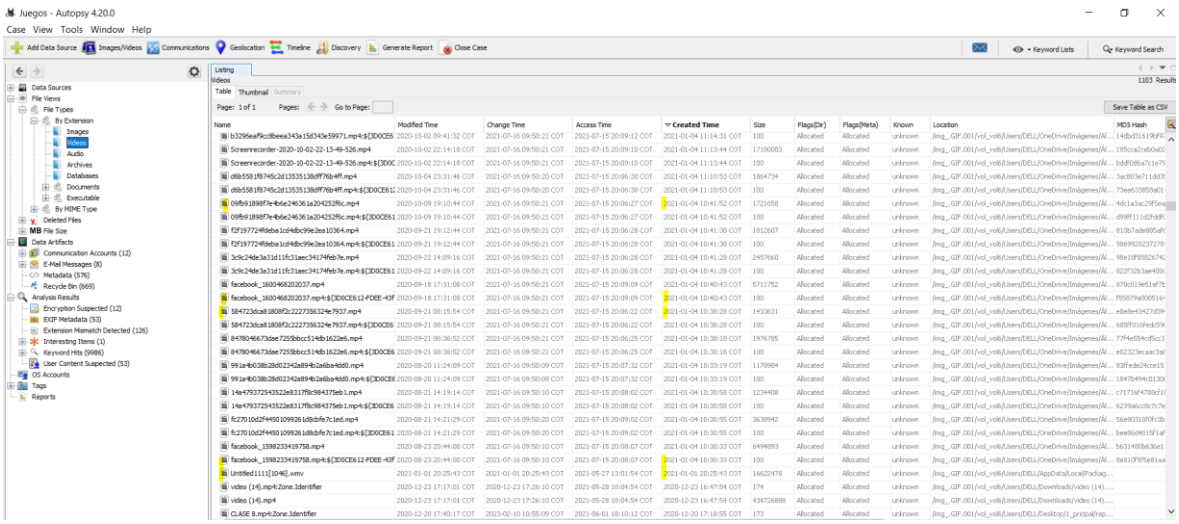
Figura 20. Registro de fotografías.



Fuente: elaboración propia

Que el sistema operativo instalado en el disco duro interno marca *TOSHIBA*, modelo MQ01ABD100, con número de serie X77HTZOMT, de tecnología IDE y capacidad 953869 MB, registra videos de pornografía a partir de la fecha 01-01-2021, ver figura 21.

Figura 21 Registro de videos.



Fuente: elaboración propia

OTROS REQUISITOS

No se incluyen otros requisitos al caso en estudio presente.

INFORMACIÓN ADICIONAL

No existe información adicional.

DECLARACIÓN JURAMENTADA

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

FIRMA Y RÚBRICA

3.2 Propuesta de políticas de buenas prácticas de acceso a video juegos en línea.

- En el pasado la ciberseguridad no era una prioridad para el tipo de industria de los juegos de video, con la evolución de la industria se considera la seguridad como un pilar fundamental para su uso.

- Conforme lo analizado en el caso de estudio se establece los siguientes puntos a considerar para mejorar la seguridad al hacer uso de los juegos de video en línea, los mismos que se han tomado en cuenta de acuerdo a la información obtenida durante toda la investigación, a continuación, se detalla las buenas prácticas para los jugadores según la revista (SEGUROS SURA, 2019):

- Tener activa la verificación en dos pasos, esto agrega un nivel de seguridad a las cuentas y ayuda a evitar accesos no autorizados.

- Evitar acceder a enlaces que sean enviados por mensajes, estos son virus con el que acceden a la cuenta de usuario para apropiarse de la misma.

- Evitar jugar con la conexión a redes *wifi* públicas desconocidas.

- No desactivar la solución de seguridad: *Keyloggers* (grabador de pulsaciones en las teclas), *exploits* (vulnerabilidades de plataformas) o malware son igual de reales en el mundo *gamer* que en cualquier otra actividad online, por lo que se necesitan soluciones de seguridad al detectar proactivamente cualquier posible riesgo. Y no es necesario que por ello se renuncie a las funcionalidades completas de un juego: los productos que cuentan con modo *gamer* no provocan interrupciones ni problemas de *lag* (retardo excesivo producido por una telecomunicación en tiempo real).

- Descargar juegos legales y de repositorios oficiales: Al descargar juegos de repositorios no confiables terminaría como víctima de *malware*, que buscan robar tu información personal o datos de tu tarjeta de crédito. Por otro lado, las tiendas virtuales reconocidas brindan garantías en la transacción. En cambio, si se opta por una versión no oficial o pirata, quizás se pierda más dinero que al comprar un juego original.

- Cuidado con la información que se comparte en foros: Se sabe que las comunidades de jugadores son un buen lugar para hacer contactos, buscar nuevas tácticas o evacuar dudas (y para los menos pacientes, buscar trucos), pero muchos cibercriminales se apuntan a los foros de juegos para obtener largas listas de usuarios y contraseñas.

- La Ingeniería Social también se adapta a los jugadores: Los ciberdelincuentes generalmente buscan robar credenciales de acceso, por lo que recuerda hacer *login* al ingresar directamente al sitio oficial y nunca ingrese la contraseña en una página a la que se llega por una redirección o correo, que pudieran ser sospechosos.

- Usa contraseñas robustas y distintas para cada plataforma: Por ser las puertas de entrada a cuentas que alojan información sensible y datos personales, las contraseñas necesitan de todo el esmero para ser construidas. Utiliza mínimo 12 caracteres.

- Cuidado con las personas que agrega: Ladrones de *bitcoins*, *trolls* o simplemente cibercriminales son personajes que se quieren evitar, por lo que tener cautela al interactuar en línea y procurar no dar demasiados detalles personales reales. A decir verdad, difícilmente se sabe quién está del otro lado: quizás hasta un compañero de equipo no es quien dice ser, y encontrarse allí solo para propagar amenazas o pescar víctimas desprevenidas.

- Verificar pagos: A la hora de efectuar pagos en plataformas de videojuegos es necesario asegurarse bien que el pago no se realice en una web falsa que simula ser la real.

CONCLUSIONES

- Se determina que después de realizar el análisis forense al equipo en custodia, se llega a la conclusión que no existe información que relacione los juegos de video instalados en el equipo con los delitos informáticos.

- De acuerdo a la información recabada durante la investigación de los juegos de video se determina que no existen registros que se hayan vulnerado al momento de la descarga e instalación.

- Existe información relacionada a búsquedas de datos pornográficos que realiza el usuario en cuanto a juegos de video relacionado al tema de pornografía, sin embargo, no se relaciona con los juegos instalados en el sistema.

- Se encontraron accesos a sitios web no seguros, los mismos que aumentan los peligros que el equipo sea vulnerado.

- Con la investigación realizada en cuanto a las buenas prácticas que se toman en cuenta al hacer uso de los juegos de video, se determina en el apartado 3.2.

RECOMENDACIONES

- Luego del proceso de análisis forense realizado al equipo de cómputo se determina que no es suficiente para la investigación por lo que se recomienda realizar un análisis forense a más equipos de cómputo que hagan uso de juegos de video y con eso lograr determinar si existe relación con los delitos informáticos al hacer uso de los mismos.

- Analizar los registros que almacena el equipo de cómputo, para determinar los posibles ataques que se haya registrado en el sistema operativo.

- Se recomienda buscar información de los *logs* del sistema para determinar rastros que se de en caso de encontrar vulneraciones al equipo de cómputo.

- En base a las recomendaciones de seguridad propuestas en el apartado 3.2, se recomienda implantar medidas de protección más específicas de acuerdo a las vulnerabilidades encontradas en el equipo de cómputo.

BIBLIOGRAFÍA

AO Kaspersky Lab. (2023). latam.kaspersky.com. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/resource-center/threats/top-10-online-gaming-risks

ciberseguridad.com. (26 de Agosto de 2022). Obtenido de ciberseguridad.com: https://ciberseguridad.com/guias/recursos/seguridad-juegos-en-linea/

ciberseguridad.com. (05 de MAYO de 2023). Obtenido de ciberseguridad.com: https://ciberseguridad.com/guias/videojuegos/#Ataques_e_impactos_predominantes_en_la_industria_del_videojuego

Correa, J. P. (13 de Junio de 2021). www.lawandtrends.com. Obtenido de www.lawandtrends.com: https://www.lawandtrends.com/noticias/tic/delitos-informaticos-en-videojuegos-1.html

Departamento de Salud y Servicios Humanos de los Estados Unidos. (14 de SEPTIEMBRE de 2021). espanol.stopbullying.gov. Obtenido de espanol.stopbullying.gov: https://espanol.stopbullying.gov/cyberbullying/cyberbullying-online-gaming

Digital, C. (20 de Diciembre de 2019). https://www.pantallasamigas.net/. Obtenido de https://www.pantallasamigas.net/:

https://www.pantallasamigas.net/decalogo-buenas-practicas-gamers-disfrutarte-videojuegos-aevi/

Duitama, K. P. (2021). https://www.larepublica.co/. Obtenido de https://www.larepublica.co/ocio/el-mundo-de-los-videojuegos-esta-tomando-fuerza-entre-personas-mayores-de-30-anos-3186705#:~:text=Seg%C3%BAn%20la%20Asociaci%C3%B3n%20de%20Software,edades%20entre%2035%20y%2054.

EALDE. (25 de Julio de 2021). www.ealde.es. Obtenido de www.ealde.es: https://www.ealde.es/informatica-forense/

es.wikipedia.org. (NOVIEMBRE de 2021). Obtenido de es.wikipedia.org: https://es.wikipedia.org/wiki/Videojuego_de_rol_en_l%C3%ADnea_competitivo

Gálvez, F. S. (30 de Abril de 2021). csecmagazine.com. Obtenido de csecmagazine.com: https://csecmagazine.com/2021/04/30/la-importancia-de-la-informatica-forense/

Grupo Atico34. (6 de JUNIO de 2022). protecciondatos-lopd.com. Obtenido de protecciondatos-lopd.com: https://protecciondatos-lopd.com/empresas/informatica-forense/

https://www.infobae.com/. (29 de ABRIL de 2020). Obtenido de https://www.infobae.com/:

https://www.infobae.com/gaming/2020/04/29/epic-games-regala-juegos-pero-con-una-condicion-habilitar-la-verificacion-en-dos-pasos/

Hushapp, T. (2020). ciberseguridad.uach.mx. Obtenido de ciberseguridad.uach.mx: https://ciberseguridad.uach.mx/tmp/tips-de-ciberseguridad-para-consolas-y-videojuegos/#:~:text=Ciberseguridad%20para%20consolas%20y%20videojuegos%20online&text=Elimina%20las%20medidas%20de%20protecci%C3%B3n,desde%20las%20p%C3%A1ginas%20web%20oficiales.

Internet Matters. (2023). www.internetmatters.org. Obtenido de www.internetmatters.org: https://www.internetmatters.org/es/resources/online-gaming-advice/the-basics/#gaming

JIMENEZ, A. D. (14 de Septiembre de 2018). https://1library.co/. Obtenido de https://1library.co/: https://1library.co/document/yjdl7x6y-diseno-metodologia-analisis-forense-consolas-videojuegos-play-station.html

Juan, M. (13 de ABRIL de 2021). www.lawandtrends.com. Obtenido de www.lawandtrends.com: https://www.lawandtrends.com/noticias/tic/delitos-informaticos-en-videojuegos-1.html

Judicatura., C. d. (2020). funcionjudicial.gob.ec. Obtenido de funcionjudicial.gob.ec: https://funcionjudicial.gob.ec/

Lerner, I. (9 de ENERO de 2023). www.3djuegospc.com. Obtenido de www.3djuegospc.com: https://www.3djuegospc.com/sistema-operativo/te-resistes-a-windows-11-cada-vez-estas-cerca-ser-minoria-gamers

Lópezlee, J. M. (28 de JUNIO de 2022). www.movistar.es. Obtenido de www.movistar.es: https://www.movistar.es/blog/gaming/windows-11-gamers-juegos/

Mestew. (17 de ABRIL de 2023). learn.microsoft.com. Obtenido de learn.microsoft.com: https://learn.microsoft.com/es-es/windows/whats-new/windows-11-overview

Microsoft. (2023). support.microsoft.com. Obtenido de support.microsoft.com: https://support.microsoft.com/es-es/windows/permisos-de-aplicaciones-aea98a7c-b61a-1930-6ed0-47f0ed2ee15c

Miguel, E. (2008). perso.unifr.ch. Obtenido de perso.unifr.ch: https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

Muncaster, P. (19 de JULIO de 2022). www.welivesecurity.com. Obtenido de www.welivesecurity.com: https://www.welivesecurity.com/la-es/2022/07/19/razones-no-descargar-juegos-pirateados/

OJEDA, B. S. (14 de Junio de 2018). https://repositorio.uisek.edu.ec/. Obtenido de https://repositorio.uisek.edu.ec/: https://repositorio.uisek.edu.ec/handle/123456789/3021

OJEDA, B. S. (14 de 06 de 2018). repositorio.uisek.edu.ec. Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/3021/1/Documento%20final%20de%20tesis%20Bryan%20C%C3%B3rdova%20Ojeda%20MTI%20UISEK.pdf

Paul Lara. (9 de Mayo de 2022). e.SPORTSMX. Obtenido de e.SPORTSMX: https://theesportsmexico.com/2022/05/09/ciberseguridad/la-ciberseguridad-no-es-un-juego-en-los-esports

Pazan, C. (25 de Julio de 2022). www.elcomercio.com. Obtenido de www.elcomercio.com: https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Redacción Seguridad. (25 de JULIO de 2022). www.elcomercio.com. Obtenido de www.elcomercio.com: https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Rodríguez, P. D. (2022). indalics.com. Obtenido de indalics.com: https://indalics.com/blog-peritaje-informatico/informatica-forense-evidencias-digitales

SEGUROS SURA. (2019). www.segurossura.com.co. Obtenido de www.segurossura.com.co: https://www.segurossura.com.co/documentos/centro-proteccion-digital/seguridad-para-gamers.pdf

Servicio de Acreditación Ecuatoriano. (09 de MAYO de 2018). www.acreditacion.gob.ec. Obtenido de www.acreditacion.gob.ec: https://www.acreditacion.gob.ec/norma-para-recopilacion-de-evidencias/

www.osforensics.com. (18 de Mayo de 2018). Obtenido de www.osforensics.com: https://www.osforensics.com/products/index.php

ANEXOS

Anexo 1. Formato de la entrevista

ENTREVISTA	
Juego más usado	Dota 2 (x) Call of Duty () Fortnite ()
Equipo que utiliza para jugar	PC (x) Móvil () Tablet ()
Sistema operativo que utiliza	Windows (x) Linux () Otro ()
Conoces sobre los ataques existentes al hacer uso de juegos de video en línea	Si(x) No ()

Fuente: elaboración propia

Anexo 2. Formato acta de entrega recepción

ACTA DE EQUIPOS COMPUTACIONALES

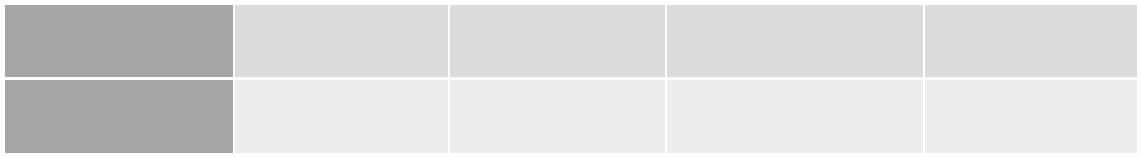
Hoy XX del mes XXXXX de XXX el departamento de TI, mediante el siguiente documento realiza la entrega formal de los equipos computacionales para la realización del análisis forense, quién declara recepción de estos en buen estado y se compromete a cuidar de los recursos y hacer uso de ellos para los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

Datos del encargado de realizar el análisis forense informático

Nombres, Apellidos	
Cédula	
Departamento	
Cargo	

EQUIPOS COMPUTACIONALES ASIGNADOS

Descripción del producto				
Número de serie				
Numero de inventario				
Descripción	**Marca**	**Modelo**	**Características**	**Serial**



OBSERVACIONES

Añadir en este apartado la cadena de custodia

ENTREGA

Fecha entrega: xx de xx de xx

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

DEVOLUCIÓN

Fecha devolución: xx de xx de xx

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

Fuente: elaboración propia

Anexo 3. Formato acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN PARA LA REALIZACIÓN DE ANALISIS FORENSE INFORMÁTICO AL EQUÍPO DE COMPUTO DE XXXXX

Intervienen en la celebración del presente ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE LA INFORMACIÓN SOBRE EL USO DE COPIAS DEL EQUIPO DE COMPUTO DEL PROPIETARIO XXXXXX como comparecientes:

Por una parte, el PROPIETARIO el señor XXXXXXX con cedula de ciudadanía Nro. XXXXXX y por otra parte el Ing. Andrea Choto con cédula de ciudadanía Nro. XXXXXX en calidad de Maestrante de la Pontificia Universidad Católica sede Ambato. Quienes libre y voluntariamente celebran el presente acuerdo. Los comparecientes reconocen recíprocamente su capacidad para obligarse, por lo que suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información con base a las siguientes cláusulas.

CLÁUSULA PRIMERA. – ANTECEDENTES:

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

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

Que se define como Información Confidencial, toda la información relativa o de propiedad del INTERESADO, que cumpla los siguientes requisitos: a. Que sea 84 reservada, en el sentido de que no sea generalmente conocida ni de fácil obtención por quienes se encuentran en el medio en, el cual, dicha información es manejada; y b. Que sea designada como confidencial por su titular. Esta

designación se la realiza de forma escrita o es ratificada de la misma manera, depende de la forma en, la cual, la respectiva Información Confidencial es divulgada por el Titular al Receptor.

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

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

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

CLÁUSULA TERCERA. - DERECHOS Y OBLIGACIONES: Las partes indistintamente son RECEPTORES y TITULARES de la información según corresponda. El Receptor declara y reconoce que el recibo o el uso de la Información Confidencial que le sea divulgada por el Titular no le concede, ni expresa ni implícitamente, autorización, permiso o licencia de uso de marcas 85 comerciales, patentes, derechos de autor o de cualquier otro derecho de propiedad intelectual de propiedad del Titular. Ni este acuerdo, ni la divulgación, recibo de información, sea confidencial o no, constituye o implica promesa de

efectuar contrato alguno por cualquiera de LAS PARTES. Son obligaciones de los comparecientes:

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

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

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

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

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

6. Devolver al Titular y/o destruir (si es solicitado por el Titular) los medios físicos en, los cuales, le haya sido entregada la Información Confidencial, junto con las copias que de la misma haya elaborado, y eliminar cualquier grabación, filmación, archivo electrónico o similar que contenga total o parcialmente Información Confidencial, en uno y otro caso dentro de los quince (15) días calendario siguientes a la fecha de cesación del uso autorizado de la Información Confidencial, o al momento en que así los solicite el Titular, lo que primero ocurra. 86

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

permita al Titular de la Información Confidencial oponerse de forma oportuna a dicha orden o solicitud.

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

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

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

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

CLÁUSULA QUINTA. – SANCIONES: Para la aplicación de sanciones se toma en cuenta lo establecido en la Constitución de la República del Ecuador, la Ley Orgánica de Transparencia y Acceso a la Información Pública, Código Orgánico 87 Integral Penal, Ley Orgánica del Sistema Nacional de Registro de Datos Púbicos y demás normativa aplicable; sin perjuicio de las acciones civiles y

penales que procedan en cada caso. La parte que incumpliera las estipulaciones de este instrumento, son sancionados por la autoridad competente.

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

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

NOMBRE REPRESENTANTE Ing. Andrea Fernanda Choto Tuquerres

NOMBRE EMPRESA MAESTRANTE

Firma: _____ Firma: _____

C.C. XXXXXXXXXX C.C. XXXXXXXXXX

Fuente: elaboración propia

Anexo 4. Formato informe Consejo de la Judicatura

FORMATO DE INFORME PERICIAL

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

"INFORME PERICIAL"

DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA

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

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

PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE, en donde se explica claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. La o el perito relacionará los contenidos de sus conocimientos

especializados con el objeto de la pericia encargada. Analizará si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

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

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

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

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

DECLARACIÓN JURAMENTADA, la o el perito en la parte final del informe, declararía bajo juramento que su informe es independiente y corresponde a su real convicción profesional, así como, también, que toda la información que ha proporcionado es verdadera.

FIRMA Y RÚBRICA, al final del informe constaría la firma y rúbrica de la o el perito, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."

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