PROPUESTA PARA ESTABLECER UNA CORRECTA RECOLECCIÓN DE EVIDENCIA DIGITAL, DE ACUERDO CON LA NORMATIVIDAD COLOMBIANA, ENFOCADO A PEQUEÑAS Y MEDIANAS EMPRESAS

JULIAN CAMILO LEGUIZAMÓN SARMIENTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2021

PROPUESTA PARA ESTABLECER UNA CORRECTA RECOLECCIÓN DE EVIDENCIA DIGITAL, DE ACUERDO CON LA NORMATIVIDAD COLOMBIANA, ENFOCADO A PEQUEÑAS Y MEDIANAS EMPRESAS

LEGUIZAMON SARMIENTO JULIAN CAMILO

Proyecto
Monografía para obtener el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director del Proyecto:
EDGAR ROBERTO DULCE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

A mi familia y mi novia a quien amo con el alma por todo el apoyo esencial durante la realización de este proyecto en su realización y revisión. A la universidad que se convirtió en el puente para hacer posible esta iniciativa. A mi empresa que permitió el desarrollo de este proyecto, guiando el camino a seguir para dicha transición.

Además, la experiencia de mis compañeros de trabajo que me motivaron y guiaron en cada paso del proyecto.

AGRADECIMIENTOS

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

Contenido

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Este trabajo monográfico busca a través de las normas vigentes en Colombia en cuanto a los delitos informáticos y la Norma ISO /IEC 27037 de 2012, hacer un estudio de aquellos procedimientos que son necesarios realizar con el fin de proteger la validez de las evidencias digitales en los casos judiciales por delitos informáticos, para finalmente generar recomendaciones de acciones a realizar para complementar los procedimientos de recolección de evidencias digitales.

Con el fin de seguir estas buenas prácticas, se hace necesario tener el conocimiento de conceptos importantes para el área de la informática forense como que es la forensia en redes y la forensia digital, aspectos generales de los objetivos de la informática forense, ciencia forense, evidencia forense, evidencia digital su clasificación y su gestión y lo más importante de la recolección de evidencia que son sus criterios de admisibilidad ante la justicia colombiana.

Para entrar en contexto a tipo de delitos que se pueden cometer y para los cuales son necesarias estas evidencias, se ven aspectos generales de la ley 1273 del 5 de enero de 2009 además se describen las características de los delitos informáticos entre otros aspectos importantes.

ABSTRACT

This monograph searches through the regulations in force in Colombia in terms of computer time and the ISO / IEC 27037 of 2012, makes a study for those in which it must be done in order to protect the validity of digital evidence in the judicial cases of computer crimes, to finally generate forms of tasks to be performed to complement the procedures of digital evidence collection.

In order to follow these good practices, it is necessary to have knowledge of important concepts for the area of forensic computer science, such as forensics in networks and digital forensics, general aspects of the objectives of forensic computer science, forensic science, forensic evidence , digital evidence, its classification and management and, most importantly, the collection of evidence that are its admissibility criteria before the Colombian justice system.

To enter into the context a type of crimes that can be committed and for those that are such as these evidences, these are general aspects of law 1273 of January 5, 2009, in addition to the characteristics of the crimes reported, among other aspects important.

GLOSARIO

EVIDENCIA DIGITAL: Es todo valor probatorio de datos almacenados o transmitidos en formato digital, para que pueda ser usada en un juicio.

CADENA DE CUSTODIA: Es el procedimiento que establece responsabilidades y puntos de control respecto a todo individuo o persona que puede llegar a tener contacto con la evidencia digital.

PERITO INFORMATICO: Es un personal colaborador de la justicia que tiene como función asesorar a la justicia acerca de temas relacionados con la informática.

SEGURIDAD INFORMATICA: Es una disciplina que tiene como misión proteger la privacidad e integridad de la información

INTRODUCCIÓN

Con los continuos ataques que se continúan reportando a diario diferentes compañías desde pequeños emprendimientos, entidades de tamaño medio, grandes corporaciones e incluso bancos se hace necesario que estas entidades cuenten con un departamento de sistemas con el suficiente conocimiento técnico y legal para poder hacer frente a estas situaciones. Pero como es de esperarse en las pequeñas y medianas empresas el contar con un profesional o grupo de profesionales dedicados a este aspecto de la ciberseguridad es muy inviable, por lo cual esta monografía busca que a través de las normas vigentes en Colombia en cuanto a los delitos informáticos y la Norma ISO /IEC 27037 de 2012, hacer un estudio de aquellos procedimientos que son requeridos con el fin de proteger la validez de las evidencias digitales en los casos judiciales por delitos informáticos, para finalmente generar o formular recomendaciones de tareas a realizar para complementar los procedimientos de recolección de evidencias digitales.

Con el fin de seguir estas buenas prácticas, se hace necesario tener el conocimiento de conceptos importantes para el área de la informática forense como que es la forensia en redes y la forensia digital, aspectos generales de los objetivos de la informática forense, ciencia forense, evidencia forense, evidencia digital su clasificación y su gestión y lo más importante de la recolección de evidencia que son sus criterios de admisibilidad ante la justicia colombiana.

Para entrar en contexto a tipo de delitos que se pueden cometer y para los cuales son necesarias estas evidencias, se ven aspectos generales de la ley 1273 del 5 de enero de 2009 además se describen las características de los delitos informáticos entre otros aspectos importantes.

Cabe destacarse que la monografía busca complementar las actividades propias de la recolección de evidencia digital en las pequeñas y medianas empresas por medio de un manual de buenas prácticas en el cual se ponga a disposición y conocimiento de los encargados de realizar este proceso.

1. PLANTEAMIENTO DEL PROBLEMA

Con los incesantes cambios en las tecnologías de la información en los últimos años, se hace necesario tener unos controles y garantías que soporten y den apoyo a los procesos legales ante delitos informáticos que puedan llegar a presentarse, por el uso inadecuado con fines ilícitos de las herramientas tecnológicas, tales como (equipos de cómputo, teléfonos inteligentes etc.)

Desde un entorno legal, se observan constantes falencias en la aplicación de los procesos propuestos en la norma ISO 27037 para la recolección de evidencias, las cuales dan unas buenas prácticas a seguir para la recolección adecuada de evidencia digital después de su hallazgo ”cadena de custodia”, puesto que al no aplicar dichos estándares o al seguir malas prácticas se podría interferir en un caso judicial, perdiendo su admisibilidad y quedando sin valor probatorio, siendo entonces una evidencia inútil como un elemento probatorio ante la Hipótesis de un caso judicial.

Haciendo referencia a la problemática en Colombia está el caso más representativo que es el del guerrillero colombiano Luis Edgar Devia Silva Reyes alias Raúl Reyes[1], pues la corte suprema dejo invalidas las pruebas en el computador de Raúl Reyes, donde se encontraron pruebas ilícitas para incriminar a congresistas como Wilson Borja debido a que para empezar, la recolección de evidencia se hizo de forma informal pues, esta evidencia se encontraba en el territorio de Ecuador y los encargados de la recolección de dichas evidencias debían ser las autoridades del gobierno ecuatoriano para que estas pudieran ser declaradas como válidas, sin embargo este proceso lo realizaron directamente los Colombianos cuando ingresaron sin autorización al territorio ecuatoriano[2].

También se presenta que muchas personas en Colombia al desconocer las normas colombianas vigentes pueden estarlas quebrantando sin tener conocimiento de ello, por el lado del criminal estas personas realizan actividades en los medios digitales con el fin de divertirse, experimentar o ganar dinero, por el lado de la víctima esta persona no tiene conocimiento de que son los delitos informáticos y como puede denunciarlos, el desconocimiento de la ley 1273 del 5 de enero de 2009 puede causar para la persona que cometiendo estos delitos penas entre los 48 y 96 meses de prisión y multas entre los 100 a 1000 salarios mínimos legales vigentes, el desconocimiento de esta ley para la victima podría ocasionar que los daños generados a su información, datos y sus sistemas de información por terceras

[1] Fernándes, 10 años de ‘Operación Fénix’ Muerte de Raúl Reyes sometió a las FARC. [en Línea], PanamPost 2018, [Consultado el 3 de agosto de 2019], Disponible en: https://panampost.com/felipe-fernandez/2018/03/05/operacion-fenix-raul-reyes/

[2] El Pais.com.co, Corte Suprema invalidó pruebas de computador de “Raúl Reyes.” [en Línea], (Colombia): El Pais.com.co 2011, [Consultado el 13 de septiembre de 2018], Disponible en: https://www.elpais.com.co/judicial/corte-suprema-invalido-pruebas-de-computador-de-raul-reyes.html

personas queden impunes legalmente, teniendo que asumir los costos que generó el ataque contra sus activos informáticos.
Debido a esto, se hace necesario realizar una investigación que permita generar recomendaciones de tareas y/o actividades a realizar para complementar los procedimientos de recolección de la evidencia digital teniendo en cuenta los delitos informáticos para evitar la pérdida y validez de la evidencia digital, por un cambio o modificación que se pudiera realizar por parte de la víctima o incluso del mismo personal encargado de la recolección de la evidencia en las pequeñas y medianas empresas.

1.1. FORMULACIÓN DEL PROBLEMA

La pregunta principal que sustenta este proyecto es la siguiente:
¿De qué manera un documento de buenas prácticas y procedimientos podría ayudar al personal encargado de la recolección de la evidencia digital en las pequeñas y medianas empresas para que esta no pierda su valor de admisibilidad y sirva como material de apoyo en un proceso legal?

2. JUSTIFICACIÓN

El presente proyecto se realiza con el fin de proveer un documento que sea útil como herramienta de apoyo para el proceso de recolección de evidencia digital en pequeñas y medianas empresas, aplicando estándares como la ISO /IEC 27037 de 2012 para el tratamiento de la evidencia digital, de esta forma se podrían evitar malas prácticas por el desconocimiento en la aplicación de las normatividades mencionadas, para prevenir que se llegue a perder la evidencia digital y no sea tenida en cuenta en procesos judiciales donde se analicen delitos informáticos o casos en los cuales se usaron dispositivos tecnológicos para cometer otro tipo de delitos.

Lo que busca esta norma es que las evidencias puedan aprovecharse al máximo en diferentes escenarios, los cuales se plantean tomando como referencia los delitos informáticos en la ley 1273 del 5 de enero de 2009 “de la protección de información y de los datos”, para contextualizar la clase de delitos para los cuales se pueden requerir evidencias y que clase de pruebas se podrían rescatar como constancia de estos delitos, haciendo todo lo que sea necesario para que estos delitos informáticos no queden impunes, pues para empezar uno de los principales factores de impunidad podría ser el desconocimiento de esta ley y la omisión de denuncia por parte de la víctima o la mala interpretación de alguno de sus artículos, la perdida de valides de la evidencia por tener cambios durante o luego de su recolección y finalmente la falta de evidencias debido a los deficientes procesos de investigación en el caso.

Finalmente se pretende generar unas recomendaciones para complementar el tratamiento de las evidencias digitales en casos de delitos informáticos en Colombia, colaborando con los encargados en los procesos de recolección de estas pruebas para conservar su cualidad de admisibilidad ante procesos judiciales.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Realizar un estudio del estado actual de la recolección de la evidencia digital donde se analicen las buenas prácticas de la ISO /IEC 27037 de 2012, relacionándola con los delitos informáticos de la ley 1273 del 5 de enero de 2009 en Colombia.

3.2. OBJETIVOS ESPECÍFICOS

- Recolectar información de casos relacionados con delitos informáticos ocurridos en Colombia.
- Tomar como referencia los delitos informáticos estipulados establecidos en la ley 1273 de 2009 para asociarlos con el procedimiento de recolección de evidencia en la ISO /IEC 27037.
- Caracterizar la documentación que se reúne en la monografía, para generar un manual de usuario con recomendaciones sobre el proceso de recolección de evidencia digital.

4. ALCANCES Y LIMITACIONES

El alcance del presente proyecto llega hasta la creación de un manual de usuario con recomendaciones sobre el proceso de recolección de evidencia digital en ambientes empresariales (pequeña y mediana empresa) de manera que no se invalide la evidencia digital y sirva como insumo ante la eventualidad de un proceso jurídico.

No se incluye el software utilizado para los diferentes procesos de recolección de la evidencia digital, aunque la mayoría del software utilizado es de uso libre puede que alguno de ellos requiera algún tipo de licenciamiento para su uso.

En suma, el trabajo permitirá guiar al personal de TI en el procedimiento para la obtención y recolección de la evidencia digital e incluso servirá como insumo y referente para el diseño y creación de procesos propios para la recolección de la evidencia con la que se garantice su admisibilidad en caso de un proceso jurídico o legal.

5. MARCO CONCEPTUAL Y TEORICO

5.1. MARCO DE ANTECEDENTES

La Seguridad informática y todos los temas relacionados con delitos informáticos en Colombia, es considerado como nuevo, la informática forense es una secuencia de elementos que permiten la acogida, estudio y procedimiento de la evidencia digital para que esta sirva como soporte ante algún evento legal.

Como referencia se toman algunos trabajos, publicaciones relacionados informática forense y el proceso de custodia.

El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos electrónicos. Publicación realizada por el Dr. Alexander Díaz García. Universidad Santiago de Cali. 2011. Facultad de Derecho. Dirección de Postgrados.

Dicho documento permite profundizar en conceptos fundamentales sobre delitos informáticos, sus principios, naturaleza y los elementos estructurales del delito.

ESET Security Report Latinoamérica 2014, informe que presenta una recopilación acerca del panorama actual de la seguridad informática para esta zona del continente.

El Proyecto para el mejoramiento del laboratorio del grupo investigativo de delitos informáticos del Cuerpo Técnico de Investigación (CTI) Pasto. Tesis presentada por Estefanía Muñoz Cerón, Universidad de Nariño, Facultad de Ingeniería Electrónica. San Juan de Pasto. 2014,

El trabajo en su estructura refiere la formulación de un proyecto para la adecuación del laboratorio de informática forense, haciendo referencia especialmente a la norma NTCISO/IEC 17025, que oriente a la Fiscalía General de la Nación en las actividades frente a la acreditación del laboratorio Forense del Grupo de Delitos Informáticos, el cual como punto de partida permite visualizar la necesidad de estandarizar los Procedimientos frente al tratamiento de la evidencia digital como elementos necesarios y obligatorios en una Norma Técnica de Calidad.

El documento del ministerio de las TIC de Colombia denominado SEGURIDAD Y PRIVACIDAD DE LA INFORMACION en el que se definen los lineamientos para realizar un proceso de informática forense adecuado, siendo a su vez un complemento al proceso de gestión de incidentes de seguridad de la información.

El trabajo de grado, estado del análisis forense digital en Colombia presentado por Diego Alejandro Jaramillo y Martha Liliana Torres en la Universidad militar Nueva Granada en el año 2016, el cual propone una verificación y recopilación de

documentos relacionados con el tema con el fin de tener una visión sobre la historia y estado actual del análisis digital forense en nuestro país.[3]

El trabajo aporta al proyecto un referente sobre cómo ha sido el tratamiento de la evidencia digital en nuestro país desde la llegada hasta la actualidad, permitiendo conocer y profundizar en todo lo relacionado con la normatividad vigente en Colombia.

5.2. MARCO CONCEPTUAL

Seguidamente se determinan las bases teórico-conceptuales de la terminología central usada en la estructuración de la propuesta y toda aquella relacionada con la informática forense.

5.2.1. La informática (o computación) forense:

Busca adquirir, preservar, obtener y presentar datos que han sido procesados y almacenados en un medio electrónico. La informática forense es una disciplina que apoya a los sistemas judiciales modernos, puesto que sirve como una herramienta para el procedimiento y procesamiento de la evidencia.

Los objetivos relacionados con informática forense son:

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

5.2.2. Uso de la Informática Forense[4]

Existen varios usos de la informática forense, estos usos provienen de la cotidianidad y no tienen que estar directamente relacionados con temas legales:

- Prosecución Criminal.
- Temas corporativos.
- Mantenimiento de la ley.
- Investigación de Seguros.

[3] Diego, J., & Torres, M., ESTADO DEL ANALISIS FORENSE DIGITAL EN COLOMBIA. [en Línea], Tesis de Maestria Universidad Militar Nueva Granada 2016, [Consultado el 18 de octubre de 2019], Disponible en: http://repository.unimilitar.edu.co/bitstream/10654/14401/1/TorresMoncadaMarthaLiliana2016.pdf

[4]Lopez, O. Informática Forense: generalidades, aspectos técnicos y herramientas. [en Línea], (Colombia): Universidad de los Andes 2001, [Consultado el 02 de noviembre de 2019], Disponible en: http://200.92.215.37/images/electronicos/Informatica/INFORMATICA-FORENSE-GENERALIDADES.pdf

- Litigación Civil.

Dentro las temáticas forenses se encuentran diferentes ramas[5]:

5.2.3. Computación forense

Es la disciplina de la computación forense en la que se consideran tareas relacionadas con la evidencia digital, busca y la información dispuesta en los dispositivos de almacenamiento con el propósito de establecer las acciones realizadas y formular hipótesis relacionadas con algún caso o evento.

5.2.4. Forensia en redes

Esta rama es considerada una de las más complicadas, pues busca comprender cual es la interacción de los protocolos, configuraciones e infraestructura tecnológica que en conjunto se acoplan para obtener un determinado suceso en el tiempo e incluso una conducta especial, que permita formar las acciones que una persona podría haber efectuado para concluir con su propósito.

5.2.5. Forensia digital

Es la forma en la que se aplican los diferentes conocimientos y protocolos de la ciencia criminalística a medios informáticos enfocados a apoyar la justicia, además de que busca el aclarar los sucesos que tuvieron lugar con algún dispositivo de almacenamiento digital (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como estafas entre otros delitos.

5.2.6. Ciencia Forense

La ciencia forense proporciona los principios y técnicas que facilitan la investigación del delito criminal o técnicas que pueden ser aplicadas con el fin de identificar, rescatar, reconstruir o estudiar la evidencia de un suceso criminal[6].
Las técnicas que apoyan a la recolección de evidencia digital son:

- Recoger y examinar huellas dactilares y ADN.
- Recuperar documentos de un dispositivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una huella digital por medio de algoritmos hash MD5 o SHA1

[5]Cano, J. Introducción a la informática forense. [en Línea], (Colombia): ACIS 2006, [Consultado el 23 de octubre de 2018], Disponible en: https://acis.org.co/archivos/Revista/96/dos.pdf
[6]Garcia, A., LA FORMACIÓN DE UN IRT (Incident Response Team) FORENSE.[en Línea], redalyc 2001 [Consultado el 11 de sempriembre de 2018], Disponible en: https://www.redalyc.org/pdf/5122/512251501006.pdf

5.2.7. Principio de transferencia de Locard

A continuación, se habla del principio de Locard establece que cualquier elemento A que entra en contacto con otro elemento B, transfiere parte de su información o materia entre estos elementos.

5.2.8. Evidencia Digital

Según Casey se define la evidencia de digital como “los datos que pueden establecer que un crimen se ha ejecutado o puede proporcionar un enlace (enlace) entre un crimen y su víctima o un crimen y su autor[7]”.

“Cualquier información que tiene intervención humana u otra semejante que ha sido extraída de un medio informático[8]”.

La evidencia computacional es frágil y la copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto importante de la evidencia es la posibilidad de realizar copias no autorizadas de archivos. Este medio permite la creación de inconvenientes relacionados con la investigación del robo de información corporativos, material investigativo, archivos de diseño realizados en computadoras y software[9].

Luego de que se produce un evento, por lo general, las partes involucradas en el ilícito intentan alterar las evidencias, intentando borrar los indicios o rastros que permitan dar muestra de los daños.

- La evidencia es de fácil borrado. Pero a pesar de que el registro se borre del equipo es muy posible recuperar este registro.
- Aun cuando se intentan eliminar las copias de seguridad en algunos casos existe copias que pueden llegar a estar ocultas en otros directorios.

5.2.9. Clasificación de las evidencias

Cano clasifica la evidencia digital que incluye párrafos de texto 3 categorías[10]:

- Generados por computadores.
- No generados sino almacenados.
- Registros híbridos.

[7] Eoghan., Digital Evidence and Computer Crime.3ra Edición, 2011.ISBN: 9780080921488
[8]Unoan1., Handbook Guidelines for the management of IT evidence. [en Línea], UNPAN 2004, [Consultado el 25 de julio de 2019], Disponible en: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016
[9] Deering, B. Data Validation Using The Md5 Hash. [en Línea],Forensics 2012, [Consultado el 13 de febrero de 2019], Disponible en: http://www.forensics-intl.com/art12.html
[10]Martines, C. Evidencia Digital. [en Línea],(Colombia): Universidad de los Andes 2005, [Consultado el 10 de octubre de 2019], Disponible en: http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

5.2.10. Criterios de admisibilidad

En legislaciones existen tres criterios que se deben tener en cuenta al momento de decidir sobre la admisibilidad de la evidencia.

5.2.11. Autenticidad: Una evidencia digital será autentica siempre y cuando se cumplan los siguientes elementos:

- El primero, demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos.
- La segunda, la evidencia digital debe mostrar que los medios originales no han sido modificados.

5.2.12. Confiabilidad: Los registros de eventos de seguridad son confiables si provienen de fuentes que son "creíbles y verificables.

Una evidencia digital es admisible si el "sistema que lo produjo no ha sido vulnerado y estaba en correcto funcionamiento[11]".

5.2.13. Completitud de las pruebas: las pruebas que se desean considerar deben ser pruebas con criterio o deben ser pruebas completas.

5.2.14. Delitos informáticos

De acuerdo con el convenio de ciber delincuencia del concejo de Europa el delito informático se define como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos[12]".

Estos delitos son muy difíciles de demostrar ya que en ocasiones encontrar las pruebas es complicado, estos delitos se pueden cometer en cuestión de segundos por el delincuente haciendo uso de un equipo tecnológico sin la necesidad de estar presencialmente en el sitio[13].

Tanto como avanza la tecnología, también evoluciona la forma de cometer estos delitos, por lo tanto, puede ser complicada la persecución al delincuente y la identificación de este.

---

[11]Cristancho, J. Evidencia Digital contexto. [en Linea], Bogotá (Colombia): Universidad de los Andes 2005,[Consultado el 13 de febrero de 2019], Disponible en: http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

[12] Europ, C. de. Convenio sobre la ciberdelincuencia. [en Línea], OAS 2001,[Consultado el 18 de enero de 2019], Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[13]Division Computer Forensic Recovery Labs. DEFINICIÓN DE DELITO INFORMÁTICO. [en Línea], Delitos Informáticos 2015, [Consultado el 7 de agosto de 2019], Disponible en:https://www.delitosinformaticos.info/delitos_informaticos/definicion.html

Los delitos informáticos en Colombia están clasificados en la ley 1273 del 5 de enero de 2009 creando el nuevo bien jurídico denominado “de la protección de la información y de los datos”.

La ley se compone de 2 capítulos, el primero “de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas de información”[14] , el capítulo segundo “de los atentados informáticos y otras infracciones[15]”.

Estos artículos describen varios delitos identificados por un número y código de artículo, tienen un nombre, una descripción breve y la pena de prisión que tiene cada uno de ellos, por ejemplo, el delito daño informático es el articulo 269D que indica que estos daños son producidos por personas no autorizadas para borrar o alterar datos informáticos o sistemas de información, estas personas pueden tener penas entre los 48 y 96 meses de prisión y multas de 100 a 1000 salarios mensuales vigentes.
Estos artículos hacen referencia a conductas delictivas como:

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos.

Cabe resaltar que conocer de primera mano los elementos dados por la legislación colombiana, sirve para tener un frente luego de ser víctima de conductas como los delitos informáticos, puede ayudar a la denuncia ya que se cuenta con el apoyo del CTI y la Policía Nacional a quienes se pueden reportar este tipo de delitos[16].

5.2.15. Características de los delitos informáticos.

[14] El congreso de la república de Colombia., Ley 1273 de 2009. [en Línea], (Colombia): Congreso de la República 2009, [Consultado el 28 de septiembre de 2019], Disponible en:http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf
[15] Ibid, P,24
[16] Molina, A. M. ¿QUÉ ES UN DELITO INFORMÁTICO? Cloud Seguro. [en Línea], (Colombia): Cloudseguro 2018, [Consultado el 18 de diciembre de 2019], Disponible en: https://www.cloudseguro.co/que-es-delito-informatico/

Julio Téllez Valdés menciona en su libro Derecho informático [17] características como:

- "Cuando el sujeto se halla trabajando, son acciones ocupacionales.
- Cuando se aprovecha una ocasión, son acciones de oportunidad.
- Ocasionan grandes pérdidas económicas, ya que además del daño en el bien jurídico, la reinversión que se debe hacer para la recuperación de este por lo general es grande.
- Se pueden generar sin estar físicamente en el sitio y sin algún límite de tiempo.
- Por su carácter técnico son complicados de comprobar y verificar.
- Son sofisticados y frecuentes en el ámbito laboral.
- Por la falta de regulación legal, pocas veces son denunciados.
- Requieren de regulación, ya que tienden a proliferarse.
- Solo personas con ciertos conocimientos pueden llegar a cometerlos" [18].

5.2.16. ISO / IEC 27037: 2012

La norma ISO 27037 de 2012 "Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence" [19] genera unas pautas para las actividades relacionadas con el manejo de la evidencia digital que pueda ser de valor probatorio.

Da una orientación a las personas en cuanto a situaciones comunes que se puedan encontrar durante los procesos que se den durante el manejo de la evidencia digital, facilitando el intercambio de esta entre sus jurisdicciones, renovando las antiguas directrices de RFC 3227 ya que la ISO 27037 está más enfocada a las situaciones que se puedan dar en esta época, dirigiéndose a técnicas actuales[20].

Las actividades para las cuales se dan recomendaciones son la identificación, adquisición, recolección y preservación de las evidencias digitales.

Dentro de las personas a las cuales se dirige esta metodología están los DEFRs "Digital Evidence First Responders" o los primeros responsables de evidencia

[17]Valdés, J. T. V. Derecho Informatico. Instituto de Investigaciones Jurídicas Universidad Nacional Autónoma de México. [en Línea], (Mexico): Derecho Informatico 2017, [Consultado el 28 de julio de 2018], Disponible en: https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

[18]Anonimo. Características de los delitos informáticos. [en Línea], AngelFire 2017, [Consultado 19 Agosto del 2018],Disponible en https://www.angelfire.com/la/LegislaDir/Defin.html

[19]Iso.org. ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. [en Línea], ISO.ORG 2012,[Consultado el 13 de julio de 2019], Disponible en: https://www.iso.org/standard/44381.html

[20]Rodrigues, R. ISO/IEC 27037:2012 Nueva norma para la Recopilación de Evidencias. PeritoIT. [en Línea], Peritoit 2012, [Consultado el 28 de agosto de 2019], Disponible en: https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/

digital, los DESs también conocidos como especialistas en respuesta de incidentes y finalmente los gerentes de laboratorios forenses.

De otro lado, va dirigido a informar a las personas que toman las decisiones para determinar la confiabilidad de estas evidencias digitales que son presentadas ante ellos. Puntualmente a las organizaciones que protegen, analizan y presentan las potenciales evidencias, como los organismos de control [21].

5.2.17. Estructura de los delitos informáticos.

5.2.17.1. Sujeto activo

Tienen habilidades y amplia experiencia manejando sistemas de información, esto generalmente gracias a su situación laboral ya que se posicionan en lugares estratégicos donde se utiliza información sensible de las organizaciones, sin embargo, también pueden ser hábiles aun sin desempeñar actividades laborales.

Lo que difiere entre ellos en realidad es el delito cometido, por lo tanto, la persona que accede a un sistema sin autorización es diferente de la persona que está contratada en una organización para trabajar en el área de sistemas y se aprovecha de su conocimiento para el desvío de fondos[22].

5.2.17.2. Sujeto pasivo

Es la víctima, la persona titular del bien jurídico en la cual recae la actividad del sujeto activo, sobre el recaen todas las acciones cometidas por el sujeto pasivo, estos sujetos pasivos pueden pertenecer al gobierno, instituciones, individuos, entre otros, que utilizan sistemas generalmente de información que están conectados entre otros[23].

5.2.18. Bien jurídico protegido – tutelado

El bien jurídico protegido de acuerdo con la definición penal[24], se entiende como la intimidad personal localizada en la morada, cualquier persona puede ser víctima de delitos, se pueden dar en el mundo real o el mundo virtual, este último bien llamado delitos informáticos y que en su mayoría resultan impunes, desvirtuados por la falta de adecuación de la normatividad vigente a la actualidad de las circunstancias nuevas que nos rodean.

---

[21] Quezada, A. Introducción a ISO/IEC 27037:2012. ReYDeS. [en Línea], Reydes 2015, [Consultado el 07 de enero de 2019], Disponible en: http://www.reydes.com/d/?q=Introduccion_a_ISO_IEC_27037_2012

[22] Acuario del pino, S. Delitos Informáticos: Generalidades. [en Línea], OAS 2007, [Consultado 11 septiembre del 2018],Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[23] Ibid p.26

[24] Ibid p.26

Los delitos informáticos se concretan mediante herramientas virtuales y sistemas informáticos, que tiene como objetivo principal la violación de cualquiera de los bienes jurídicos tutelados por ley protegidos por el Derecho Penal en cualquier momento dado, entre ellos se puede destacar la propiedad privada y la protección para quienes crean obras artísticas o literarias previstas por la Ley[25].

5.2.19. La seguridad informática.

Es una disciplina que tiene como misión proteger la privacidad e integridad de la información [26]que es almacena en un sistema informático.

Dentro de las funciones que realiza están: el proceso de prevenir y detectar uso no autorizado dentro de los sistemas informáticos comprende medidas de seguridad como la implementación, uso de software antivirus, firewalls [27] y UTM, las medidas de seguridad dependen principalmente del entorno tecnológico del que disponga la persona para asegurar.

El conjunto de herramientas, estrategias y procedimientos para la seguridad de la información [28] deben asegurar estos tres principios:

- Integridad: Solo los usuarios autorizados pueden acceder a los recursos, datos e información y modificarlos si es necesario, hace referencia a que los datos no tienen ningún tipo de alteración por terceras personas o software malicioso[29].
- Disponibilidad: es la capacidad de garantizar que los datos y el sistema están disponibles cuando se requiere[30].
- Confidencialidad: La información es accesible solo para el personal autorizado, por lo tanto, es necesario generar acciones que peritan prevenir que la información se divulgue a personas o sistemas no autorizados[31].

[25]Barbosa, R, Derecho informático. Editorial Digital Tecnológico de Monterrey. [en Línea], (México): Monterrey 2013,[Consultado 17 de Noviembre de 2019], Disponible en http://prod77ms.itesm.mx/podcast/EDTM/ID042.pdf

[26] Definición.de. SEGURIDAD INFORMÁTICA. [en Línea], Definiciones de 2012, [Consultado el 30 de marzo de 2019], Disponible en:https://definicion.de/seguridad-informatica/

[27]Universidad Internacional de Valencia. ¿Qué es la seguridad informática y cómo puede ayudarme? Universidad Internacional de Valencia. [en Línea], (España): Universidad Internacional de Valencia 2016, [Consultado el 01 de octubre de 2019], Disponible en: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

[28] Significados.com. Significado de Seguridad informática. Significados.Com. [en Línea], Significados 2019, [Consultado el 13 de febrero de 2019], Disponible en: https://www.significados.com/seguridad-informatica/

[29] Firma-e. Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad. Firma-E. [en Línea], Firme-e 2014, [Consultado el 12 de diciembre de 2018], Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

[30] INFOSEGUR. Objetivos de la seguridad informática. INFOSEGUR. [en Línea], Infosegur 2013, [Consultado el 21 de marzo de 2019], Disponible en: https://infosegur.wordpress.com/tag/integridad/

[31] pmg-ssi.com. ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? Pmg-Ssi.Com. [en Línea], PMG-SSI 2017, [Consultado el 03 de noviembre de 2019], Disponible en: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

- No repudio: el emisor comunica un mensaje que llega exactamente a la persona que corresponde, además el emisor y el receptor no pueden negar que existe comunicación.

Toda esta seguridad se logra atacando y protegiendo frentes como la red, el software y el hardware, por lo tanto, en la red se estará protegiendo la infraestructura de amenazas como los virus, intrusiones por parte de hackers, ataques de denegación de servicios entre otros.

A nivel de hardware este se debe proteger de accesos no autorizados o de daños intencionales, finalmente a nivel de software este debe protegerse de ataques maliciosos de modo que se pueda tener confianza en el correcto funcionamiento del software[32].

5.2.20. Evidencia digital

La evidencia digital puede provenir desde dispositivos digitales, redes, bases de datos, entre otros, haciendo referencia a los datos existentes en formato digital, a partir de la ISO 27037 de 2012 no se espera abarcar la conversión de datos analógicos en formatos digitales[33].

En términos generales, es todo valor probatorio de datos almacenados o transmitidos en formato digital, para que pueda ser usada en un juicio[34], pero para esto se debe determinar si la prueba es auténtica, pertinente para el caso, es real o es un rumor, además determinar si una copia es aceptable para llevar el caso o se hace necesario el contar con la evidencia digital original.

Estas posibles fuentes de datos, de forma más específica pueden ser[35]:

- Computadoras de escritorio y portátiles.
- Dispositivos de almacenamiento en red.
- Celulares, cámaras digitales, grabadoras de video y audio.
- Servidores web, DHCP, FTP, VoIP, cualquier servicio de filesharing o de correo electrónico.
- Medios digitales como: discos ópticos, USB, discos magnéticos, discos duros externos, memorias microSD, cintas, entre otros.

[32] Universidad Internacional de Valencia. Tres tipos de seguridad informática que debes conocer. Universidad Internacional de Valencia. [en Línea], (España): Universidad Internacional de Valencia 2016, [Consultado el 06 de noviembre de 2018], Disponible en: https://www.universidadviu.com/es/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer/

[33] Quezada, A. Introducción a ISO/IEC 27037:2012. ReYDeS. [en Línea], Reydes 2015, [Consultado el 07 de enero de 2019], Disponible en: http://www.reydes.com/d/?q=Introduccion_a_ISO_IEC_27037_2012

[34] Macudi. La Evidencia Digital. En Informatica Foresnse Colombia. [en Línea], (Colombia): Informatica Forense 2017, [Consultado el 20 de agosto de 2019], Disponible en: https://www.informaticaforense.com.co/la-evidencia-digital

[35]Mintic., Evidencia Digital. [en Línea], (Colombia): Mintic 2016, [Consultado el 08 de octubre de 2019], Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

- Logs de dispositivos de seguridad como IDS, Firewalls, Proxy, plataformas Antispam que sean consolidados en algún sistema de gestión de eventos e información de seguridad SIEM [36].
- Logs de elementos en red como los routers puntos de acceso entre otros.
- Registros de proveedores de servicios (estos son solicitados solo bajo órdenes judiciales).

Todo elemento valido para el caso es aquel que demuestra tener un valor probatorio, por lo tanto, tiende a demostrar y a buscar la verdad.

De acuerdo con la legislación, la evidencia que no posee valor probatorio es inadmisible permitiendo que esta sea excluida de un proceso de investigación siendo objetada por oposición de un abogado, en conclusión, para que una prueba digital pueda ser aceptada, el valor de esta debe tener la posibilidad de ser sopesado frente a su naturaleza perjudicial[37].

Estas evidencias pertenecen a la categoría de pruebas frágiles, ya que por su origen pueden ser fácilmente destruidos o modificados, por lo tanto, otra de las condiciones para que una prueba sea admisible será que esta no ha sido alterada o ha tenido cambios o modificaciones desde que fue recogida en la escena del crimen.

5.2.21. Cadena de Custodia

La cadena de custodia es el proceso de gran relevancia en la informática forense, ya que en él es donde se debe determinan los compromisos u elementos de control relacionado al personal que interviene o está en contacto con las evidencias.[38]

Dentro del proceso de cadena de custodia se debe diligenciar un formato en el que se registran los datos completos de los actores que tienen relación con el proceso de las copias, este proceso establece todos los hechos desde su creación a partir de la evidencia, hasta el momento en que se almacena. Dicho documento debe contener información cómo, cuándo, dónde y quién tuvo contacto con la evidencia, también sus nombres completos, su cargo, las fechas y horas exactas; adicional a esto también se debe registrar los datos del custodio de la evidencia, el tiempo que esta estuvo bajo su poder y dónde fue guardada; también es de gran importancia si se presenta o se requiere cambiar de guardián se debe registrar el evento del cuándo y cómo se produce el canje, al igual que los datos de la persona que trasladó la evidencia[39].

[36] Rouse, M. Gestión de eventos e información de seguridad (SIEM). [en Línea], Searchdatacenter.Techtarget 2017, [Consultado el 02 de agosto de 2018], Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM
[37] I Macudi. Op.Cit p28
[38] Arellano, L. E. y Castañeda, C. M. La cadena de custodia informáticoforense.[en Línea], (Colombia): ACTIVA 2012, [Consultado 15 de septiembre de 2018], Disponible en: Revista ACTIVA, 3, 67–81.
[39] Quezada, A. C. Op Cit p28

El proceso de la cadena de custodia es mantener y preservar la integridad tanto física como lógica del material probatorio o evidencia. Esta preservación se debe llevar a cabo desde el instante de la recolección o registro, su almacenamiento, transporte y análisis hasta culminar con la entrega a las autoridades judiciales o al ente de control que corresponda.

Las evidencias deben contar con una algunas características especiales desde la recolección conservación y transporte las cuales serán enunciadas a continuación:[40]

- Los indicios digitales, generalmente se encuentran cifrados y almacenados en un espacio digital específico, lo cual quiere decir que todo tipo de información se encuentra guardada.
- Existen diferencias entre el elemento que contiene la información y su contenido, es decir, la misma información. Para esto se considera lo siguiente:
  - La información hace referencia al conocimiento que puede ser referido a un hecho u objeto y que puede ser cifrado y almacenado.
  - El objeto se refiere a un conjunto que se pueda determinar físicamente o que se pueda definir lógicamente.

- La presentación de la información puede estar establecida por alguno de los estados que se indican a continuación:
  - Almacenada: indica que se encuentra guardada en un almacenamiento que puede ser primario, secundario o terciario y que se encuentra lista para ser accedida. Este es un estado estático y se puede tener acceso a la información bien sea por medios locales o remotos.
  - En desplazamiento: indica que se encuentra transportándose por algún medio físico y su recolección se puede dar por la interceptación de dicho medio, teniendo en cuenta las leyes que cobijan la interceptación de comunicaciones o la violación de correspondencia.
  - En proceso: es el estado más complejo y hace parte de la primera decisión que se debe tomar por parte de la persona encargada de la recolección. Al estar en uso un equipo de cómputo, la información se encuentra en proceso, es decir, se modifica, se actualiza y vuelve a ser almacenada, entonces se 39 debe decidir si se apaga o no el equipo de cómputo. Esta es una decisión vital ya que de ella depende la posible pérdida de la información y la alteración o daño de la posible evidencia que se quiere recolectar.

[40] ibid

5.3. MARCO LEGAL

A continuación, se relacionan los componentes que hacen parte de la normatividad y legislación que rige y controla el comportamiento de los ciudadanos de Colombia y son importantes cuando se habla de ciber seguridad.

- La constitución política de Colombia 1991.
- El decreto 1360 del año 1989 el cual relaciona todos los derechos de autor y software, que se reglamentaria mediante los artículos 51 y 52 del capítulo IV de la ley 44 de 1993 en la cual se establecen una serie de conductas que modifican el código penal mediante la ley 599 de 2000, en su capítulo séptimo del libro segundo donde hacen referencia a la violación de la intimidad, reserva e interceptación de comunicaciones.
- Ley 600 de 2000 en el cual se establece el código de procedimiento penal colombiano.
- Ley 679 de 2001, establece parámetros para advertir y contrarrestar la explotación, la pornografía y el turismo sexual con menores de edad y su respectivo uso de medios tecnológicos.
- La resolución No-0-1890 de noviembre de 2002, de la fiscalía general de la nación, reglamenta el artículo de la ley 600 del año 2000. El cual establece las responsabilidades de la entidad para dirigir y manejar los cargos órganos que estipula la ley que garantizan los procedimientos penales en conjunto con la autenticidad e identidad de los elementos físicos que servirán como material probatorio.
- La Resolución 0-2869 de diciembre 29 de 2003, de la Fiscalía General de la Nación “refiere la necesidad de establecer el manual que permita desarrollar los procedimientos de cadena de custodia, adoptado mediante resolución 0-1890 de noviembre 5 de 2012[41].
- La Ley Estatutaria 1266 de 2008, de hábeas data y otras disposiciones, involucra al tema del dato personal, refiriendo textualmente: “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que pueden asociarse con una persona natural o jurídica” y que más adelante sería modificada y regulada por la Ley 1581 de 2012 denominada de “Hábeas Data” la cual protege el derecho que tenemos todas las personas a conocer, actualizar y rectificar la información que reposen en bancos de datos de entidades públicas y privadas[42] .
- La Ley 1273, promulgada en el año 2009 por el Congreso de la Republica, por medio de la cual se modificó el código penal y se creó un nuevo bien

[41] Fiscalia General de la Nación., Policía Judicial. Informativo Interno Huellas. [en Línea],(Colombia): Fiscalia General de la Nación 2019, [Consultado el 13 de marzo de 2019], Disponible en: https://www.redjurista.com/Documents/resolucion_2869_de_2003_fiscalia_general_de_la_nacion.aspx

[42] Congreso de la República., Ley 1266 de 2008. [en Línea], Bogotá (Colombia): Congreso de la republica 2008, [Consultado el 16 de septiembre de 2018], Disponible en: https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1266-2008.

jurídico denominado “De la protección de la información y de los datos”, que se preservan integralmente.

Esta Ley incluyó un nuevo título al Código Penal Colombiano denominado “De la Protección de la información y de los datos”, enmarcado en dos capítulos: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos” y “De los atentados informáticos y otras infracciones”. En contexto estos capítulos clasifican una serie de Delitos:

- Suplantación de sitios WEB.
- Hurto por medios informáticos.
- El acceso abusivo a un sistema informático.
- Violación de datos personales.
- La obstaculización ilegítima del sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Uso de software malicioso.
- Daño informático.
- Transferencia no autorizada de activos[43].
- Ley 527 DE 1999, define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones, frente a la aceptación y probatoria de los mensajes de información o datos estos serán admisibles como medios de prueba[44].
- La norma Técnica ISO/IEC 17025 Internacional, contiene los requisitos que tienen que cumplir los laboratorios de ensayo y calibración, de cara a la aplicación de un sistema de gestión en el proceso de certificación, demostrando técnicamente componentes para generar resultados válidos[45].
- El documento CONPES 3701: establece Lineamientos de Política para seguridad y ciberdefensa. “enfocados al desarrollo de estrategias que contrarresten el incremento de las amenazas informáticas que afectan al país y que recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

[43]El congreso de la república de Colombia, Op. Cit p 24
[44] El congreso de la República de Colombia., LEY 527 DE 1999. [en Línea], (Colombia): Congreso de la República 1999, [Consultado el 28 de septiembre de 2019], Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html
[45] Icontec. Norma Técnica Colombiana ISO17025. [en Línea], (Colombia): Invima 2018, [Consultado el 11 de agosto de 2019], Disponible en: https://www.invima.gov.co/images/pdf/red-nal-laboratorios/resoluciones/NTC-ISO-IEC_17025-2005.pdf.

6. DISEÑO METODOLÓGICO

A partir punto de la metodología, el trabajo se está desarrollado por medio de acciones descriptivas y explicativas reunidas en este trabajo, por lo tanto, se identifican, recolectan y analizan elementos suficientes para proporcionar una visión sobre la evidencia digital respecto a la normatividad de los delitos informáticos en Colombia ley 1273 de 2009.

De acuerdo con el aporte o definición presentada por Manuel Luis Rodríguez en su publicación sobre el tema, la define como: “un proceso sistemático y secuencial de recolección, selección, clasificación, evaluación y análisis de contenido del material empírico impreso y gráfico, físico y/o virtual que servirá de fuente teórica, conceptual y/o metodológica”.[46]

El uso aplicado de esta metodología de investigación permite el uso de técnicas y herramientas para localizar, identificar, analizar y obtener información relevante.

Etapas basadas en “los criterios de selección de la pertinencia, exhaustividad y actualidad”, presentados por Manuel Rodríguez, los cuales permiten inicialmente

- La definición de los tipos de fuentes bibliográficas y documentales, acordes con los objetivos de la presente investigación.
- La clasificación de las fuentes bibliográficas consultadas en función de la investigación y que, en su contenido aporten datos significativos para la construcción del documento.
- La verificación de las fuentes de consulta frente a su actualización, con el fin de garantizar que su aporte este acorde con la normatividad legal en Colombia y de las normas internacionales sobre el tratamiento de la evidencia digital y los procedimientos vigentes.

De esta forma se presentan a continuación las experiencias obtenidas por diferentes entidades y casos en el país algunos de gran renombre otros no tanto, pero todos en conjunto hacen parte elemental del proceso de recolección indebida de evidencias.

[46] Rodríguez, M. L. ACERCA DE LA INVESTIGACIÓN BIBLIOGRÁFICA Y DOCUMENTAL. [en Línea], Guiadetesis 2013, [Consultado el 01 de agosto de 2018], Disponible en: https://guiadetesis.wordpress.com/2013/08/19/acerca-de-la-investigacion-bibliografica-y-documental/

7. RESULTADOS

7.1. CASOS DE EJEMPLO

A continuación, se describen algunos hechos sucedidos en Colombia en los cuales se pierde la admisibilidad de la evidencia digital por la ejecución de malas prácticas en los procedimientos de recolección de la evidencia digital o el desconocimiento legal que protege o ampara a las victimas ante estos hechos.

En el artículo publicado por el periódico el tiempo el día 17 de enero de 2018 titulado “Denuncias por delitos informáticos crecieron el 31 % el año pasado” se identifica que las denuncias por delitos como Ciber pirámides pornografía infantil, venta de drogas y armas, estafas, inducción al suicidio, secuestro de información, hurto a cuentas bancarias y tarjetas de crédito, extorsiones sexuales, suplantación de personas han aumentado a 11.332 respecto al mismo periodo del año anterior.

Tabla 1. Estadísticas Ciberdelitos Fiscalía Colombia

Fuente: el autor

De los casos más denunciados estuvo el de una empresa en el norte de Bogotá en la cual encriptaron toda la información del área contable en la que solicitaban grandes sumas de dinero a cambio de las claves para acceder a la información el pago era exigido en bitcoins.

Se encontró que se violó información de servidores en Holanda bloqueando uno a uno todos los filtros de seguridad[47].

7.1.1. Sector empresarial

En un año las denuncias por delitos informáticos aumentaron del 5 al 28 por ciento la mayoría de los casos sucede por suplantación de correos electrónicos empresariales, donde se solicita datos de información sensible de la empresa como la confirmación de pagos o transferencias a cuentas bancarias especificas; en estos casos se detectó que los atacantes conocen los cargos, nombres y funciones de las personas entre las cuales se intercambian este tipo de correos todo esto a través de ataques de ingeniería social y phishing.
Este tipo de ataques dejo para el año 2016 pérdidas de más de 600 millones de dólares a nivel nacional[48].

7.1.2. Caso Nicolas Castro

El estudiante de la universidad Jorge Tadeo Lozano Nicolas Castro fue denunciado por Jerónimo Uribe hijo del expresidente y ahora senador Albaro Uribe Vélez ante la Fiscalía General de la Nación, denunciando la creación de una página en la red social Facebook donde claramente manifestaba amenazas de muerte.
Debido a que Jerónimo Uribe como demandante tenía un gran poder, ya que en ese momento su padre era el presidente electo de la república, el caso estuvo sujeto a todo tipo de abusos y violaciones al debido proceso por parte del ente acusador. La inocencia de Nicolas Castro se determinó a través de las evidencias digitales presentadas ante el juez, ya que la prueba era una copia de un chat sostenido entre el acusado y su novia en formato Microsoft Word copiado y pegado desde Microsoft Messenger. La evidencia fue catalogada como invalida puesto que carecía de un contexto valido y carecía de características como Integridad, Autenticidad y no repudio con lo cual fue absuelto de las acusaciones[49].

En este caso se demostró el desconocimiento de los entes encargados de recolectar, presentar y mantener la evidencia digital.

[47] Cortés, N. . Denuncias por delitos informáticos crecieron el 31 % el año pasado. [en Linea], Bogotá (Colombia): El Tiempo 2017,[Conusltado el 23 de septiembre de 2018], Disponible en: https://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

[48] Semana. Aumenta el número de empresas víctimas de delitos cibernéticos en Colombia. Semana. [en Línea],(Colombia): Semana 2017[Consultado el 24 de julio de 2019], Disponible en: https://www.semana.com/nacion/articulo/presentan-informe-sobre-el-cibercrimen-en-colombia/520236/

[49] Lombana, J. Radicado de denuncia de jeronimo uribe por amenazas y terrorismo.[en Línea], (Colombia): 2018, [Consultado el 13 de julio de 2019], Disponible en: http://farm3.static.flickr.com/2784/4489237955_e77280e244_b.jpg

7.1.3. Caso ISA S.A.

Uno de los empleados de la empresa abre un correo electrónico en el que el remitente era una dirección de correo electrónico con el mismo dominio de la empresa, por el sentido de urgencia del mensaje el empleado descarga el archivo adjunto y descomprime el adjunto. Luego de esta acción se desencadeno la propagación del software informático denominado RANSOMWARE en el equipo y posteriormente en la red LAN afectando 5 equipos de dicha empresa.

En el suceso aconteció que se perdió información relevante del negocio como:

- Información del estado de las garantías.
- Datos de las importaciones.
- Datos de comprobantes de pago de los clientes.
- Datos de repuestos de vehículos, entre otros.

No fue posible recuperar esta información la cual tenía más de 5 años de antigüedad, a pesar de que el negocio se vio afectado la empresa no realizo la correspondiente denuncia ya que por desconocimiento no conocía los canales o medios para realizarla.

Con el fin de recuperar la operación de la empresa los equipos fueron formateados, acto que desencadeno en la destrucción de la evidencia digital, segundo acto que ocasiono que las malas acciones de la víctima provocaron que este delito quedara impune sin la posibilidad de localizar al atacante[50].

7.1.4. Caso Fedimel

En esta empresa aconteció que uno de los empleados del área de contabilidad intentaba descargar un elemento de internet, pero por desgracia lo que descargo fue un archivo con una variante del virus RANSOMWARE provocando una infección en los servidores de aplicaciones y base de datos de la entidad. Para este suceso los administradores optaron por intentar realizar la recuperación de los archivos infectados por medio de utilitarios de software libre, este proceso fue de gran impacto para la compañía puesto que tuvieron que reprocesar información de aproximadamente 6 meses puesto que la última copia funcional era de esta fecha.

Por desconocimiento de las normatividades se realizó una respectiva denuncia de los hechos acontecidos, pero ya no se contaba con la evidencia digital de este suceso causando que la denuncia no se procesara de forma adecuada[51].

[50] Gutierres, A. C. ISA S:A. [Entrevista], (Colombia), Kennertech SAS 2018.
[51] Sarmiento, J., Fedimel [Entrevista], (Colombia), Kennertech SAS 2018.

7.1.5. Caso Alianza

La entidad del sector financiero sufre una infección de tipo ransomware en una de las estaciones que tienen full acceso al servidor de base de datos de la entidad, por tal motivo la entidad se ve obligada a detener sus actividades. La entidad muy diligentemente realizo la denuncia formal ante la policía por medio de la plataforma disponible para estos hechos. A el servidor afectado se le realizo el proceso respectivo de creación de imagen mediante el programa FTK ya que el personal quiere realizar pruebas para recuperar alguna información que no tenían respaldada.
Se restableció el servicio configurando de cero, en un servidor alterno que la entidad tiene en el cual se instaló, el motor de BD y se restauró toda la data teniendo como perdida o reproceso de trabajo un aproximado de 2 horas.[52]

7.1.6. Inadmisión pendrive como prueba penal

A continuación, se relaciona la sentencia ocurrida en España STC114/1984, de 29 noviembre del 84 en la cual se desestiman unas pruebas recopiladas por medio de dispositivos electrónicos en los cuales se recurre a argumentos como:

- No reconoce exactamente que fuese la voz del cliente.
- No es un medio fehaciente probatorio.
- No tenía conocimiento de que estuviese siendo grabado.

En el caso, aunque no sucede concretamente en Colombia se tiene un claro ejemplo de que los malos procesos de recolección de las evidencias pueden llevar a la impugnación de hechos acontecidos con premeditación.
Para este caso el procedimiento debió haber notificado previamente a la persona que podía estar siendo grabado, de esta forma el implicado no podrá argumentar o defenderse mediante los Artículos 18.1 y 18.3 de la CE en los cuales se habla de la intimidad y el secreto de las comunicaciones.

7.1.7. Evidencia clave para judicializar implicados en delitos informáticos.

.
A continuación, se relacionan algunos delitos informáticos ocurridos en Colombia en los cuales se logró dictaminar o decidir la culpabilidad de los implicados por medio de evidencia digital encontrada en el lugar de los hechos.

[52] Gomez, W. Alianza [Entrevista], (Colombia), Kennertech SAS 2018.

7.1.8. El acceso indebido a datos o sistemas informáticos ART 269A

13 policías capturados por acceder de forma abusiva a sistemas informáticos.[53] En coordinación la Policía Nacional y la Fiscalía General de la Nación hicieron un operativo en el cual se lograron 16 órdenes judiciales efectivas, 13 de ellas contra miembros de la institución adscritos a la metropolitana de Barranquilla.
La policía Nacional encontró que los 13 uniformados a través de una herramienta que les permite tener información sobre vigencias de seguros obligatorios y revisión técnico-mecánica de automotores estarían incurriendo en el delito de acceso abusivo a sistema informático para obtener beneficios personales exigiendo dádivas a cambio de no aplicar la norma.
Los policías enfrentaron cargos por delitos como acceso abusivo a sistemas informáticos, concusión, peculado por uso, abuso de funciones públicas, prevaricato por omisión y concierto para delinquir con agravación punitiva.
Los tres restantes delincuentes enfrentaron delitos como concierto para delinquir, concusión como interviniente y acceso abusivo a sistemas informáticos.

7.1.9. Fraudes y estafas informáticas ART 269J - ART 269I – 269F

Unas 20 personas fueron capturadas en el Eje Cafetero por desocupar cuentas bancarias a través de estafa informática[54].
Las aprehensiones se dieron en departamentos como Quindío, Caldas y Risaralda; los delincuentes compraban bases de datos de tarjetas débito y crédito a los funcionarios de los bancos y engañaban a las víctimas a través de llamadas telefónicas.
La investigación fue realizada por la Seccional de Investigación Criminal (SIJIN) en coordinación con Incocredito y la fiscalía.
Los capturados deberán responder por el delito de concierto para delinquir con fines de violación de datos personales, ya que se habrían apropiado de más de 1.200 millones de pesos haciendo uso de diferentes modalidades, según el coronel Luis Hernando Benavides, en el operativo se incautaron 112 discos duros, 3 servidores, 1 mini datafono, 1 grabadora, 3.949 folios y 14 cuadernos con bases de datos de tarjetas bancarias

[53] RCN RADIO. Policías capturados por acceder de forma abusiva a sistemas informáticos.[en Línea],(Colombia): RCN 2019, [Consultado el 27 de agosto de 2019], Disponible en: https://www.rcnradio.com/colombia/caribe/13-p olicias-capturados-acceder-forma-abusiva-sistemas-informáticos s
[54]Bonilla, R.. Unas 20 personas fueron capturadas en el Eje Cafetero por desocupar cuentas bancarias a través de estafa informática. [en Línea], (Colombia): RCN 2014, [Consultado 14 de octubre de 2018], Disponible en https://noticias.canalrcn.com/nacional-justicia/1 1-capturados-estafas-clientes-

7.1.10. Phishing ART 269A – ART 269I

El ladrón de las millas de los famosos[55].
De la ciudad de Neiva, Jaime Alejandro Solano de 23 años imito voces de empleados de aerolíneas para encontrar los primeros datos de sus víctimas.
Luego de esto a través del phishing, falsifico el sitio web LifeMiles
Dentro de sus víctimas se encuentran celebridades como Juanes, Sofía Vergara, Iván Villazón, Laura Acuña, Carolina Cruz, entre otros correos electrónicos a las víctimas, haciendo la solicitud de actualización de datos.
Con las millas que logró obtener, hizo viajes a Estados Unidos, México, África, Río de Janeiro y otros destinos nacionales.
Además de las millas, el joven obtenía ilegalmente datos de tarjetas de crédito con las que pagó los impuestos de los tiquetes adquiridos con las millas.
Tiene prisión domiciliaria condenada por transferencia no consentida de activos, violación de datos personales y hurto por medio informático [56]

7.1.11. Suplantación de identidad digital

Joven que fue suplantada en redes vive una terrible pesadilla[57].
Jennifer Alba fue suplantada en la red social Instagram ya que crearon una cuenta con el mismo nombre de usuario, pero con una letra diferente, finalmente agregaron a las personas conocidas de ella y suplantaron su identidad.
De acuerdo con la Policía nacional, el delito primario es el de la violación de datos personales que da entre 4 y 8 años de prisión.
Además, según los aportes de la DIJIN hasta febrero de 2018 había cerca de 1.314 denuncias por suplantación de cuentas en redes sociales de Colombia.
También se considera delito que una persona utilice sus fotografías publicadas en redes sociales sin su autorización y para actuaciones que no son de su conocimiento.

7.1.12. Daño informático ART 269D

Capturan a juez involucrado en el caso Hyundai[58].
La fiscalía general de la nación capturó a Reinaldo Huertas que es el juez sexto civil del circuito de Bogotá, por presunta manipulación en el reparto en el caso Hyundai.
Se le imputaron delitos como la utilización ilícita de redes informáticas, daño informático agravado, cohecho impropio y acceso abusivo a sistema informático.

---

[55] El Tiempo., El ladrón de las millas de los famosos. EL Tiempo. [en Línea],(Colombia): El Tiempo 2016, [Consultado el 15 de julio de 2018], Disponible en: https://www.eltiempo.com/justicia/cortes/delitos -de-hackers-en-colombia-52232.
[56] Franco, M. El ladron de Millas. [en Línea],(Colombia): Soho (2017).[Consultado el 1 de octubre de 2019], Disponible en: http://www.soho.co/historias/articulo/el-ladronde-millas-viajo-por-el-mundo-a-costa-de-los-fa mosos/40745
[57] Castro, R. El robo de identidad y sus cifras en América Latina. [en Línea], welivesecurity 2011, [Consultado 14 de octubre de 2018], Disponible en: https://www.welivesecurity.com/la-es/2011/04/0
[58] El Economista. México, entre los más afectados por el malware Wanna Cry. [en Línea], (Mexico): El Economista 2018, [Consultado el 13 de abril de 2019], Disponible en: https://www.eleconomista.com.mx/tecnologia/Mexico-entre-los-mas-afectados-por-el-malware-Wanna-Cry-20180510-0067.html

7.2. LA EVIDENCIA DIGITAL COMO MATERIAL PROBATORIO EN COLOMBIA.

En cualquier proceso legal, la información que se transmite de forma digital sirve como evidencia en un juicio, para llegar a esta instancia las evidencias digitales deben ser admitidas por un tribunal el cual es el encargado de determinar si es aceptable una copia o es requerido el original.

En Colombia más allá de unas normas, leyes o elementos regulatorios de obligatoriedad existen algunos procedimientos establecidos por las entidades competentes, los cuales permiten dar una idea o bosquejo de lo que se debe contemplar y establecer al momento de una recolección de la evidencia. Algunas de las instituciones mencionadas con anterioridad son:

- Fiscalía General de la Nación con el documento titulado “MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA”[59].
- MINTIC con su guía para denominada “Seguridad y Privacidad de la Información Evidencia Digital”[60].

Estos documentos están basados en estándares y normas internacionales como lo es la ISO 27307 DEL 2012 que permiten hacer una gestión adecuada del material probatorio. Gracias a que se cuenta con un marco estandarizado en materia de informática forense, se puede garantizar la admisibilidad de la evidencia digital, para atender un procedimiento penal o civil.

Los avances tecnológicos, sumado a las tendencias en herramientas especializadas a la informática forense, los litigios penales y civiles conllevan a plantear un reordenamiento de la realidad de las entidades y empresas.

Ahora las administraciones públicas, más que nunca deben estar atentas a los cambios que son o serán objeto de protección y tutela jurídica. Todo en concordancia con los elementos de naturaleza electrónica, soportado en la informática forense, como eje principal de una prueba.

Algo muy importante al momento de hacer una correcta recolección de evidencia digital dentro de los entornos corporativos “Pequeñas y Medianas Empresas” es la obtención de los diferentes permisos y derechos para ejecutar estos procesos o se podría estar incurriendo en actos ilícitos.

[59] Fiscalia General de la Nación. MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA. [en Línea],(Colombia): Fiscalia General de la Nación 2012, [Consultado el 13 de marzo de 2019], Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf

[60] Mintic., Evidencia Digital. [en Línea], (Colombia): Mintic 2016, [Consultado el 08 de octubre de 2019], Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

En algunos entornos corporativos y sobre todo en las pequeñas y medianas empresas se suele tener la mala práctica de permitir que los empleados manejen o trabajen desde dispositivos de su propiedad para efectos de una recolección de evidencia digital, se podría complicar la situación dado que sin los permisos respectivos del propietario del equipo dicha evidencia podría ser considerada como invalida, es por ello que siempre se sugiere aprovisionar a los empleados con equipos propiedad de la compañía, por este medio se lograra una recolección sin problemas, si bien el dispositivo es de propiedad de la compañía, la misma podrá disponer del dispositivo cuando lo desee y/o mejor convenga.

7.2.1. Estándar ISO/IEC 27037:2012

De acuerdo con los estándares ISO/27037:2012 se manejan tres principios internacionales que permiten establecer un análisis respecto a la relevancia, confiabilidad y suficiencia de la evidencia digital, estos puntos o principios permiten generar un entorno de entendimiento y trabajo sobre el cual se plantean las mejores prácticas y procedimientos para la recolección de la evidencia digital.

Tabla 2 Estándar ISO/IEC 27001

Principio	**Contexto**	**finalidad**	**utilidad**
Relevancia	Condición jurídica que contempla elementos analizados bajo la pertinencia de los mismos respecto del caso.	Probar o no la hipótesis planteada a partir de la exclusión del material que resulte irrelevante	Si se encuentran elementos que no cumplan esta condición deben ser excluidos
Confiabilidad	Permite desde la parte técnica facilitar la contradicción.	Valida la respetabilidad y auditabilidad aplicado para la obtención de evidencia	Si un tercero sigue el mismo proceso debe obtener los mismos resultados.
Suficiencia	Permite entender la experiencia y formalidad del perito	Valida si las evidencias recolectadas y analizadas tienen elementos suficientes para sustentar los hallazgos	Analiza la completitud de las pruebas

Fuente: Adaptación del autor

7.3. PROCEDIMIENTO DE RECOLECCIÓN EVIDENCIA DIGITAL

Antes de iniciar con los pasos que se proponen a continuación, es necesario verificar que el evento que está siendo objeto de recolección en realidad atenta contra la confidencialidad, integridad o disponibilidad de la información.

Se plantean los siguientes pasos para realizar una correcta recolección de la evidencia digital.

- Aislamiento de la escena: en este punto se restringe el acceso a la zona del incidente, para evitar algún tipo de alteración en la posible evidencia a recolectar.
- Identificación de fuentes de información: Los datos relacionados con un evento especifico son identificados y evaluados a su vez que el incidente se controla, para posteriormente proceder con la fase de recolección.
- Examinación y recolección de información: Son todas aquellas técnicas y herramientas forenses que se pueden aplicar a los datos recolectados para extraer información relevante, sin alterar la integridad de este.

7.3.1. Aislamiento de la escena

Tan pronto como se cataloga el evento como un incidente de seguridad de la información, es necesario restringir el acceso a la zona donde se produce el evento con el fin de evitar cualquier alteración o contaminación de la evidencia.

- Dentro de la ejecución de esta actividad lo más recomendable es realizar una toma en video o con fotografías del sitio donde están dispuestos los elementos que serán objeto del aislamiento y en general de todo el procedimiento realizado.
- Posterior a ello se requiere sellar los puertos USB, Unidades CD/DVD con el fin de impedir alguna extracción de elementos, aquí es muy importante emplear medio o elementos como las etiquetas de seguridad.
- Ahora bien, si el equipo de cómputo se encuentra encendido, no se debe apagar y se deberá proceder con la toma de fotografías o video de los elementos que se encuentran en ejecución y es muy importante que se pueda apreciar la fecha y hora en la que se realiza.
- Adicional a esto se deben verificar los puertos lógicos que se puedan encontrar abiertos, junto con la tabla arp del dispositivo en donde se pueda

apreciar las diferentes direcciones Mac que con las cuales se ha establecido una comunicación.

- Luego de esto se debe proceder con el apagado forzoso a el equipo (esto se puede aplicar con equipos de mesa) se desconecta el cable de energía del equipo sin ejecutar o indicarle alguna orden de apagado, esto permitirá posteriormente la extracción de los elementos guardados en la memoria volátil (RAM).
- Si el equipo se encuentra apagado, no realizar el encendido, puede alterar la escena y/o causar borrado de información que podría lograr obtenerse posteriormente.
- En este punto se debería almacenar los dispositivos en un sitio con acceso restringido, para garantizar la cadena de custodia de la información.
- Complementario a esto se debe recolectar información de los demás elementos que tuvieron contacto o interacción con el equipo en cuestión tal como (Firewall, Puntos de acceso inalámbrico entre otros).

Anteriormente se mencionaba la **cadena de custodia** en la cual se decía que es un procedimiento en el cual se detallan las actividades minuto a minuto que se realizan con la evidencia digital en todo el proceso de recolección por lo cual se establece un principio de mismidad que no es más que asegurar que lo que se encontró es lo mismo que se presenta ante el ente penal o disciplinario.

Por lo cual se propone un modelo o línea base de cadena de custodia la cual se encuentra en el **ANEXO C**.

7.3.2. Identificación de fuentes de información

Lo primero que se debe realizar para recolectar o encontrar la información es identificar los siguientes elementos:

- Servidores WEB, DHCP, CORREO, FTP entre otros.
- Elementos de almacenamiento en la red.
- Medios de almacenamiento externo como: USB, CD/DVD, Discos Ópticos, Discos duros, Memorias SD entre otros.
- Dispositivos celulares, PDAs, Cámaras Digitales, Grabadores de video.
- Computadores de mesa y portátiles.
- Logs de dispositivos de red como IDS, Firewall, antivirus, Proxy, SIEM, switches o routers.

7.3.3. Examinación y recolección de información

Como primera medida y como ya se había planteado con anterioridad se debe ir diligenciando el formato de cadena de custodia.

7.3.3.1. Imagen de datos

El personal encargado de la recolección de la evidencia digital debe contar con dispositivos de almacenamiento sanitizados lógicamente, dispositivos de inicio en caliente con elementos de protección de escritura, en el cual se debe contener el software para la autenticación y creación de la copia de la evidencia digital.

Las copias o imágenes que se realizan de los dispositivos deben ser creadas bit a bit para poder extraer toda la información contenida en el disco duro, en los que se incluyan todos los ficheros borrados, ocultos entre otros.

El software empleado para estos fines debe cumplir con algunas características especiales:

- El software debe tener acceso a discos tipo SCSI e IDE.
- Se debe emplear elementos de hardware que bloqueen la escritura para asegurar que el dispositivo accedido no sea alterado.
- El software debe validar la integridad de la información generada.
- El software no debe alterar el disco original.
- El software debe registrar errores de entrada y salida, de igual forma debe notificar si el dispositivo de origen es de mayor o menor tamaño que el destino.

En este punto se deberían considerar emplear o emplear software de creación de copias bit a bit como lo son:

- FTK IMAGER.
- Encase Forensic Software.
- Acronis Cloud Backup.
- LINUX dd.

7.3.3.2. Recolección Y Registros De Evidencia Digital En Medios Volatiles (RAM)

Los equipos que se encuentran encendidos, se les debe realizar un proceso especial para tomar la información contenida en los dispositivos de almacenamiento volátil. Como lo son las memorias RAM en la cual al momento de que el equipo es apagado de forma controlada pierde la información contenida.[61]

El almacenamiento volátil es el encargado de mostrar todo el funcionamiento actual del sistema operativo junto con todas las herramientas y procesos que se encuentran en ejecución, además del estado de la cola de impresión, así como las conexiones de red que se encuentran activas y los puertos TCP/UDP abiertos.

Para acceder a dispositivos de almacenamiento volátil se debe:

- Hacer el debido registro de las diferentes aplicaciones que se relacionen con los puertos mencionados en el anterior ítem.
- Hacer el registro de hora, fecha y zona horaria del sistema.
- Hacer el registro de los procesos que se encuentren en ejecución.
- Hacer el registro de los tiempos en que se crean, acceden y modifican todos los archivos.
- Hacer la debida documentación de todas las tareas y los comandos que se llevaron a cabo durante este proceso de recolección.
- Identificar los usuarios que tengan sesión abierta.
- Identificar y registrar los puertos que se encuentren abiertos.
- Validar la integridad de la información.
- Validar y hacer el registro de todas las conexiones de red activasen el momento o recientemente.
- Verificar y registrar la fecha y hora actual del sistema.

Después de esto, lo ideal es hacer una recolección más específica y estricta sobre la información contenida en el almacenamiento volátil, para lo cual se debe hacer lo siguiente[62]:

- Hacer la verificación de la legitimidad de los comandos del sistema operativo.
- Hacer una revisión sobre la base de datos o los módulos del núcleo del sistema operativo.
- Identificar y extraer la información que se encuentre en la memoria RAM.

[61] Gimeno, J. M. ,Pruebas y evidencias telemáticas. [en Línea], (España): Universitat Politècnica de València 2015, [Consultado el 27 de junio de 2018], Disponible en: https://riunet.upv.es/bitstream/handle/10251/55392/Magraner - Pruebas y evidencias telemáticas..pdf?sequence=1&isAllowed=y

[62] Ibid

- Identificar y extraer los archivos de configuración más importantes del sistema operativo.
- Revisar y obtener los registros de eventos del sistema.
- Validar y obtener los archivos con las claves del sistema operativo.

7.3.3.3. Verificación de Integridad de la evidencia.

Al momento de realizar la recolección de la evidencia digital para posteriormente ser trasladada y analizada es muy importante que el personal encargado realice las siguientes acciones:

- Certificar por medio de alguna tecnología (hash, o cadena de bloques, por ejemplo) la evidencia, una herramienta muy útil en este proceso podría ser **Acronis Notary** incluido dentro del paquete de recursos de **AcronisCyber Backup Cloud**
- Hacer registro de la evidencia obtenida dentro del formato de cadena de custodia.
- Elaborar un acta en presencia de testigos.

7.3.3.4. Creación de una copia de la imagen suministrada.

Previo al respectivo envió de la evidencia al laboratorio forense para su análisis, se debe realizar una copia de la imagen creada previamente, dado que los análisis de la información se deben procurar no realizar en la imagen original.

Es decir, se tiene que garantizar el siguiente escenario:

- Equipos originales o material de estudio.
- Copia o imagen máster (Recolectada en primera instancia).
- Copia secundaria la cual se crea a partir de la copia Máster y es la que será entregada al laboratorio forense.
- Copias terciarias si se requieren, estas son creadas en el laboratorio forense y se emplean para verificar diferentes elementos de una imagen o copia de información creada.

Esta jerarquía y garantizando la correcta verificación de integridad permitirá garantizar una correcta recolección y cadena de custodia.

7.3.3.5. Aseguramiento de la imagen original suministrada y elementos objeto del análisis.

Se debe asegurad que la imagen o copia máster no tenga ningún tipo de modificación para conservar la cadena de custodia y su calidad de validez jurídica.

En este punto es muy importante contar con elementos como los siguientes:

- Bolsas Antiestáticas.
- Cinta.
- Bolsas de recolección de evidencia.
- Papel de embalaje" burbuja".
- Etiquetas de seguridad.

Los elementos mencionados con anterioridad se emplean para todo el etiquetado y rotulado de la información. En estos elementos se debe diligenciar las fechas, horas de guardado y quien realiza cada proceso. Esta información debe coincidir con la registrada dentro de los formatos de cadena de custodia garantizando así la protección. La importancia de que los elementos físicos originales no se requieran es producto de que se realiza la correcta recolección, pero en caso de que sean requeridos deben estar almacenados y custodiados durante todo el proceso disciplinario o legal.

Para este punto se debería tener el siguiente escenario:

- Archivo de cadena de custodia, con datos de todas las personas que intervienen durante el proceso incluyendo los testigos.
- Video o fotografías del escenario de análisis.
- Procedimiento fotografiado o filmado, del procedimiento de extracción y copia de las evidencias.
- Verificación de integridad de la información por medio de tecnología tipo hash o cadena de bloques.
- Rotulado de la información y/o evidencias.
- Guardado y embalaje de los discos, equipos, celulares entre otros.
- Bitácora de cadena de custodia con cada uno de los procedimientos realizados, con hora y nombre de quien lo realiza.

7.3.3.6. Movilización de la evidencia digital

El traslado de la evidencia digital obtenida se hace para el laboratorio forense que se estipulo en el procedimiento pericial. El tiempo que la evidencia reposara en

dichas instalaciones sebera asegurar y mantener todo el protocolo de la cadena de custodia.[63]

7.4. Software y hardware propuesto para la recolección de la evidencia digital.

7.4.1. Hardware

Se plantea entonces así los siguientes elementos tecnológicos o hardware que se requieren para la recolección de la evidencia digital.

- Discos Duros externos mínimo de 1 tb de capacidad de almacenamiento
- Bloqueador de lectura y escritura
- Adaptadores para bloqueadores
- Equipo portátil o de mesa com software necessário.

Ilustración 1 Hardware para recolección de evidencia digital

Fuente: Edición del autor

[63]Arellano, L. E. y Castañeda, C. M. La cadena de custodia informáticoforense.[en Línea], (Colombia): ACTIVA 2012, [Consultado 15 de septiembre de 2018], Disponible en: Revista ACTIVA, 3, 67–81..

Ilustración 2 Bloqueadores de Disco y Adaptadores

Fuente: Edición del autor

7.4.2. Software

En materia de recolección de evidencia digital existen herramientas especializadas según la línea de investigación por lo cual se proponen las más eficientes para recolección de evidencia digital.

Estas herramientas permiten generar copias exactas de un disco o una partición de un disco duro, algunas de las más utilizadas en el mercado son:

Ghost: realizar imágenes o copia por contenido o partición específica, también está en la funcionalidad copiar discos de gran tamaño.

Disponible en: http://www.portalprogramas.com/norton-ghost/

Acronis: este software puede realizar la copia bit a bit de los servidores y equipos sin importar el SO con todos sus componentes como lo puede ser la Base de datos, esta operación tiene la ventaja de tener entornos especializados en la nube para simplemente almacenar las copias como para restaurarlas, dentro de sus cualidades más usadas está el **NOTARY** basado en tecnología de bloques el cual permite notarizar o garantizar las versiones de un fichero muy similar a la tecnología usada en hash.

Disponible en: https://www.acronis.com/es-mx/

FTK Imager. Es una herramienta especializada en la extracción y análisis de dispositivos tipo volátil. Permitiendo exportar los procesos de la memoria en un

fichero, logrando de esta forma la posibilidad de demostrar los procesos en la memoria RAM y allí apreciar la información relevante del proceso.

KALI: Distribución Linux especializada en ciberseguridad, creada a partir de Debian, el sistema operativo es muy empleado en el mundo de la ciberseguridad ya que permite realizar desde análisis de vulnerabilidades, gestión de reportes, entre otros utilitarios y categorías dentro del mismo se puede encontrar todo un conjunto de herramientas destinado a la informática forense.

Disponible en:https://www.kali.org/

FTK Imager Lite este software se trabaja mediante volcado de memoria para dispositivos móviles con el fin de conseguir evidencia luego del respectivo análisis.

Disponible en: http://accessdata.com/product-download/ftkimager

8. CONCLUSIONES

Los constantes avances tecnológicos en materia de ciberseguridad hacen que día a día las compañías requieran más elementos de control como firewalls, WAF, IDS, IPS y SIEM por mencionar solo algunos de ellos. Estos elementos requeridos en su totalidad para poder garantizar la seguridad, confidencialidad y disponibilidad de la información. Pero en ocasiones estos elementos sumados no son suficiente control para prevenir la afectación de los activos de información, es en estos escenarios que se hace imperativo el contar con un equipo que dé respuesta a estos incidentes el cual este en la capacidad de realizar una correcta recolección de la evidencia digital.

Ahora bien, es de vital importancia que al interior de las compañías estos procedimientos se realicen por medio de protocolos establecidos, adecuados y estandarizados. Que permitan realizar una recolección de evidencia digital. Todo enmarcado dentro de los estándares y normativas legales vigentes que puedan permitir la admisibilidad de la información como soporte para casos legales.

Con lo mencionado a lo largo del documento y gracias al trabajo realizado el personal técnico de las pequeñas y medianas empresas tendrán un elemento de soporte y control que les podrá guiar para tomar y recabar las evidencias de las diferentes fuentes, y en conjunto con la normatividad y la clasificada en la ley 1273 del 2009 podrán reportar estas acciones para que los entes disciplinarios y legales puedan sancionar las acciones de estas personas o delincuentes.

De este modo surge la necesidad de investigadores o profesionales capacitados en la búsqueda y recolección de evidencias digitales que sirvan como apoyo a los casos judiciales, dichas pruebas serán validadas si y solo si se cumple y se ejecuta con rigor el proceso de recolección de la evidencia digital soportado en la cadena de custodia la cual garantiza la veracidad de la evidencia.

Habiendo realizado un procedimiento adecuado para la cadena de custodia y su uso para el análisis de delitos informáticos, se aprecia que algunas de las falencias y errores más comunes de las empresas consiste en no tener una correcta capacitación y formación en los procedimientos o técnicas de recolección de evidencia digital.

9. RECOMENDACIONES

Las siguientes recomendaciones surgen como propuesta o puntos para mejorar o quizás sirvan para futuros proyectos.

Diseñar material didáctico he ilustrativo, que permita el fortalecimiento, capacitación y habilidades del personal técnico mediante prácticas que permitan el afianzamiento de las habilidades obtenidas producto del presente proyecto, esto garantizara el correcto entendimiento.

Crear una herramienta tecnológica que permita la práctica de la recolección de la evidencia tecnológica, que permita identificar las buenas prácticas o falencias de las personas que la realicen.

Mantener actualizados los procedimientos de acuerdo con las nuevas tendencias tecnológicas que se implementen en la industria, esto para garantizar el cumplimiento a nivel normativo para la recolección de la evidencia digital.

Mantener actualizada la normativa de acuerdo con los diferentes entes regulatorios que apliquen de acuerdo con el sector u objeto del negocio, dado que en el presente documento se aplican las generalidades de la ley sin entrar al detalle en las diferentes normas o leyes dispuestas por cada ente regulador. Como por ejemplo la super intendencia de industria y comercio.

Realizar un plan de auditoria que contemple monitoreo al proceso para identificar mejoras o fallas planteadas en el procedimiento.

BIBLIOGRAFÍA

Acuario del pino, S. *Delitos Informáticos: Generalidades*. [en Línea], OAS 2007, [Consultado 11 septiembre del 2018],Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Anonimo. *Características de los delitos informáticos*. [en Línea], AngelFire 2017, [Consultado 19 Agosto del 2018],Disponible en https://www.angelfire.com/la/LegislaDir/Defin.html

ARCINIEGAS, D. A. J. y MONCADA, M. L. T. M. (2016). Estado Del Análisis Forense Digital En Colombia. [en Linea], *IOSR 2016,* [Consultado 15 de septiembre de 2018], Disponible en: *Journal of Economics and Finance* (Vol. 3, Issue 1). https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/MT_Globalization_Report_2018.pdf%0Ahttp://eprints.lse.ac.uk/43447/1/India_globalisation%2C society and inequalities%28lsero%29.pdf%0Ahttps://www.quora.com/What-is-the

Arellano, L. E. y Castañeda, C. M. La cadena de custodia informáticoforense.[en Línea], (Colombia): ACTIVA 2012, [Consultado 15 de septiembre de 2018], Disponible en: *Revista ACTIVA*, *3*, 67–81.

Barbosa, R., Derecho informático. *Editorial Digital Tecnológico de Monterrey*. [en Línea], (México): Monterrey 2013,[Consultado 17 de Noviembre de 2019], Disponible en http://prod77ms.itesm.mx/podcast/EDTM/ID042.pdf

Bonilla, R.. *Unas 20 personas fueron capturadas en el Eje Cafetero por desocupar cuentas bancarias a través de estafa informática*. [en Línea], (Colombia): RCN 2014, [Consultado 14 de octubre de 2018], Disponible en https://noticias.canalrcn.com/nacional-justicia/1 1-capturados-estafas-clientes-bancos

Caballero Velasco, M. Á., y Cilleros Serrano, D. (La Evidencia Digital) Análisis Forense.[en Línea], *El libro del hacker 2018* (p. 429).[Consultado 11 de octubre del 2018], Disponible en https://www.casadellibro.com/libro-el-libro-del-hacker-ed-2018/9788441539648/6023315

Cano, J. *Introducción a la informática forense*. [en Línea], (Colombia): ACIS 2006, [Consultado el 23 de octubre de 2018], Disponible en:]https://acis.org.co/archivos/Revista/96/dos.pdf

Castro, R. *El robo de identidad y sus cifras en América Latina*. [en Línea], welivesecurity 2011, [Consultado 14 de octubre de 2018], Disponible en: https://www.welivesecurity.com/la-es/2011/04/0

Congreso de la República., *Ley 1266 de 2008*. [en Línea], Bogotá (Colombia): Congreso de la republica 2008, [Consultado el 16 de septiembre de 2018], Disponible en: https://www.habitatbogota.gov.co/transparencia/normatividad/normatividad/ley-1266-2008

Cortés, N. . *Denuncias por delitos informáticos crecieron el 31 % el año pasado*. [en Linea], Bogotá (Colombia): El Tiempo 2017,[Conusltado el 23 de septiembre de 2018], Disponible en: https://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

Cristancho, J., *Evidencia Digital contexto*. [en Linea], Bogotá (Colombia): Universidad de los Andes 2005,[Consultado el 13 de febrero de 2019],Disponible en: http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

Deering, B. *Data Validation Using The Md5 Hash*. [en Línea],Forensics 2012, [Consultado el 13 de febrero de 2019], Disponible en: http://www.forensics-intl.com/art12.html

Definición.de. *SEGURIDAD INFORMÁTICA*. [en Línea], Definiciones de 2012, [Consultado el 30 de marzo de 2019], Disponible en:https://definicion.de/seguridad-informatica/

Diego, J., & Torres, M., *ESTADO DEL ANALISIS FORENSE DIGITAL EN COLOMBIA*. [en Línea], (Colombia): Universidad Militar Nueva Granada 2016, [Consultado el 18 de octubre de 2019], Disponible en: http://repository.unimilitar.edu.co/bitstream/10654/14401/1/TorresMoncadaMarthaLiliana2016.pdf

Division Computer Forensic Recovery Labs. *DEFINICIÓN DE DELITO INFORMÁTICO*. [en Línea], DelitosInformaticos 2015, [Consultado el 7 de agosto de 2019], Disponible en:https://www.delitosinformaticos.info/delitos_informaticos/definicion.html

El congreso de la República de Colombia., *LEY 527 DE 1999*. [en Línea], (Colombia): Congreso de la República 1999, [Consultado el 28 de septiembre de 2019], Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

El congreso de la república de Colombia., *Ley 1273 de 2009*. [en Línea], (Colombia): Congreso de la República 2009, [Consultado el 28 de septiembre de 2019], Disponible

en:http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

El Economista. *México, entre los más afectados por el malware Wanna Cry*. [en Línea], (Mexico): El Economista 2018, [Consultado el 13 de abril de 2019], Disponible en: https://www.eleconomista.com.mx/tecnologia/Mexico-entre-los-mas-afectados-por-el-malware-Wanna-Cry-20180510-0067.html

El Pais.com.co., *Corte Suprema invalidó pruebas de computador de "Raúl Reyes."* [en Línea], (Colombia): El Pais.com.co 2011, [Consultado el 13 de septiembre de 2018], Disponible en: https://www.elpais.com.co/judicial/corte-suprema-invalido-pruebas-de-computador-de-raul-reyes.html

El Tiempo., *El ladrón de las millas de los famosos*. EL Tiempo. [en Línea],(Colombia): El Tiempo 2016, [Consultado el 15 de julio de 2018], Disponible en: https://www.eltiempo.com/justicia/cortes/delitos -de-hackers-en-colombia-52232.

Eoghan., *Digital Evidence and Computer Crime.3ra Edición, 2011.**ISBN:** 9780080921488*

Europ, C. de. *Convenio sobre la ciberdelincuencia*. [en Línea], OAS 2001,[Consultado el 18 de enero de 2019], Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Fernándes, A. . *10 años de 'Operación Fénix' Muerte de Raúl Reyes sometió a las FARC*. [en Línea], PanamPost 2018, [Consultado el 3 de agosto de 2019], Disponible en: https://panampost.com/felipe-fernandez/2018/03/05/operacion-fenix-raul-reyes/

Fernándes, A. . *10 años de 'Operación Fénix' Muerte de Raúl Reyes sometió a las FARC*. [en Línea], PanamPost 2018, [Consultado el 3 de agosto de 2019], Disponible en: https://panampost.com/felipe-fernandez/2018/03/05/operacion-fenix-raul-reyes/

Firma-e. *Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad*. Firma-E. [en Línea], Firme-e 2014, [Consultado el 12 de diciembre de 2018], Disponible en: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

Fiscalia General de la Nación. *MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA*. [en Línea],(Colombia): Fiscalia General de la Nación 2012, [Consultado el 13 de marzo de 2019], Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf

Fiscalia General de la Nación., *Policía Judicial. Informativo Interno Huellas*. [en Línea],(Colombia): Fiscalia General de la Nación 2019, [Consultado el 13 de marzo de 2019], Disponible en: https://www.redjurista.com/Documents/resolucion_2869_de_2003_fiscalia_general_de_la_nacion.aspx

Franco, M. *El ladron de Millas*. [en Línea],(Colombia): Soho (2017).[Consultado el 1 de octubre de 2019], Disponible en: http://www.soho.co/historias/articulo/el-ladronde-millas-viajo-por-el-mundo-a-costa-de-los-fa mosos/40745

Garcia, A. , *LA FORMACIÓN DE UN IRT (Incident Response Team) FORENSE*.[en Línea], redalyc 2001 [Consultado el 11 de sempriembre de 2018], Disponible en: **https://www.redalyc.org/pdf/5122/512251501006.pdf**

Gimeno, J. M., *Pruebas y evidencias telemáticas*. [en Línea], (España): Universitat Politècnica de València 2015, [Consultado el 27 de junio de 2018], Disponible en: https://riunet.upv.es/bitstream/handle/10251/55392/Magraner - Pruebas y evidencias telemáticas..pdf?sequence=1&isAllowed=y

Gomez, W. ,*Alianza, [Entrevista]*, (Colombia), Kennertech SAS 2018.

Gutierres, A. C. *ISA S:A. [Entrevista]*, (Colombia), Kennertech SAS 2018.

Icontec. *Norma Técnica Colombiana ISO17025*. [en Línea], (Colombia): Invima 2018, [Consultado el 11 de agosto de 2019], Disponible en: https://www.invima.gov.co/images/pdf/red-nal-laboratorios/resoluciones/NTC-ISO-IEC_17025-2005.pdf

INFOSEGUR. *Objetivos de la seguridad informática*. INFOSEGUR. [en Línea], Infosegur 2013, [Consultado el 21 de marzo de 2019], Disponible en: https://infosegur.wordpress.com/tag/integridad/

Iso.org. *ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. [en Línea], ISO.ORG 2012,[Consultado el 13 de julio de 2019], Disponible en: https://www.iso.org/standard/44381.html

Lombana, J. *Radicado de denuncia de jeronimo uribe por amenazas y terrorismo*.[en Línea], (Colombia): 2018, [Consultado el 13 de julio de 2019], Disponible en: http://farm3.static.flickr.com/2784/4489237955_e77280e244_b.jpg

Lopez, O. *Informática Forense: generalidades, aspectos técnicos y herramientas*. [en Línea], (Colombia): Universidad de los Andes 2001, [Consultado el 02 de noviembre de 2019], Disponible en: http://200.92.215.37/images/electronicos/Informatica/INFORMATICA-FORENSE-GENERALIDADES.pdf

Macudi. La Evidencia Digital. En Informatica *Foresnse Colombia*. [en Línea], (Colombia): Informatica Forense 2017, [Consultado el 20 de agosto de 2019], Disponible en: https://www.informaticaforense.com.co/la-evidencia-digital

Martines, C. *Evidencia Digital*. [en Línea],(Colombia): Universidad de los Andes 2005, [Consultado el 10 de octubre de 2019], Disponible en: http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf

Mintic. *Evidencia Digital*. [en Línea],(Colombia): Mintic 2016, [Consultado el 16 de junio de 2019], Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Mintic., *Evidencia Digital*. [en Línea], (Colombia): Mintic 2016, [Consultado el 08 de octubre de 2019], Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Molina, A. M. *¿QUÉ ES UN DELITO INFORMÁTICO?* Cloud Seguro. [en Línea], (Colombia): Cloudseguro 2018, [Consultado el 18 de diciembre de 2019], Disponible en: https://www.cloudseguro.co/que-es-delito-informatico/

pmg-ssi.com. *¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información?* Pmg-Ssi.Com. [en Línea], PMG-SSI 2017, [Consultado el 03 de noviembre de 2019], Disponible en: https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

Quezada, A. *Introducción a ISO/IEC 27037:2012*. ReYDeS. [en Línea], Reydes 2015, [Consultado el 07 de enero de 2019], Disponible en: http://www.reydes.com/d/?q=Introduccion_a_ISO_IEC_27037_2012

RCN RADIO. *Policías capturados por acceder de forma abusiva a sistemas informáticos*.[en Línea],(Colombia): RCN 2019, [Consultado el 27 de agosto de 2019], Disponible en: https://www.rcnradio.com/colombia/caribe/13-p olicias-capturados-acceder-forma-abusiva-sistemas-informáticos

Rodrigues, R. *ISO/IEC 27037:2012 Nueva norma para la Recopilación de Evidencias*. PeritoIT. [en Línea], Peritoit 2012, [Consultado el 28 de agosto de 2019], Disponible en: https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/

Rodríguez, M. L. *ACERCA DE LA INVESTIGACIÓN BIBLIOGRÁFICA Y DOCUMENTAL*. [en Línea], Guiadetesis 2013, [Consultado el 01 de agosto de 2018], Disponible en: https://guiadetesis.wordpress.com/2013/08/19/acerca-de-la-investigacion-bibliografica-y-documental/

Rouse, M. *Gestión de eventos e información de seguridad (SIEM)*. [en Línea], Searchdatacenter.Techtarget 2017, [Consultado el 02 de agosto de 2018], Disponible en: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-eventos-e-informacion-de-seguridad-SIEM

Sarmiento, J. *Fedimel [Entrevista]*, (Colombia), Kennertech SAS 2018..

Semana. Aumenta el número de empresas víctimas de delitos cibernéticos en Colombia. *Semana*. [en Línea],(Colombia): Semana 2017[Consultado el 24 de julio de 2019], Disponible en: https://www.semana.com/nacion/articulo/presentan-informe-sobre-el-cibercrimen-en-colombia/520236/

Significados.com. *Significado de Seguridad informática*. Significados.Com. [en Línea], Significados 2019, [Consultado el 13 de febrero de 2019], Disponible en: https://www.significados.com/seguridad-informatica/

Universidad Internacional de Valencia. *¿Qué es la seguridad informática y cómo puede ayudarme?* Universidad Internacional de Valencia. [en Línea], (España): Universidad Internacional de Valencia 2016, [Consultado el 01 de octubre de 2019], Disponible en: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

Universidad Internacional de Valencia. *Tres tipos de seguridad informática que debes conocer*. Universidad Internacional de Valencia. [en Línea], (España): Universidad Internacional de Valencia 2016, [Consultado el 06 de noviembre de 2018], Disponible en: https://www.universidadviu.com/es/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer

Unoan1., *Handbook Guidelines for the management of IT evidence*. [en Línea], UNPAN 2004, [Consultado el 25 de julio de 2019], Disponible en: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016

Valdés, J. T. V. *Derecho Informatico*. Instituto de Investigaciones Jurídicas Universidad Nacional Autónoma de México. [en Línea], (Mexico): Derecho Informatico 2017, [Consultado el 28 de julio de 2018], Disponible en: https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

ANEXOS

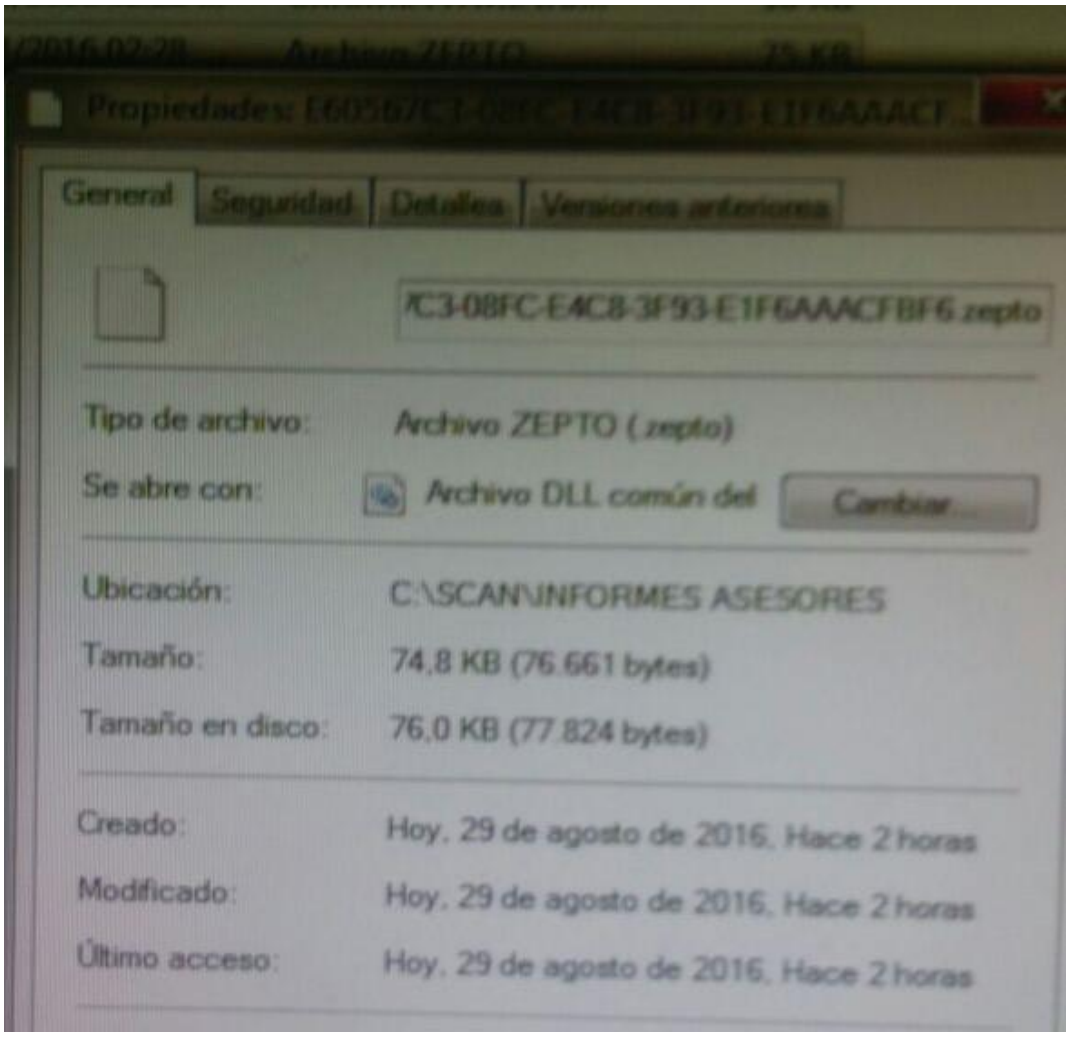
Anexo A. Documento presentado a Gerencia de ISA SA

"DIA 1, 29 AGOSTO DE 2016.

Carlos abre correo electrónico de remitente desconocido, específicamente - document@isasa.com – el correo dice que es de un email/fax de carácter confidencial para la persona u organización que lo recibe, tiene un archivo comprimido en zip. "**158F.zip**", lo descarga y lo descomprime.

Los archivos compartidos en su equipo, cambian a extensión .ZEPTO.

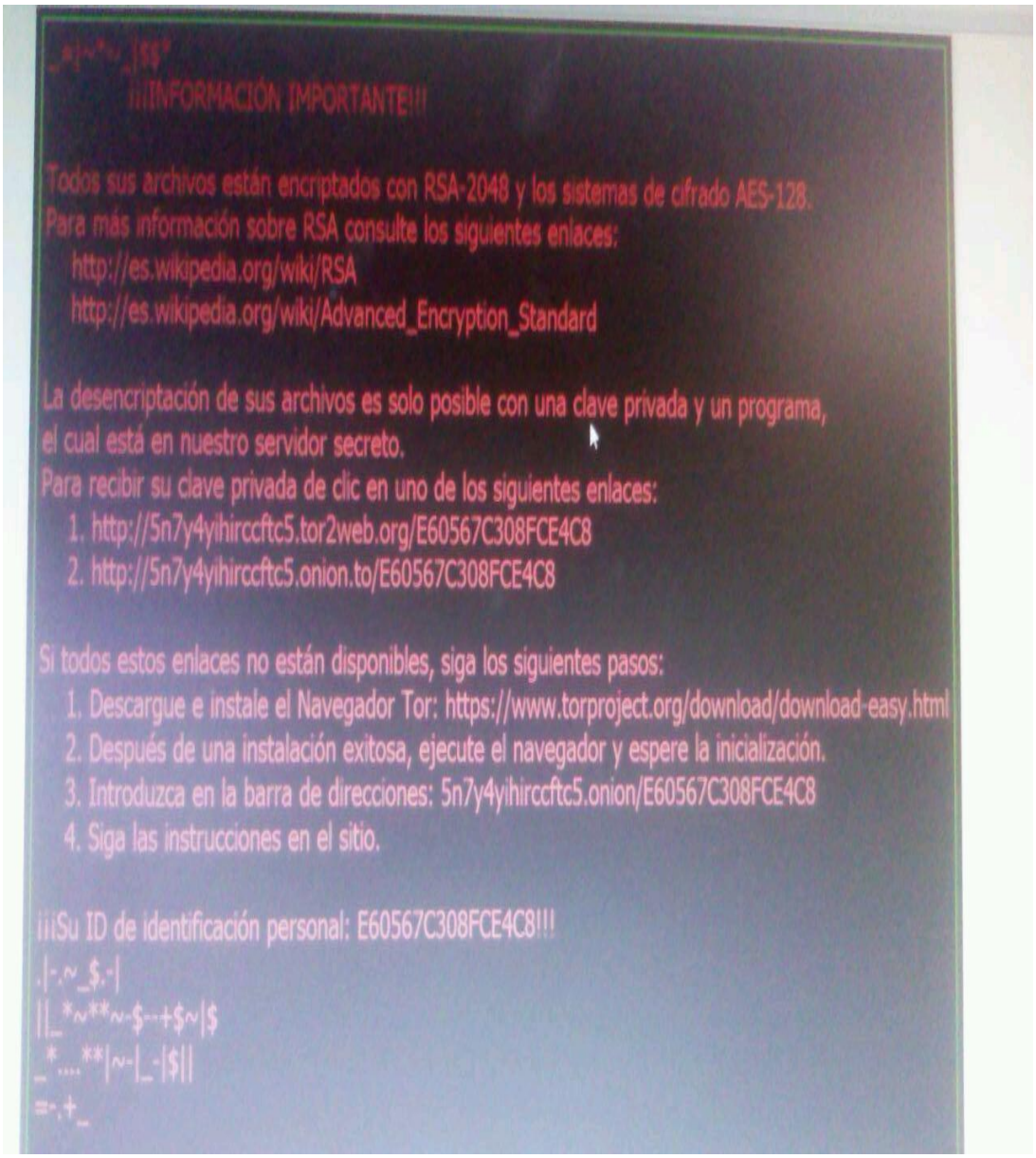
Ilustración 3. Propiedades del archivo infectado



Fuente: Sistemas ISA SA

Luego de unos minutos se muestra el siguiente mensaje en pantalla.

Ilustración 4. Mensaje en pantalla del Ransomware

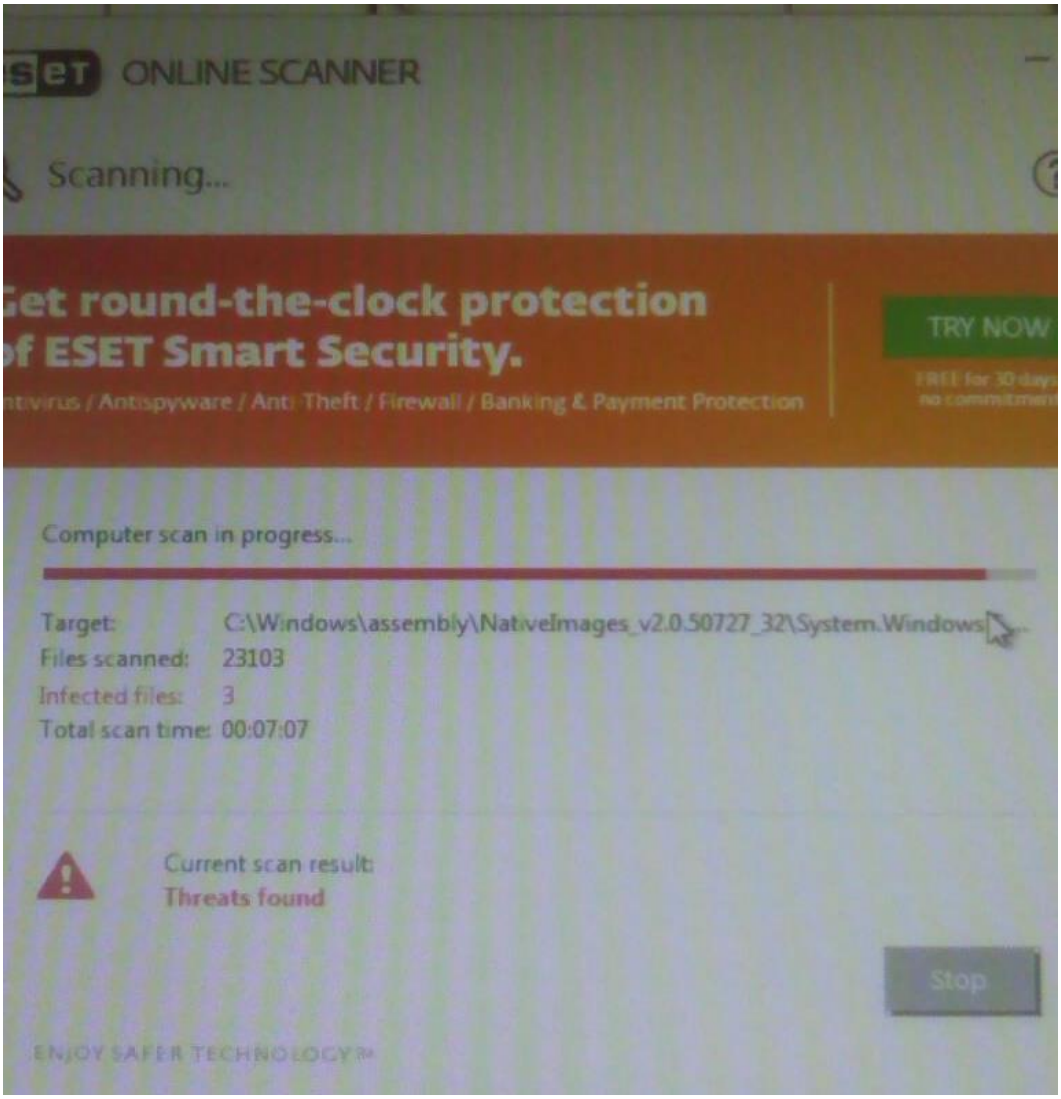


Fuente: Sistemas ISA SA

Por seguridad lo primero que hago es desactivar el uso de carpetas compartidas, y activar el uso compartido con protección por contraseña.

Luego de esto ejecuto un análisis de virus con un antivirus en línea, “eset” el cual luego del análisis encuentra 3 virus.

Ilustración 5. Resultados del análisis con Eset



Fuente: Sistemas ISA SA

Finalizado el análisis se eliminan los virus, le digo a Carlos que desconecte el equipo de la red y restauro el sistema a la fecha 26 de agosto.

Luego de finalizar el proceso, revisamos nuevamente los archivos, pero con la restauración no se logran recuperar los archivos, ya que estos continúan encriptados en .ZEPTO.

DIA 2, 30 AGOSTO DE 2016

Todos los usuarios informan que sus archivos compartidos tienen la extensión .ZEPTO, se les informa que deben hacer copias en memorias flash o discos duros externos con el fin de salvar los archivos que aún no han sido comprimidos por el virus, pero en esta sede no cuentan con estos medios, entonces les digo que creen cuentas en GMAIL y guarden todos sus archivos no infectados en ONEDRIVE.

Uno de los usuarios “LINA” tiene infectados archivos de su carpeta “DOCUMENTOS” la cual no está compartida, es evidente que el virus comprime también archivos que no están compartidos.
El equipo de Carlos no enciende, cambio el disco duro de equipo y encuentro que los archivos de registro están dañados entonces el sistema operativo no inicia.
Los usuarios confirman que han almacenado toda su información en correos electrónicos, entonces doy comienzo al formateo de los equipos.
Los equipos quedan con Windows 7 a 32 bits, particiones de disco para que almacenen todos sus archivos en una unidad diferente a la de archivos del sistema, no se crean carpetas compartidas y finalmente se instala Avast free antivirus. Los equipos se dejan instalando actualizaciones para poder instalar los paquetes de office.
Le indico a todos los usuarios “ALAMOS”, que deben tener muy en cuenta el remitente y los archivos que reciben adjuntos en estos correos, ya que si desconocen el remitente o a pesar de conocerlo el archivo adjunto no tiene indicio de ser algo que realmente solicitaron, entonces no deben descargar estos archivos.
Finalmente le indico a Alexander y a Fernando que se necesita un disco duro extraíble para realizar backups de la información en esta sede, para tener respaldo de la información, Alexander dice tener un disco duro externo y me confirma lo llevara el día siguiente.
DIA 3, 31 AGOSTO
Continúo con la configuración y descarga de programas necesarios para el trabajo normal de los compañeros de ALAMOS, los usuarios descargan los archivos subidos a ONEDRIVE, pero LINA pierde los archivos subidos en la nube de Hotmail, ya que, aunque en el momento de la carga de archivos no se presentaron mensajes de archivos pendientes o archivos infectados, estos no se encuentran en la nube.
Por el contrario, la nube de GMAIL funcionó adecuadamente y ninguno de los usuarios que uso esta aplicación perdió archivos…
Pregunto a Alexander por el disco externo, pero no lo llevo…
Informo nuevamente a Fernando que se necesita un disco duro externo para la sede de Álamos, pero no autoriza la compra.

DIA 4, 1 SEPTIEMBRE DE 2016:
A través de conexión remota se realizan configuraciones pequeñas en los equipos de la sede de álamos, vía telefónica pregunto si Alexander ha llevado el disco extraíble pero los compañeros informan que aún no lo han llevado...

INFORMACIÓN PERDIDA

Dentro de los documentos perdidos se tienen:
Lina:

- Importaciones.
- Formatos.

Dayan:

- Cartera

- Formatos.

Carlos:

- Listas de precios.
- Informes de venta de los asesores.

Para TENER EN CUENTA

El activo más importante luego de los empleados es la información, es una negligencia no contar con algo tan básico como un disco externo para realizar backups en la sede de Álamos.

Aun con antivirus no estamos a salvo de virus como el RANSOMWARE, ya que muchos son desapercibidos por los antivirus, (Un ransomware (del inglés ransom, 'rescate', y ware, por software) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción.)

Lo sucedido en álamos es algo que le puede pasar a cualquier y no contar con respaldos de información es un descuido bastante costoso."

Anexo B. Documento Orden de servicio para empresa Alianza

INGENIERO CONSULTOR	JULIAN CAMILO LEGUIZAMON

CLIENTE	FECHA DE SERVICIO
ALIANZA	**8/12/2018**
RESPONSABLE	TIPO DE SERVICIO
ALIANZA	**SERVICIO TÉCNICO ESPECIALIZADO**
CUIDAD	ORDEN DE SERVICIO
BOGOTA	**STE**

DESCRIPCIÓN DE ACTIVIDADES REALIZADAS
Se recibe el servidor de la entidad ya que tienen un problema con un virus ransomware, por recomendación la entidad dispuso la respectiva denuncia por los hechos sucedidos. De esta forma se procede con la creación de una imagen de la maquina por medio del programa FTK, esta imagen será de insumo para las pruebas que desea realizar el personal de intento de descifrado. Se procede entonces con la restauración del servicio ya que la entidad funciona 7x24 para lo cual se utiliza otro servidor de respaldo que la entidad tiene a su disposición.

Ilustración 6 Foto del Ransomware

Fuente: Alianza

1. **Alistamiento del equipo**

Se realizó ensamble e Instalación física de componentes del hardware; se validó y se actualizan los archivos micro códigos, firmware del nuevo Hardware versión (**BIOS VB3TS440 Versión V4.40.0**);

2. **Características técnicas**

Tabla 3 Características del servidor

CARACTERISTICAS	DESCRIPCION
Marca	Lenovo
Modelo	ThinkServer RD450
Formato	Altura en rack 2U
Procesadores	Intel ® Xeon ® CPU E5-2609 v4 @ 1.70 Ghz
Conjunto de chips	Intel C610 Series
Memoria	Memoria RAM 32 GB DDR4 2400M (2Rx4) RDIMM
Driver RAID	Dynamic Smart Array 720i Controller
Unidades de Disco Duro	(2) Disco Duro 2 TB 7.2K 12Gbps SAS 3.5"
Sistema Operativo	Microsoft Windows Server 2016 Standard
Serial	MJ04X4JY

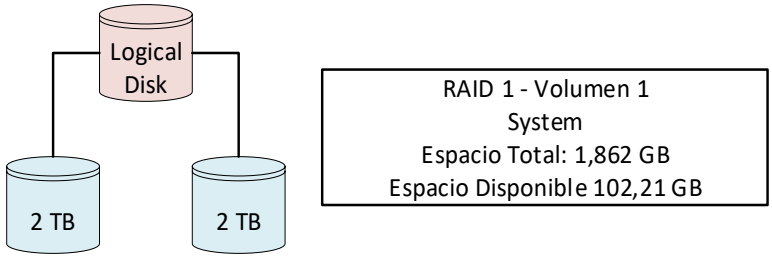
Hostname	srvwinhvirt01
Dirección IP	0.0.0.0

Fuente: Kennertech SAS

3. Arreglo de discos duros

Se define y se crea arreglo RAID discos locales, se configuran en RAID 1 en la controladora:

Ilustración 7 Nivel Raid



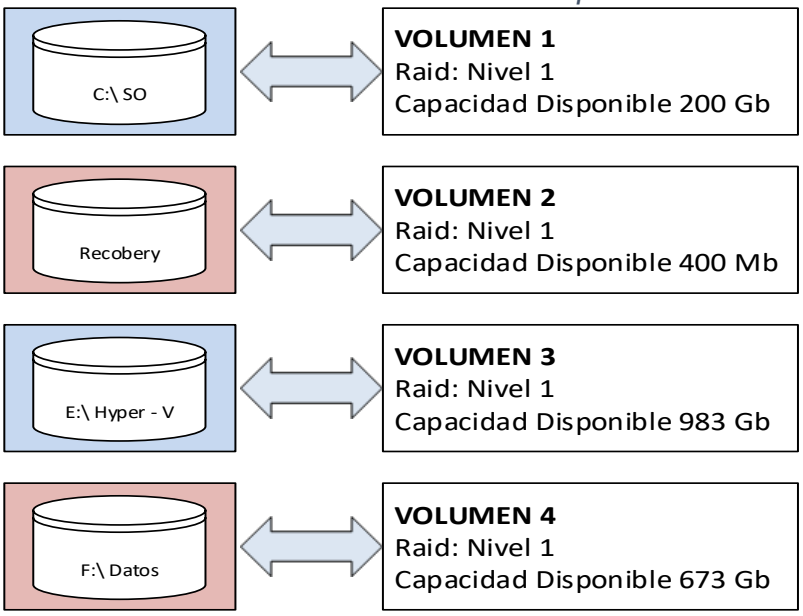
4. Instalación de sistema operativo

Se realizó la instalación y configuración del sistema operativo Microsoft Windows Server 2016 Standard con Product Key **XXXXX-XXXXX-XXXXX-XXXXX**. El cual tomara las funciones de **XXXXXX**

5. Configuración de particiones y espacio

Se activaron las particiones en formato **NTFS** con el fin de asignar un espacio dinámico a cada partición.

Ilustración 8 distribución de espacio



Fuente: Kennertech SAS

Tabla 4 Particiones

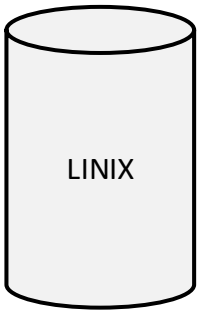
PARTICION	VOLUMEN LOGICO	TAMAÑO
NTFA system	C:\ Sistema Operativo	200 GB
	RECOBERY	400 MB
	E:\	983 GB
	F:\	673 GB

Fuente: Kennertech SAS

6. Instalación y Configuración base de datos - instancia LINIX

Se realizó instalación de Oracle **11g** Reléase **11.2.0.4.0** y una instancia **LINIX PRODUCCIÓN** con los siguientes parámetros:

Ilustración 9 Parámetros Instancia BD



SID: LINIX
Memoria asignada: 3276.8 MB (40%)
SGA: AUTO
PGA: AUTO
Tipo: General o Procesamiento Transacciones
Set de caracteres: WE8ISO8859P15
Juego de Caracteres Nacional: UTF8
Idioma: Inglés Americano
Formato fecha: Estados Unidos

Fuente: Kennertech SAS

Tabla 5 Datafiles rutas

INSTANCIA	TIPO DATAFILES	UBICACIÓN DATAFILES
LINIX	DATOS	u1/oracle/oradata/linix/DATOS/
	INDICES	u2/oracle/oradata/linix/INDICES/

Fuente: Kennertech SAS

7. Instalación de copia de seguridad automática en el servidor de base de datos

Para realizar la configuración de la copia de seguridad para la base datos en producción; se programan las siguientes tareas con ejecución diaria:

Tabla 6 Hora de Backup

TAREA	PROGRAMACIÓN	ARCHIVO PARA EJECUTAR
Copia BD Linix	23:00 Diaria	exportAutov6_GZIP.bat

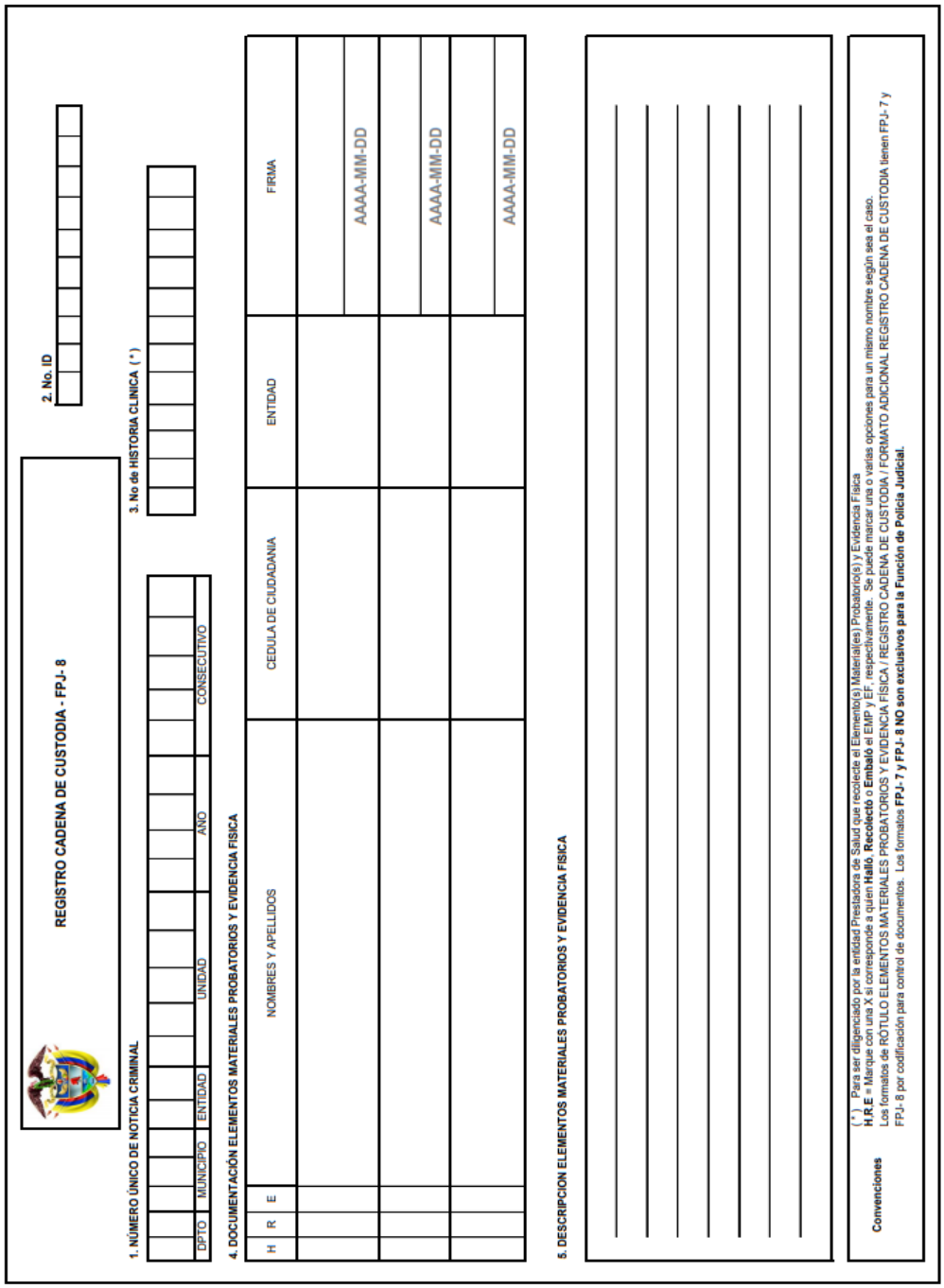
Fuente: Kennertech SAS

GARANTÍA:
Treinta (30) días contados a partir de la entrega de este servicio, las claves aquí consignadas, quedan en la total responsabilidad y administración de **ALIANZA** Cualquier alteración o cambio en las configuraciones o en los servicios contratados, y que afecten el correcto funcionamiento de la IT intervenida será causal de la perdida de la presente garantía.

Fecha y hora de Inicio		Fecha y hora de Finalización		Tiempo Utilizado
8/12/2018	11:00 AM	9/12/2018	03:00 AM	16 horas
			Tiempo total utilizado	**16 horas**

KENNERTECH S.A.S	ALIANZA
Firma Ingeniero Consultor	Firma Responsable Cliente

Anexo C Formato para recolección para el proceso de Custodia.



REGISTRO CADENA DE CUSTODIA - FPJ- 8

2. No. ID

1. NÚMERO ÚNICO DE NOTICIA CRIMINAL

DPTO | MUNICIPIO | ENTIDAD | UNIDAD | AÑO | CONSECUTIVO

3. No de HISTORIA CLINICA (*)

4. DOCUMENTACIÓN ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FISICA

H	R	E	NOMBRES Y APELLIDOS	CEDULA DE CIUDADANIA	ENTIDAD	FIRMA
						AAAA-MM-DD
						AAAA-MM-DD
						AAAA-MM-DD

5. DESCRIPCION ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FISICA

Convenciones

(*) Para ser diligenciado por la entidad Prestadora de Salud que recolecte el Elemento(s) Material(es) Probatorio(s) y Evidencia Física
H,R,E = Marque con una X si corresponde a quien **Halló**, **Recolectó** o **Embaló** el EMP y EF, respectivamente. Se puede marcar una o varias opciones para un mismo nombre según sea el caso.
Los formatos de ROTULO ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA / REGISTRO CADENA DE CUSTODIA / FORMATO ADICIONAL REGISTRO CADENA DE CUSTODIA tienen FPJ- 7 y FPJ- 8 por codificación para control de documentos. Los formatos **FPJ- 7 y FPJ- 8 NO son exclusivos para la Función de Policía Judicial.**

6. REGISTRO DE CONTINUIDAD ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FISICA

FECHA								HORA	NOMBRES Y APELLIDOS DE QUIEN RECIBE EL EMP y EF	CEDULA DE CIUDADANIA	ENTIDAD	CALIDAD EN LA QUE ACTUA		PROPOSITO DEL TRASLADO (Almacenamiento, Análisis, Presentación audiencia, Consulta, Disposición final)	ESTADO EN QUE SE RECIBE EL EMBALAJE O CONTENEDOR DEL EMP Y EF	FIRMA
A	A	A	A	M	M	D	D					C (custodio)	P (perito)			

7. PARA SER DILIGENCIADO POR EL TECNICO EN PRUEBA DE IDENTIFICACION PRELIMINAR HOMOLOGADA "PIPH"

¿ PRACTICÓ PRUEBA PRELIMINAR ?				
Si		No		
CANTIDAD DE MUESTRAS TOMADAS				
Número del Rótulo(s).				

8. OBSERVACIONES(*)

Nota:
1) Nunca interrumpa el Registro de Cadena de Custodia
2) El Registro de Cadena de Custodia siempre debe acompañar a los Elementos Materiales Probatorios y Evidencia Física
3) Si esta hoja no alcanza para diligenciar el REGISTRO DE CONTINUIDAD ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FISICA, utilizar **FORMATO ADICIONAL REGISTRO CADENA DE CUSTODIA - FPJ- 8**
4) (*) Cuando se registren observaciones se debe escribir el nombre de quien la realiza y la fecha.

Versión: 04
Aprobación: 2018-04-18 CNPJ
Publicación: 2018-12-27