ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE METODOLOGÍA DE ANÁLISIS FORENSE PARA LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE LA ARMADA DEL ECUADOR (DIRTIC)"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA

Presentada por:

ALEX PAUL TAPIA CHICHANDE

GUAYAQUIL - ECUADOR

Año: 2017

AGRADECIMIENTO

A Dios:

Por permitirme cumplir este sueño y ser parte fundamental en mi tranquilidad espiritual.

A la Master Laura Ureta, Directora de Tesis:

Por sus consejos y asesoramiento para feliz término de este trabajo

A la Armada del Ecuador:

Por el apoyo en la consecución de este grado.

A las personas que han colaborado en este trabajo:

Aunque no pueda enumerar a todas las personas que han colaborado con este trabajo como son: maestros, compañeros del programa, compañeros de trabajo, etc.

DEDICATORIA

A una persona especial en mi vida, la cual llevaré en mí corazón, quien con su aliento, palabras y apoyo supo darme fuerzas para terminar este trabajo.

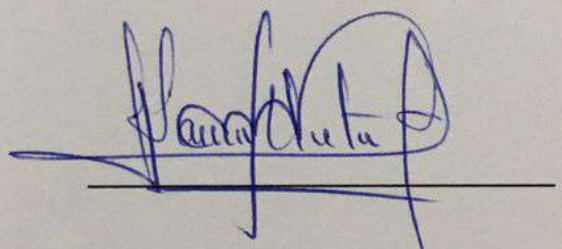
A mis hijos Doménica y Alex mis tesoros preciados por su comprensión en los momentos de ausencia.

A mis familiares y amigos quienes depositaron su confianza desde el inicio y hasta el fin del programa.

TRIBUNAL DE GRADUACIÓN

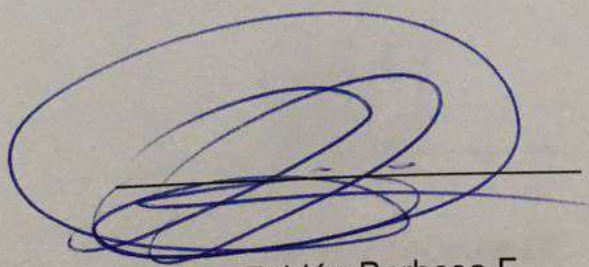
Ing. Lenin Freire

DIRECTOR MSIG/MSIA



Lic. Laura Ureta

DIRECTOR DE TESIS



Ing. Fabián Barbosa F.

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

ALEX TAPIA CHICHANDE

RESUMEN

En este trabajo, se presenta la problemática existente por la falta de una metodología de análisis forense para la Dirección de Tecnologías de Información y Comunicaciones de la Armada del Ecuador, DIRTIC, por lo que se propone la aplicación de una metodología forense para el análisis de sistemas de redes y equipos de cómputo, además se realizan algunas tareas sobre equipos de interés, logrando detallar de forma particular, el análisis sobre una computadora de escritorio. Esta metodología pretende ser una herramienta que permita a la DIRTIC, dar solución a incidentes y resolver contiendas o incidentes en los sistemas a su cargo.

La metodología a seguir está compuesta por cuatro Fases: I.- Identificación del problema, II.- Recolección, III.- Análisis de datos y IV.- Presentación de resultados obtenidos. Estas fases representan lo mínimo indispensable a la hora de investigar un incidente, logrando tener un trabajo sistémico y estructurado que permita obtener los resultados esperados.

Con el presente trabajo se pretende establecer un marco referencial base para el departamento de seguridad del DIRTIC, que requiera el establecimiento de

una investigación forense en los equipos de la Armada del Ecuador, ARE y sobre todo sea un aporte para el mejoramiento de las investigaciones de los incidentes que ocurren en los equipos y redes que forman parte del Sistema de Comunicaciones Navales, SCN.

La metodología propuesta se aplicará en un caso hipotético presentado en las instalaciones de la Dirección de Tecnologías de Información y Comunicaciones.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

COIP	Código Integral Penal.
DFRWS	Grupo de Trabajo de Investigación Forense Digital.
DIRTIC	Dirección de Tecnologías de Información y comunicaciones.
DIGMAT	Dirección General del Material.
DOJ	Departamento de Justicia de los Estados Unidos.
FDA	Análisis Forense de Datos
ISP	Proveedor del servicio de Internet.
NIST	Instituto Nacional de Estándares y Tecnologías de los Estados Unidos.
TIC	Tecnologías de Información y Comunicaciones

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Este trabajo surge por la importancia de la Tecnología Informática en todos los estratos sociales y productivos de la sociedad, a causa de la globalización, el incremento de los canales de comunicación y la facilidad y comodidad de procesar y gestionar la información, la cual en muchos casos son el tesoro preciado de personas mal intencionadas, que aprovechando las vulnerabilidades que presentan las tecnologías tanto en hardware como en software, son capaces de realizar acciones ilegales.

El diagnóstico situacional ha establecido que, en la DIRTIC, existen vulnerabilidades tecnológicas en la gestión de la información, que son producto del trabajo diario y de ciertas limitaciones en las áreas de infraestructura y redes, desarrollo de software, lo cual se traduce en problemas de seguridad como: perdida de los servicios, mal uso de la información confidencial, accesos no autorizados, mal uso de los recursos, etc.

La implementación de una metodología que se presenta en este proyecto forma parte de un inicio en el tratamiento a los problemas citados anteriormente, y el cual sugiere una serie de pasos para originar un espacio de análisis y estudio

hacia el esclarecimiento de los hechos y así presentar las evidencias que identifiquen en el lugar donde se llevaron a cabo las acciones no autorizadas o ilegales.

Se debe destacar que, con el surgimiento del campo de la informática forense, ha ido tomando más fuerza el campo del derecho y la aplicación de la justicia en el área informática, debido al aparecimiento de desafíos y técnicas de intrusión informática, que van desde una simple intromisión hasta verdaderos accesos maliciosos a bases de datos de misión crítica, por lo que es demandante que se realice el seguimiento postmorten de estos delitos.

CAPÍTULO 1

GENERALIDADES

1.1. ANTECEDENTES

El estado ecuatoriano desde el año 2008, promulgó como política pública, el uso obligatorio del software libre, mediante el Decreto Ejecutivo No. 1014, del 10 de abril del 2008, negando la adquisición de software que no se ajuste al decreto 1014. El cambio ha sido progresivo pero constante, a esta fecha (2016) todas las entidades públicas tienen la obligación de analizar y utilizar alternativas de software libre.

En el año 2014, entro en vigencia el Código integral Penal, COIP, en su Disposición Derogatoria Novena derogó el Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensaje de

Datos, referidos anteriormente e incorporó otras figuras delictivas relacionadas con los sistemas informáticos y amplió el alcance de las infracciones informáticas contempladas en el anterior Código Penal. Entre otros tenemos: revelación ilegal de base de datos, interceptación ilegal de datos, ataque a la integridad de sistemas informáticos, acceso no consentido a un sistema informático, etc.

1.2. DESCRIPCIÓN DEL PROBLEMA

Las Fuerzas Armadas se encuentran en un proceso de reestructuración en todos sus niveles, este proceso ha hecho que los organismos encargados de las TIC´s, también planteen su nueva forma de trabajar. Como parte de esta reestructuración es necesario el mejoramiento del área de Seguridad Informática, sin embargo, una de las áreas en las cuáles se debe trabajar es el Análisis Forense donde se tiene poco o nada en cuanto a una metodología a seguir cuando se presente un incidente, lo que limita contar con una respuesta eficaz al momento de determinar las causas o motivos que originaron los problemas.

Han existido varios incidentes en el Centro de Computo del Centro de Tecnologías Guayaquil, los cuales por falta de un procedimiento/estándar y herramientas a utilizar no se ha podido generar un informe que determine las causas y sobre todo se tome

acciones que impidan nuevamente se vuelvan a ocurrir estos acontecimientos.

Entre los incidentes más comunes que han afectado la continuidad de los servicios tenemos:

- Denegación de los servicios, por saturación en la red.
- Perdida de conectividad con los servicios.
- Saturación del Firewall
- Incidentes de código malicioso
- Mal uso de información confidencial
- Acceso no autorizado.
- Uso inapropiado de los recursos[1].

Los problemas detallados anteriormente han hecho que los servicios permanezcan inestables por periodos de tiempo mayores a lo normal, lo que ha influido en una mala percepción del servicio brindado por la DIRTIC a los usuarios, además de no contar con una base del conocimiento de problemas anteriormente suscitados que permitan asociar los problemas nuevos y solventarlos de una forma más eficiente.

[1] Uso de equipos y/o servicios (internet), para fines diferentes a sus actividades laborales.

1.3. SOLUCIÓN PROPUESTA

A fin de poder dar una solución a los diferentes problemas descritos y ayudar al departamento de Seguridad Informática, en el ámbito del Análisis Forense se propone implementar una metodología que permita a este departamento actuar con un orden y uso de herramientas para que los resultados sean mucho más eficaces y confiables.

Para este trabajo se propone identificar los diversos problemas que se encuentran en la Dirección de Tecnologías por medio de un análisis estadístico; luego de ello se realizará una revisión de las metodologías aplicadas en el ámbito del Análisis Forense como son: Departamento de Justicia (DOJ), Instituto Nacional de estándares y tecnología de los Estados Unidos (NIST) y el Grupo de Trabajo de Investigación Forense Digital (DFRWS) y en base al comportamiento organización de la Institución, implementar la metodología que se adapte a las necesidades de la organización. Posteriormente se realizará una revisión de diferentes herramientas informáticas de uso libre que permita obtener resultados esperados y confiables. Se pondrá en práctica la metodología escogida en casos reales y finalmente se evaluarán los resultados haciendo una comparación con respecto a los procedimientos actuales.

Esta propuesta permitirá a los funcionarios de la DIRTIC identificar las causas, documentar todo lo observado y mantener una base del conocimiento para futuros incidentes, lo que lograría en un futuro disminuir los tiempos de paralización de los servicios informáticos.

Este trabajo a realizarse es de gran importancia, dado que en la actualidad en DIRTIC, no se realiza de forma metódica el análisis de los incidentes, siendo en el mejor de los casos encontrar la solución del problema, sin llegar a la determinación de las fuentes o conclusiones de lo que ocurrió, lo que limita el control de incidentes en caso de volver a ocurrir.

1.4. OBJETIVO DEL TRABAJO

1.4.1. OBJETIVO GENERAL

Implementar una metodología de análisis forense para la Dirección de Tecnologías de Información y Comunicaciones de la Armada del Ecuador con énfasis en el análisis de redes y equipos de cómputo personal, a fin de contribuir con la Seguridad informática de la Organización.

1.4.2. OBJETIVOS ESPECÍFICOS

- Recopilar, revisar y analizar información, conceptos fundamentales y herramientas de informática forense.

- Diagnosticar la situación actual del departamento de seguridad de la Dirección de Tecnologías de Información y Comunicaciones, mediante un análisis estadístico en un período determinado
- Definir la metodología a utilizarse mediante la comparación de los diferentes estándares de trabajo
- Presentar las pruebas desarrolladas a la metodología implementada.
- Analizar los resultados obtenidos de las pruebas realizadas.

1.5. ALCANCES Y LIMITACIONES

1.5.1. ALCANCE

El trabajo en desarrollo tiene como alcance Implementar una metodología de Análisis Forense en la Dirección de Tecnologías de Información y Comunicaciones, DIRTIC, ubicada en la ciudad de Guayaquil, en la Base Naval Sur, edificio de la Dirección General del Material, DIGMAT.

Los aspectos puntuales que comprende este trabajo están referidos a los problemas existentes en los equipos de cómputo personales y equipos de redes existentes en la DIRTIC, dentro de los cuales podemos encontrar equipos de escritorios,

portátiles, switches, routers, etc. Se analizará tres metodologías de reconocido uso como son: Departamento de Justicia (DOJ), Instituto Nacional de estándares y tecnología de los Estados Unidos (NIST) y Grupo de Trabajo de Investigación Forense Digital (DFRWS) de los cuales se buscará los mejores procedimientos para la implementación en la DIRTIC.

Se realizará un análisis de las mejores herramientas OPEN SOURCE, para uso y aplicación en la metodología y finalmente se aplicará la metodología en un caso hipotético.

No se incluirá el análisis de costo de la implementación, ni tampoco el costo beneficio de la misma.

1.5.2. LIMITACIONES

Dada la confidencialidad de la información que se maneja en las Instituciones militares, se debe establecer que la información reflejada en este trabajo es referencial y de carácter académico.

Debido a la estructura jerárquica que tiene la Institución militar la metodología tiene un alcance de trabajo en la Dirección de Tecnologías de Información y Comunicaciones.

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD INFORMÁTICA

Entender el concepto de seguridad tiene matices abstractos, en muchos de los casos depende del punto de vista desde el cual se observe el nivel de seguridad, se debe comprender que es imposible alcanzar un nivel total de seguridad, pero si se puede mantener un nivel de seguridad óptimo.

Para el caso de la seguridad informática es muy aplicable este preámbulo, ya que no podemos encontrar sistemas informáticos cien por ciento seguros, sino tendremos sistemas con niveles aceptables de seguridad.

Las personas tienden a confundir la seguridad de la información con la seguridad informática por lo que es menester dejar sentado la definición de la seguridad informática:

El Instituto Nacional de estándares y tecnología de los Estados Unidos, NIST, define la seguridad informática como las medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y la información que procesan, almacenan e intercambian. [1]

La seguridad informática es una rama de la seguridad de la información y se utiliza a menudo de forma intercambiable. Incluye una serie de medidas de seguridad, como programas de software, suites de antivirus, cortafuegos y medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX que permitan proteger el uso de la computadora y los recursos de la red o de Internet.

Por otro lado, debemos comprender que la seguridad de la información tiene un sentido más amplio, el NIST establece a la seguridad de la información como establecer los procesos que permitan la protección de la información y sus sistemas, del acceso no autorizado, uso, divulgación, alteración, modificación o destrucción con el fin de proporcionar:

1) Integridad, que significa proteger la información de la inadecuada modificación o destrucción e incluye información que asegure el no repudio y la autenticidad;

2) Confidencialidad, que significa la preservación de las restricciones en el acceso y divulgación, incluyendo los medios para la protección personal, la privacidad y la propiedad de la información; y

3) Disponibilidad, que significa garantizar el acceso oportuno y confiable para el uso de la información [1].

2.2 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA

De acuerdo a Alvin Toffler en su libro de las “La tercera Ola”, donde describe las tres grandes épocas de la humanidad: revolución agrícola, revolución industrial y la revolución de era de la Información [2], es justamente en la última, en la cual se evidencia grandes cambios, pues se ha generado un incremento en el uso de equipos móviles, ocasionando un problema en el control de los mismos y es allí donde la seguridad informática toma su gran importancia, la misma ha ido incrementándose a menudo que las organizaciones han visto la necesidad del incremento del uso de la tecnología, así como han reconocido la importancia de proteger su información.

Para poder entender acerca de la seguridad informática es menester establecer ciertos conceptos que nos permitirán conocer que es lo que se desea proteger:

- Dato: “Un subconjunto de la información en formato electrónico que permite que sea recuperados o transmitidos” [1].

- Información: “Cualquier comunicación o representación del conocimiento, tales como hechos, datos u opiniones en cualquier medio o forma, incluyendo texto, números, gráficos, cartografía, narrativa, o audiovisual” [1].

- Seguridad: “Una condición que resulta de la creación y el mantenimiento de medidas de protección, que permiten a una empresa llevar a cabo su misión o funciones críticas a pesar de los riesgos planteados por las amenazas a la disponibilidad de los sistemas de información. Las medidas de protección pueden implicar una combinación de disuasión, prevención, anulación, detección, recuperación y la corrección que debe formar parte de la administración del riesgo de la empresa” [1].

Con los conceptos citados se puede observar que la seguridad informática es un concepto bastante amplio y también se debe mencionar que no existe un sistema ciento por ciento seguro, sino que

se debe establecer niveles de seguridad que permitan minimizar el impacto de los riesgos. Se debe considerar también que mientras más seguro es un sistema, la inversión económica o el nivel de seguridad debe ser más alto. A todo esto, se suma que no solo basta la tecnología para lograr niveles de seguridad importantes sino también deben existir una correcta organización y predisposición de las personas para mejorar la seguridad.

Del incremento en el uso de la tecnología, de comprender mejor los conceptos de la información que se guardan en un sistema informático y de la forma en que las organizaciones se han estructurado, radica la importancia de mantener niveles óptimos de seguridad y evitar el robo o pérdida de la información.

2.3 ANÁLISIS FORENSE

Existen diversas motivaciones por parte de los atacantes para intentar el ingreso a un sistema informático, estos van desde situaciones personales: ego, fama, rating, etc.; situaciones económicas, políticas, de gobierno, etc., pero el resultado de estos ataques es justamente encontrar una vulnerabilidad al sistema, obtener la información presente en el mismo y causar un daño.

Los ataques informáticos cualquiera que haya sido su motivación, requiere de un tratamiento y solventar ciertas incógnitas: ¿quién realizó

el ataque?, ¿cómo se lo realizó?, ¿qué vulnerabilidad se explotó?, ¿qué hizo el atacante dentro del sistema?, etc., estas incógnitas pueden ser resueltas mediante un análisis forense.

Según el diccionario de Oxford, la palabra forense se define como "relacionado con o que denota la aplicación de métodos científicos y técnicas para la investigación del delito; y lo relacionado con los tribunales de justicia" [3]. Estas definiciones aparentan ser bastante amplias, pero lo importante en la primera definición es que se resalta el uso de métodos científicos usados en la investigación y la segunda definición hace hincapié en el hecho de que la actividad forense se refiere a los tribunales de justicia. A pesar que no todos los casos investigados acaban en los tribunales, como, por ejemplo: las investigaciones internas y audiencias disciplinarias. En conclusión, se puede establecer que cuando se pone en marcha una investigación forense, esta debe llevarse de una manera científica y con una base jurídica como soporte.

La Informática forense se puede definir como "técnicas analíticas y de investigación, empleados para la conservación, identificación, extracción, documentación, análisis e interpretación de los medios de comunicación del ordenador (datos digitales) que se almacena o codificada para el análisis de pruebas y/o causa raíz" [4].

Otro concepto que debemos definir como un insumo central del análisis forense es la **evidencia digital** que la podemos definir como “la información electrónica guardada o transferida en forma digital” [1].

La evidencia digital tiene las siguientes características: **volátil, anónima, duplicable, alterable y modificable, y eliminable.**

La evidencia digital se puede clasificar en dos categorías: **volátil y no volátil**. La evidencia volátil comprende cuando la información desaparece cuando el equipo es desconectado de la fuente de alimentación eléctrica: contenido de la memoria RAM, procesos en ejecución, usuarios conectados, información de la red, etc. La evidencia no volátil se refiere a la información contenida en el disco duro la cual puede ser grabada sin necesidad de tener encendido el equipo [5].

2.4 IMPORTANCIA DEL ANÁLISIS FORENSE

Existen normas que pueden ayudar a eludir la pesada tarea de elegir qué factores son aplicables a una investigación forense en particular y que pueden ser adaptadas por las organizaciones entre sus normas, políticas y procedimientos como ayuda en una investigación.

Así como las normas y políticas internas, hay varias medidas legislativas que intentan perseguir los delitos informáticos. En Ecuador podemos citar el Código Integral Penal, la cual sanciona los delitos

informáticos, sin embargo, este no es un instrumento procedimental en cuanto a cómo debe llevarse una investigación forense para garantizar la idoneidad legal.

En consecuencia, una forma importante para que la mayoría de las organizaciones se protejan de los delitos informáticos es instituir políticas y procedimientos internos que especifiquen exactamente lo que constituye la acción dañina en contra o dentro de una organización.

Hasta el momento se ha determinado que la aplicación de ciertas normas, como ISO 17799, puede ser un primer paso útil por una organización hacia la protección efectiva de su información y activos. Por otra parte, que las políticas y procedimientos específicos también deben ser implementadas dentro de una organización para ayudar a proteger la integridad interna de la información y de los activos.

2.5 METODOLOGÍAS PARA EL ANÁLISIS FORENSE.

Hay un viejo refrán que dice: es mejor prevenir que lamentar. Cuando se aplica un método forense sobre algún incidente, esto parecería implicar que la preparación, es la clave para la correcta obtención de un resultado de la investigación forense. A pesar de que la preparación es importante, es imposible estar preparado para todo tipo de comportamiento. Una base sólida de conocimientos y experiencia

previa siempre ayuda, pero una sugerencia o caso documentado no es una solución completa a la solución de un problema.

El número de modelos forenses que se han propuesto revela la complejidad del proceso forense. La mayoría se centra en cualquier etapa de la investigación o enfatiza en una etapa particular de la investigación.

Kruse y Heiser con el modelo Lucent se refieren a una metodología de investigación forense de computadoras de tres componentes básicos. Ellos son: la adquisición de pruebas, autentificación de las pruebas y el análisis de los datos [6]. Estos componentes se centran en el mantenimiento de la integridad de las pruebas durante la investigación.

El Departamento de Justicia de Estados Unidos propuso un modelo de proceso para medicina forense. Este modelo se abstrae de la tecnología y consta de cuatro fases: colección, examen, análisis y generación de informes [7]. Existe una correlación entre la etapa de 'la adquisición de la evidencia' identificado por Kruse y Heiser y la etapa de "colección" que aquí se propone. "El análisis de los datos" y "análisis" son los mismos en ambos marcos. Kruse sin embargo, ha olvidado de incluir un componente vital: la presentación de informes. Esto si está incluido en el marco del Departamento de Justicia.

El modelo del Instituto Nacional de Estándares y Tecnología (NIST), en su publicación especial SP 800-86, propone cuatro fases básicas para el proceso forense: recolección, examinación, análisis y presentación de informes [8].

El modelo de investigación científica de la escena del crimen propuesto por Lee consiste en cuatro pasos. Ellos son: el reconocimiento, identificación, individualización y la reconstrucción [9]. Estos pasos se refieren sólo a una parte del proceso de investigación forense. Estas etapas se encuentran claramente dentro de la etapa de "investigación" del proceso, no hay una "preparación" ni “presentación" del escenario.

Casey propone un marco similar a Lee. Este marco se centra en el procesamiento y el examen de la evidencia digital. Los pasos que se incluyen son: el reconocimiento, preservación, clasificación y la reconstrucción [8]. En ambos modelos de Casey y de Lee, el primero y último paso son idénticos.

El Grupo de Trabajo de Investigación Forense Digital (DFRWS) desarrolló un marco con los pasos siguientes: identificación, preservación, colección, examen, análisis, presentación y la decisión [7]. Este marco pone en marcha una base importante para los trabajos futuros, incluye dos etapas cruciales de la investigación: la etapa de investigación y la etapa de presentación.

Reith propone un marco que incluye una serie de componentes que no están mencionado en los marcos anteriores. Los componentes listados completos son: identificación, preparación, enfoque, estrategia, preservación, colección, examen, análisis, presentación, y la evidencia de regresar [7]. Este proceso es extenso y ofrece una serie de ventajas, como lo indican sus autores.

El modelo propuesto por Ciardhuáin es probablemente el más completo hasta la fecha. Los pasos o fases también se denominan “actividades”. El modelo incluye las siguientes actividades: sensibilización, autorización, planificación, notificación, buscar e identificar las evidencias, colección, transporte, almacenamiento, examen, hipótesis, presentación, prueba / defensa y la difusión [10]. Los pasos se discuten en profundidad por el autor del artículo.

A partir de los marcos mencionados anteriormente se puede establecer lo siguiente:

- Cada uno de los modelos propuesto se basa en la experiencia previa
- Algunos de los modelos tienen enfoques similares.
- Algunos de los modelos se centran en diferentes áreas de la investigación.

Sin embargo, la mejor forma de equilibrar el proceso forense es asegurar la consecución del objetivo primordial: producir pruebas concretas adecuadas para su presentación en un tribunal de justicia.

CAPÍTULO 3

DIAGNÓSTICO SITUACIONAL

3.1 ANÁLISIS ESTADÍSTICO DE LOS INCIDENTES

Entre los incidentes más comunes que han afectado la continuidad de los servicios en la Dirección de Tecnologías de Información y Comunicaciones tenemos:

- Denegación de los servicios, por saturación en la red, DDOs.
- Perdida de conectividad con los servicios.
- Saturación del Firewall
- Incidentes de código malicioso
- Mal uso de información confidencial

- Acceso no autorizado.
- Uso inapropiado de los recursos.

Para el presente análisis estadístico, se tomará en cuenta los incidentes ocurridos en el presente año 2016, cuya información lo maneja el departamento de seguridad informática de la DIRTIC.

Del informe estadístico presentado en el Anexo “A”, se pueden establecer las siguientes observaciones:

- La mayor cantidad de incidentes reportados son por el departamento de seguridad, es decir lo que está relacionado con acceso no autorizado, uso inapropiado de los recursos, mal uso de la información y saturación del firewall.
- En segundo lugar, de incidentes reportados tiene que ver con el departamento de redes, es decir lo relacionado con saturación de la red y pérdida de conectividad.

Como se puede observar la figura 3.1 tipo de incidentes, un alto porcentaje de los incidentes corresponden al uso inapropiado de los recursos.

Figura 3.1 Tipos de Incidentes

La Encuesta Global de seguridad de la Información del año 2015[2], estableció entre otros puntos los siguientes [11]:

- Existe un incremento del 38% de los incidentes detectados, donde cada vez resultan menos eficaces los sistemas de protección y prevención.
- El 69% utiliza servicios de ciberseguridad basado en la nube.

[2] Estudio mundial realizado por PricewaterhouseCooopers, PwC y la revista CIO Magazine y CSO Magazine, basado en la respuesta de más de 10.000 ejecutivos. Investigación realizada del 7 de mayo al 12 de Junio del 2015.

- Existe un alto involucramiento de los ejecutivos y directorio de ciberseguridad.

Al observar las estadísticas a nivel mundial comparado con lo que sucede en la DIRTIC, podemos establecer los siguientes aspectos:

- Existe un mayor involucramiento en las organizaciones en el tema de ciberseguridad, el hecho de llevar estadísticas sobre incidentes en la DIRTIC, establece la importancia que conlleva el tratamiento de los mismos.
- Existen áreas o incidentes que requieren de mayor atención en la organización.

En la encuesta Global de Análisis Forense de Datos 2016 de EY[3], se destacaron los siguientes aspectos [12]:

- La alta gerencia encuentra la necesidad de implementar herramientas de Análisis Forense de Datos, FDA para tratar los principales riesgos del negocio.
- Existe un aumento considerable de empresas que utilizan herramientas de Análisis Forense.

---

[3] Encuesta realizada por la empresa Ernst & Young, líder mundial en servicios de auditoría, entre junio y septiembre del 2015 a 665 ejecutivos de empresas de 17 países a nivel mundial.

- El 56% de las empresas que han implementado herramientas FDA, han obtenido resultados positivos.

Considerando que la DIRTIC tiene un mayor involucramiento en el tema de la gestión de los incidentes y dado los buenos resultados de las empresas que han implementado FDA, es de gran beneficio implementar una metodología que permita realizar Análisis Forense dentro de la Organización

3.2 EVALUACIÓN DE LAS CAPACIDADES EN EL ÁMBITO FORENSE

Para el análisis de las capacidades de la DIRTIC en el ámbito forense se llevó a cabo una encuesta que permitió verificar dos aspectos:

- Se formularon 06 preguntas relacionados con la Seguridad de la Información
- Se formularon 05 preguntas en referencia con el Análisis Forense.

Para esta encuesta se determinó la población muestra de 42 servidores de la Dirección de Tecnologías de Información y Comunicaciones, como se muestra en la Tabla No 1, como la población es de pequeñas dimensiones, los encuestados seleccionados fueron todos, lo que nos permite tener una muestra representativa de lo que se desea investigar.

Tabla 1: Descripción del numérico de DIRTIC

Departamento u Oficina	**Cantidad de Personas**
DIRTIC	
Dirección	2
Subdirección	2
Departamento Administrativo Financiero	4
Departamento de Desarrollo y Gestión de Proyectos Informáticos	2
Departamento de Comunicaciones	3
Departamento de Criptografía y Seguridad Telemática	3
Departamento de Control de Centros	2
CETEIG	
Centro de Tecnología de la Información y Comunicaciones	24
Total	**42**

Fuente: DIRTIC

La encuesta realizada fue elaborada en la herramienta informática LimeSurvey, las preguntas de respuestas fueron elaboradas en formato de escala tipo Likert: Totalmente en desacuerdo (TD), Desacuerdo (D) Neutral (N), De Acuerdo (A) y Totalmente de acuerdo (TA); y preguntas de SI / NO, con el fin de diagnosticar cómo se encuentra la Seguridad de la Información y el Análisis Forense en la DIRTIC y su contenido se observa en el Anexo “B”.

Para presentar los resultados se usaron los recursos de la estadística descriptiva con el diseñó de los cuadros, donde se organizaron los datos obtenidos en distribuciones por frecuencias absolutas y luego cambiados a porcentajes, se representó mediante diagramas de barras cada una de las preguntas del instrumento de recolección de datos.

En la primera sección donde se buscó conocer el grado de conocimiento de la seguridad de la información se obtuvieron los siguientes resultados:

Tabla 2: Resultados de las respuestas a las preguntas sobre la seguridad de la información

SEGURIDAD DE LA INFORMACIÓN	TD	%	D	%	N	%	A	%	TA	%
Pregunta 1	3	7.14%	1	2.38%	11	26.19%	19	45.24%	8	19.05%
Pregunta 2	3	7.14%	3	7.14%	8	19.05%	22	52.38%	6	14.29%
Pregunta 3	2	4.76%	5	11.90%	15	35.71%	14	33.33%	6	14.29%
Pregunta 4	33	78.57%							9	21.43%
Pregunta 5	2	4.76%	1	2.38%	1	2.38%	8	19.05%	30	71.43%
Pregunta 6	7	16.67%	10	23.81%	10	23.81%	8	19.05%	7	16.67%

Fuente: Autor

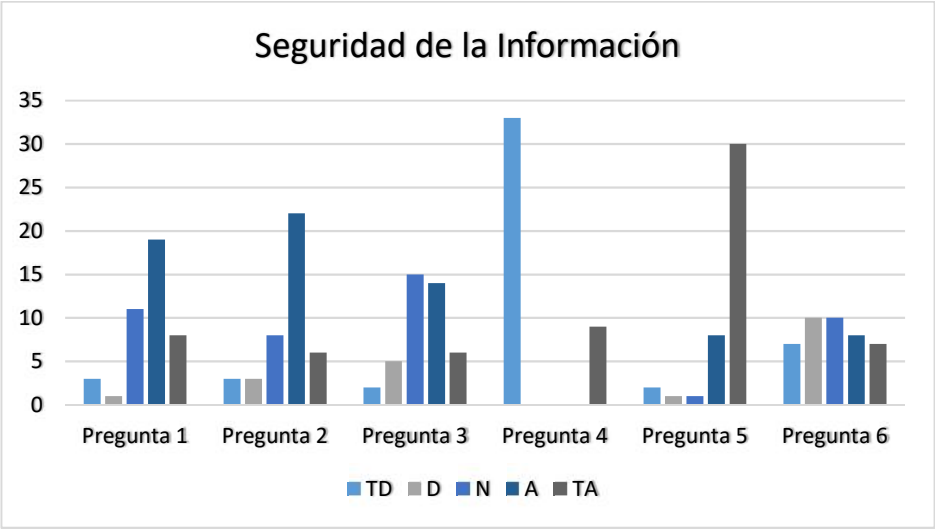


Figura 3.2 Resultados de las respuestas a las preguntas sobre la seguridad de la información

Fuente: Autor

De acuerdo a las respuestas emitidas de los sujetos en estudio y el análisis e interpretación de las mismas, se puede visualizar en el Tabla

No. 2 y figura 3.2, en la pregunta 1) ¿Se implementan controles de detección, prevención y recuperación de la información, para la protección contra código malicioso o virus?, el **45,24%** está de **acuerdo** con esta pregunta.

En la pregunta 2) ¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información?, el **52,38%** está de **acuerdo** con la pregunta.

En la pregunta 3) ¿Han existido varios incidentes de seguridad de la información en la DIRTIC en el último año?, **33,33%** de los encuestados estuvo de **acuerdo.**

En la pregunta 4) ¿Ha sido víctima de un ataque informático?, el **78,57%** contestó que **NO**

En la pregunta 5) ¿Considera que debe haber campañas de prevención de los delitos informáticos?, el **71,43%** opinó que está **totalmente de acuerdo**.

En la pregunta 6) ¿En su opinión considera suficiente la inversión en seguridad informática?, **23,81%** estableció un **desacuerdo** y en igual porcentaje una posición neutral

En conclusión, podemos observar que existe una concientización del personal de la DIRTIC en la importancia de la seguridad de la información, considerando que la inversión es neutral para llevar a cabo el proceso de seguridad y que en su mayor parte no ha sufrido un ataque informático.

En la segunda sección donde se buscó conocer el grado de conocimiento de en el análisis forense se obtuvieron los siguientes resultados:

Tabla 3: Resultados de las respuestas a las preguntas sobre el análisis forense

ANALISIS FORENSE	**NO**	**%**	**NO SABE**		**SI**	**%**
Pregunta 7	16	38.10%			26	61.90%
Pregunta 8	24	57.14%			18	42.86%
Pregunta 9	23	54.76%	17	40.48%	2	4.76%
Pregunta 10	33	78.57%			9	21.43%
Pregunta 11	13	30.95%			29	69.05%

Fuente: Autor

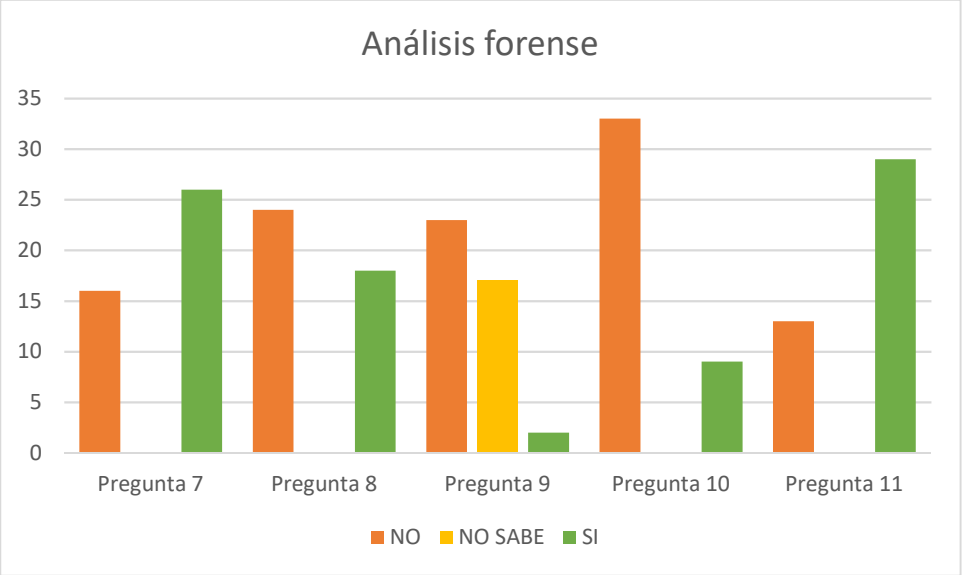


Figura 3.3: Resultados de las respuestas a las preguntas sobre el análisis forense

Fuente: Autor

En la pregunta 7) ¿Ha escuchado hablar sobre el análisis forense digital?, el **61,90%** de los encuestados contestó que **SI**, lo que evidencia que el personal de la DIRTIC en algún momento ha escuchado sobre el proceso forense.

En la pregunta 8) ¿Conoce las ventajas del análisis forense?, el **57,14%** de los encuestados contestó que **NO**, a pesar que en la pregunta anterior se evidenció haber escuchado sobre el proceso forense, las personas desconocen las ventajas de este trabajo.

En la pregunta 9) ¿Conoce si el departamento de seguridad realiza análisis forense?, el **54,76%** de los encuestados contestó que **NO**, lo

que refleja que en la DIRTIC todavía no se ha implementado una metodología o esta no ha sido difundida.

En la pregunta 10) ¿Conoce alguna metodología aplicada al análisis forense?, el **78,57%** de los encuestados contestó que **NO**, lo que demuestra que el personal que labora en DIRTIC, no tiene un pleno conocimiento del análisis forense.

En la pregunta 11) ¿Considera que la implementación de una metodología de análisis forense contribuirá a la seguridad de la información?, el **69,05%** de los encuestados contestó que **SI**, esto evidencia que, a pesar del poco conocimiento sobre análisis forense en el personal de la DIRTIC, están de acuerdo que la implementación de una metodología contribuiría a la seguridad de la información.

En conclusión, podemos observar que a pesar de que personal de la DIRTIC ha escuchado sobre el análisis forense, desconoce las ventajas y las metodologías utilizadas para llevar a cabo el proceso forense, sin embargo, está de acuerdo en que la implementación de la metodología contribuiría a la seguridad de la información.

3.3 INFORMACIÓN DE LA INFRAESTRUCTURA DEL LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La Dirección de Tecnologías de Información y Comunicaciones, se encuentra actualmente conformada por los siguientes departamentos: Dirección, Subdirección, Departamento Administrativo Financiero, Departamento de Desarrollo y Gestión de Proyectos, Departamento de Comunicaciones, Departamento de Criptografía y Seguridad Telemática, Departamento de Control de Centros y el Centro de Tecnología de la Información y Comunicaciones, como se ilustra en la figura 3.4.

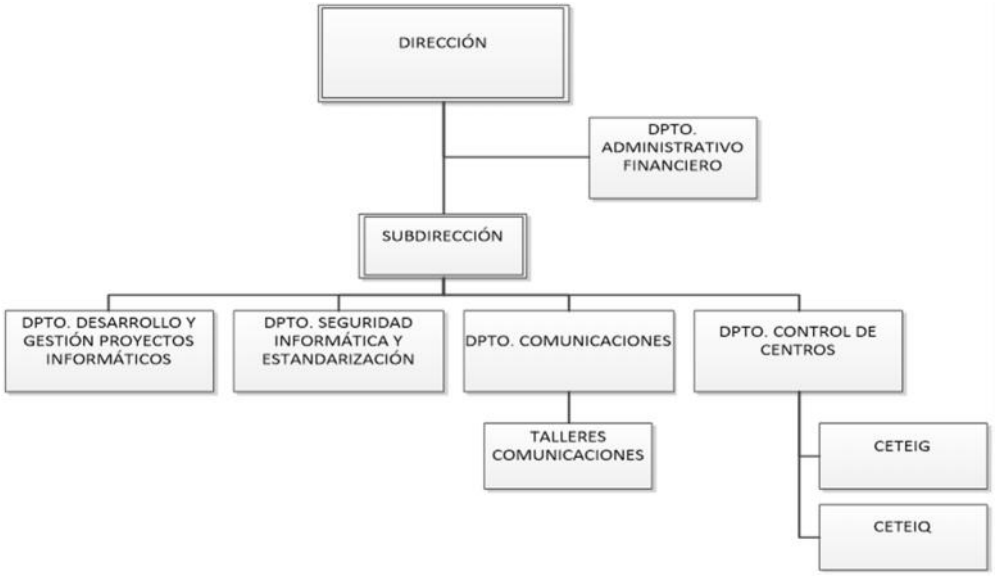


Figura 3.4: Organigrama de la DIRTIC

La DIRTIC tiene como Misión “Gestionar las tecnologías de la información y comunicaciones, mediante su desarrollo, administración, mantenimiento; a fin de contribuir al direccionamiento estratégico, al desarrollo de las capacidades marítimas, la seguridad integral de los espacios acuáticos y el apoyo al desarrollo marítimo nacional” [13].

Como se pudo observar en el organigrama existe un Departamento de Seguridad Informática y Estandarización y en el interior de este existen dos divisiones: División de seguridad y división de Estandarización. Sin embargo, en la división de seguridad informática no existe un área de análisis forense, o un encargado de realizar estas actividades.

El inventario de equipos que tiene la DIRTIC, está dividido en tres áreas: equipos que son parte del Centro de Datos, los equipos de redes y los equipos personales, los cuales se encuentran detallados en la Tabla No. 4.

Tabla 4: Inventario de Equipos de DIRTIC

CANTIDAD	EQUIPOS
DATACENTER	
2	SERVIDORES HP DL
8	SERVIDORES IBM X3550
19	SERVIDORES HP BLADE
1	STORAGE HITACHI HUS130
1	STORAGE IBM STORWISE V7000
2	FIREWAL CISCO ASA 5520
REDES	
2	SWITCH CISCO 2960 48 PTOS
1	SWITCH CISCO 2960 24 PTOS
2	SWITCH CISCO 4550
EQUIPOS PERSONALES	
21	EQUIPOS DE ESCRITORIO
20	LAPTOPS

Fuente: Dirtic

CAPÍTULO 4

DEFINICIÓN DE LA METODOLOGÍA

4.1 DEFINICIÓN DE LA METODOLOGÍA

Las metodologías utilizadas para la implementación provienen de los siguientes organismos: Departamento de Justicia de los Estados Unidos (DOJ) [14], Instituto Nacional de estándares y tecnología de los Estados Unidos (NIST) [8] y el Grupo de Trabajo de Investigación Forense Digital (DFRWS) [15].

Establecer las ventajas y desventajas de las metodologías escogidas, es el primer paso para poder implementar la metodología en la Dirección de Tecnologías de Información y comunicaciones, así como también las

fases que tienen cada una de ellas. En el anexo “C” podemos encontrar las ventajas y desventajas de cada una de ellas.

La metodología NIST dada las ventajas y desventajas conocidas será la base para la aplicación en DIRTIC, y para ello utilizaremos los cuatro procesos básicos: recolección, revisión, análisis y presentación de resultados, como se muestra en la figura No 4.1.

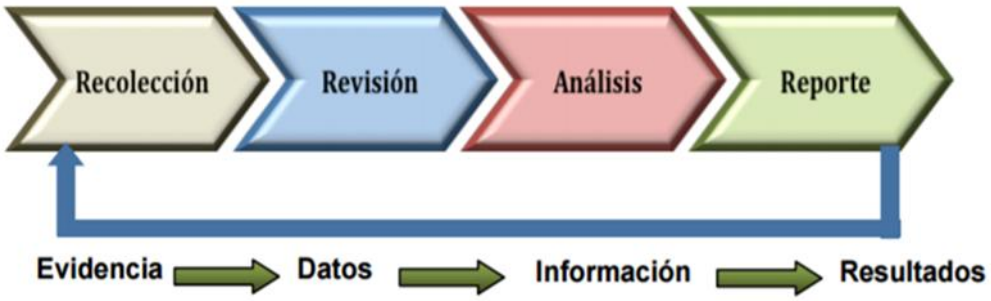


Figura 4.1: Procesos básicos de la Metodología NIST

Sin embargo, para comenzar con la metodología debemos comenzar primero con el requerimiento de la investigación para lo cual utilizaremos el formulario FOR-SIN-001 – Solicitud de análisis forense, descrito en el anexo “D”

4.2 FASE I: RECOLECCIÓN

El primer paso en la metodología forense es identificar las posibles fuentes de datos y que podemos encontrar en ellos, para ello debemos seguir los siguientes pasos: Identificar las posibles fuentes de datos,

adquisición de los datos y las consideraciones de respuestas a incidentes.

Para esta fase se utilizará los formatos del anexo “E”: Formulario de recolección de información y Formato de Cadena de Custodia.

4.2.1 IDENTIFICAR POSIBLES FUENTES DE DATOS

El gran uso de la tecnología digital, tanto para fines profesionales y personales ha ocasionado que exista una gran cantidad de fuentes de datos. Las fuentes de datos más comunes son los computadores, servidores, dispositivos de almacenamiento en red y ordenadores personales. Estos equipos poseen periféricos tales como CD y DVD, y también tienen varios tipos de puertos: USB, firewire, tarjeta de memoria y PCMCIA a los cuales los dispositivos de almacenamiento pueden unirse. Los equipos de cómputo también contienen datos volátiles que están disponibles temporalmente mientras estos estén en funcionamiento. Además, existen muchos otros tipos de dispositivos digitales como: teléfonos celulares, cámaras digitales, grabadoras digitales, reproductoras de audio que también pueden contener datos.

Esta fase establece la necesidad de reconocer las posibles fuentes de datos en un área física, las fuentes podrían ser

internas y externas. Las fuentes internas son aquellas que se encuentra la información dentro de la organización y las externas aquellas donde la información están fuera de la organización, como son los registros de actividad en la red de un proveedor de servicios de Internet (ISP). Se debe tener el control del propietario de cada fuente de datos y el efecto que esto podría tener en la recogida de datos. Por ejemplo, obtener copia de los registros del ISP normalmente requiere una orden judicial. También se debe tener en cuenta las políticas de la organización, así como las consideraciones legales, con respecto a los bienes que no son de la organización y se encuentran en las instalaciones de la organización (por ejemplo, un ordenador portátil de propiedad de un empleado o contratista). Pueden existir complicaciones si existen lugares fuera de control de la organización, como un incidente con un equipo de oficina en casa de un trabajador que trabaja a distancia. A veces no es factible recoger datos de una principal fuente de datos, por lo tanto, se debe ser consciente de las fuentes de datos alternativas que podrían contener alguna o la totalidad de los mismos datos, y se deben utilizar esas fuentes en lugar de la fuente inalcanzable.

Una de las medidas proactivas para recopilar datos que pueden ser útiles para el análisis forense, es la configuración para auditar

y registrar ciertos eventos en los sistemas operativos, como los intentos de autenticación y cambios en las políticas de seguridad. Los registros de auditoría pueden proporcionar información valiosa, incluyendo el tiempo que se produjo un evento y el origen del evento. Otra acción útil es poner en práctica el registro centralizado, lo que significa que los sistemas más importantes y aplicaciones envían copia de sus registros, con esto se evita usuarios no autorizados manipulen los registro y empleen técnicas anti-forenses que dificulten el análisis. Realizar copias de seguridad de los sistemas permite ver el contenido de los sistemas en un momento particular. Además, la presencia de software de detección de intrusos, antivirus, detección y eliminación de spyware pueden generar registros que muestren cuándo y cómo un ataque o intrusión se llevaron a cabo.

4.2.2 ADQUISICIÓN DE LOS DATOS

Después de identificar posibles fuentes de datos, se necesita adquirir los datos de las fuentes. La adquisición debe realizarse utilizando un proceso de tres pasos: desarrollar un plan para adquirir los datos, la adquisición de los datos y la verificación de la integridad de los datos adquiridos.

4.2.2.1 DESARROLLAR UN PLAN PARA ADQUIRIR DATOS

El desarrollo de un plan es un paso importante en la mayoría de los casos debido a la presencia de múltiples fuentes de datos. Se debe priorizar las fuentes, estableciendo el orden en que se deben adquirir los datos. Los factores para priorizar son:

- Valor Probable: Basado en la comprensión de la situación y la experiencia previa en situaciones similares, se debe estimar la importancia relativa de cada potencial fuente de datos.
- Volatilidad: Los datos volátiles se refieren a los datos que un sistema activo pierde después de que un equipo es apagado o debido al paso del tiempo. Los datos volátiles también pueden perderse como resultado de acciones realizadas en el sistema. En muchos casos, la adquisición de datos volátiles debe tener prioridad sobre los datos no volátiles. Sin embargo, los datos no volátiles también pueden ser algo dinámico (por ejemplo, archivos de registro que se sobrescriben a medida que se producen nuevos eventos).

- Cantidad de esfuerzo requerido: La cantidad de esfuerzo requerido para adquirir diferentes fuentes de datos puede variar ampliamente. El esfuerzo no implica sólo el tiempo que pasan los analistas y otros dentro de la organización (incluidos los asesores legales), sino también el costo de los equipos y servicios (por ejemplo, expertos externos).

4.2.2.2 ADQUISICION DE DATOS

Si los datos no han sido adquiridos por herramientas de seguridad, herramientas de análisis u otros medios, el proceso general para la adquisición de datos implica el uso de herramientas forenses para recolectar datos volátiles, duplicación de fuentes de datos no volátiles para recopilar sus datos y asegurar la fuente de datos original. La adquisición de datos se puede realizar localmente o en una red.

Aunque es preferible adquirir datos localmente porque hay mayor control sobre el sistema y los datos, la recolección local de datos no siempre es factible (por ejemplo, el sistema en una habitación cerrada, el sistema en otra ubicación). Cuando se adquieren datos a través

de una red, se deben tomar decisiones sobre el tipo de datos a recopilar y la cantidad de esfuerzo a utilizar. Por ejemplo, puede ser necesario adquirir datos de varios sistemas a través de diferentes conexiones de red, o puede ser suficiente copiar un volumen lógico desde un solo sistema.

4.2.2.3 VERIFICAR LA INTEGRIDAD DE LOS DATOS

Una vez adquiridos los datos, se debe verificar su integridad. Es importante probar que los datos no han sido manipulados, esto podría ser una necesidad de carácter legal. La verificación de la integridad de los datos suele consistir en el uso de herramientas para calcular el resumen de los datos originales y los copiados, luego comparando los resúmenes para asegurarse de que son los mismos. Para esta verificación podemos utilizar herramientas que generan automáticamente el código hash, que consiste en aplicar un algoritmo (MD5, SHA1, SHA512, etc.) a un conjunto de datos (archivo, contraseña, texto, etc.) y obtener una salida alfanumérica que representa el resumen de los datos.

Figura 4.2: Representación de la función Hash

Antes de empezar a recopilar cualquier dato (de acuerdo con las políticas de la organización y los asesores legales) se debe tomar la decisión sobre la necesidad de recopilar y preservar la evidencia de una manera que apoye su uso en el futuro legal o interno. En tales situaciones, se debe seguir una cadena de custodia claramente definida para evitar las denuncias de mal manejo o manipulación de pruebas. Esto implica mantener un protocolo o un registro de cada persona que tenía la custodia física de la evidencia, documentar las acciones que realizaron con la evidencia y en qué momento, almacenar la evidencia en un lugar seguro cuando no se está usando, hacer una copia de la evidencia y realizar el examen y el análisis usando sólo la evidencia copiada y verificar la integridad de la evidencia original y copiada.

4.2.3 CONSIDERACIONES DE RESPUESTAS A INCIDENTES

Cuando se realiza un análisis forense durante la respuesta a un incidente, se debe considerar cómo y cuándo se debe contener un incidente. El aislamiento de los sistemas pertinentes de las influencias externas puede ser necesario para evitar más daños al sistema y sus datos o para preservar la evidencia. En muchos casos, se debe trabajar con el equipo de respuesta a incidentes para tomar una decisión de contención (por ejemplo, desconectando los cables de red, desconectar el poder, aumentar las medidas de seguridad física, desconectar un host). Esta decisión debe basarse en las políticas y procedimientos existentes en materia de contención de incidentes, así como en la evaluación del riesgo planteado por el incidente, de modo que la estrategia de contención o la combinación de estrategias adecuadas mitiguen suficientemente el riesgo manteniendo la integridad de la potencial evidencia, siempre que sea posible.

La organización también debe considerar de antemano el impacto que las estrategias de contención pueden tener sobre la capacidad de la organización para operar con eficacia. Por ejemplo, dejar un sistema crítico sin conexión durante varias horas para adquirir imágenes de disco y otros datos podría

afectar negativamente a la capacidad de la organización para realizar sus operaciones necesarias. En la actualidad existen herramientas que permiten obtener imágenes en caliente de los datos de un dispositivo de almacenamiento. Sin embargo, se debe considerar para minimizar las interrupciones en las operaciones de una organización.

Un paso a menudo tomado para contener un incidente es asegurar el perímetro alrededor de una computadora y limitar el acceso al personal autorizado durante el proceso de recolección para asegurar que la evidencia no se altere. Además, debe documentarse una lista de todos los usuarios que tengan acceso a la computadora, ya que estas personas pueden proporcionar contraseñas o información sobre dónde se encuentran los datos específicos. Si la computadora está conectada a una red, desconectar los cables de red conectados a la computadora puede impedir que los usuarios remotos modifiquen los datos de la computadora. Si el equipo utiliza una conexión de red inalámbrica, el adaptador de red externo se puede desenchufar de la computadora o el adaptador de red interno se puede deshabilitar para cortar la conexión de red. Si no es posible ninguna opción, el punto de acceso a la red inalámbrica que el equipo está utilizando debe ser apagado y el mismo resultado

debe obtenerse. Sin embargo, hacerlo puede impedir que los usuarios fuera del alcance de la investigación realicen sus rutinas diarias. Además, podría haber más de un punto de acceso dentro del alcance de la computadora. Algunos adaptadores de red inalámbrica intentan automáticamente conectarse a otros puntos de acceso cuando el punto de acceso principal no está disponible, de modo que el que contenga el incidente de esta manera podría implicar la desconexión de varios puntos de acceso.

Debido a que existen algunos servicios y equipos, se debe realizar una priorización de los mismos en función de su criticidad para su restauración y posterior análisis. Para lo cual se establecerá la clasificación de criticidad de los recursos [16].

Tabla 5 Criticidad de los recursos

Ponderación	**Detalle**
Alta	Los recursos afectados son muy importantes dentro de la institución y como tal comprometen el normal funcionamiento y prestación de servicios.

Media	Los recursos afectados causan molestias solo a cierta área de la institución.
Baja	Los recursos afectados causan molestias solo a cierta área de la institución.

Se debe considerar los daños producidos en los sistemas y/o equipos, durante el incidente, según la siguiente tabla.

Tabla 6 Clasificación de los daños

Ponderación	**Detalle**
Grave	Los recursos afectados son muy importantes dentro de la institución y como tal comprometen el normal funcionamiento y prestación de servicios.
Moderado	Los recursos afectados causan molestias solo a cierta área de la institución.

Leve	Los recursos afectados causan molestias solo a cierta área de la institución.

Correlacionando la criticidad de los servicios y/o equipos con el grado de afectación de incidente podemos obtener la prioridad de recuperación.

Tabla 7 Priorización de recuperación

		Criticidad de los recursos		
		Alta	Media	Baja
Daño producido	Grave	10	7	4
	Moderado	7	4	1
	Leve	4	1	1

En función de la priorización de recuperación podemos establecer que mientras más alto sea la prioridad de recuperación, también es mayor la necesidad de un análisis forense.

4.3 FASE II: REVISIÓN

Después de recopilar los datos, la siguiente fase consiste en examinar los datos, lo que implica evaluar y extraer las informaciones pertinentes de los datos recopilados. Esta fase también puede implicar pasar por alto o mitigar el SO o las características de la aplicación que obscurecen los datos y el código, como la compresión de datos, el cifrado y los mecanismos de control de acceso. Un disco duro adquirido puede contener cientos de miles de archivos de datos; La identificación de los archivos de datos que contienen información de interés, incluida la información oculta a través de la compresión de archivos y el control de acceso, puede ser una tarea desalentadora. Además, los archivos de interés pueden contener información extraña que debe ser filtrada. Por ejemplo, el registro de firewall de ayer puede contener millones de registros, pero sólo cinco de los registros pueden estar relacionados con el evento de interés.

Afortunadamente, se pueden utilizar varias herramientas y técnicas para reducir la cantidad de datos que hay que tamizar. Las búsquedas de texto y patrones se pueden utilizar para identificar datos pertinentes, tales como encontrar documentos que mencionan un sujeto o persona en particular, o identificar entradas de registro de correo electrónico para una dirección de correo electrónico particular.

Otra técnica útil es utilizar una herramienta que puede determinar el tipo de contenido de cada archivo de datos, como texto, gráficos, música o un archivo comprimido. El conocimiento de los tipos de archivos de datos se puede utilizar para identificar los archivos que merecen un mayor estudio, así como para excluir los archivos que no son de interés para el examen. También hay bases de datos que contienen información sobre archivos conocidos, que también se pueden utilizar para incluir o excluir

4.4 FASE III: ANÁLISIS

Una vez extraída la información relevante, se debe estudiar y analizar los datos para sacar conclusiones de la misma. La base de la investigación forense es utilizar un enfoque metódico para buscar conclusiones basadas en los datos disponibles o determinar que todavía no se puede sacar ninguna conclusión. El análisis debe incluir identificar personas, lugares, artículos y eventos, y determinar cómo estos elementos están relacionados para que se pueda llegar a una conclusión. A menudo, este esfuerzo incluirá la correlación de datos entre múltiples fuentes. Por ejemplo, un registro del sistema de detección de intrusos de red (IDS) puede vincular un evento a un host, los registros de auditoría del host pueden vincular el evento a una cuenta de usuario específica y el registro IDS del host puede indicar qué acciones realizó ese usuario. Herramientas como el registro centralizado y el software de gestión de

eventos de seguridad pueden facilitar este proceso reuniendo y correlacionando automáticamente los datos. La comparación de las características del sistema con las líneas de base conocidas puede identificar varios tipos de cambios realizados en el sistema.

Una técnica muy utilizada para el análisis de la información es la línea de tiempo donde es posible identificar y correlacionar los eventos ocurridos durante un incidente en una secuencia de tiempo.

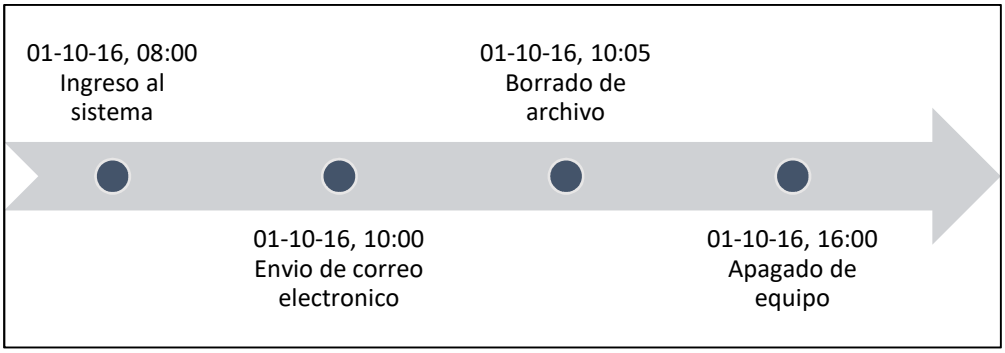


Figura 4.3: Ejemplificación de línea de tiempo

4.5 FASE IV: PRESENTACIÓN DE RESULTADOS

La fase final es la presentación de informes, que es el proceso de preparación y presentación de la información resultante de la fase de análisis. Muchos factores afectan al reporte, incluyendo los siguientes:

- Explicaciones alternativas: Cuando la información sobre un evento es incompleta, puede que no sea posible llegar a una explicación definitiva de lo sucedido. Cuando un evento tiene dos o más

explicaciones plausibles, cada uno debe tener la debida consideración en el reporte. Se debe utilizar un enfoque metódico para tratar de probar o refutar cada posible explicación que se propone.

- Consideración de la audiencia: Es importante conocer la audiencia a la que se mostrarán los datos o la información. Un incidente que demanda la aplicación de la ley, requiere de informes altamente detallados de toda la información recopilada, y también puede necesitarse la copia de todos los datos probatorios obtenidos. Es posible que el administrador del sistema desee ver el tráfico de la red y las estadísticas relacionadas con gran detalle. La alta dirección podría simplemente querer una visión general de alto nivel de lo ocurrido, como una representación visual simplificada de cómo ocurrió el ataque y qué se debe hacer para prevenir incidentes similares.
- Información Procesable: Los informes también incluyen la identificación de la información procesable obtenida de los datos que pueden permitir recopilar nuevas fuentes de información. Por ejemplo, una lista de contactos puede ser desarrollada a partir de los datos que podrían dar lugar a información adicional acerca de un incidente o delito. Además, podría obtenerse información que pudiera prevenir eventos futuros, como una puerta trasera en un sistema que podría utilizarse para futuros ataques, un crimen que se está planificando, un gusano programado para comenzar a propagarse en un momento

determinado o una vulnerabilidad que podría ser explotada. Los informes también incluyen la identificación de información.

Como parte del proceso de la presentación del informe, se debe identificar cualquier problema que pueda necesitar ser remediado, como deficiencias en las políticas o los errores de procedimiento. Muchos equipos de análisis forense y respuesta a incidentes realizan revisiones formales después de cada evento importante. Tales revisiones tienden a incluir consideraciones de posibles mejoras en las directrices y procedimientos y por lo menos algunos cambios menores son aprobados e implementados después de cada revisión. Por ejemplo, un problema común es que muchas organizaciones consideran que requieren muchos recursos para mantener actualizadas las listas de personal a contactar con respecto a cada tipo de incidente que puede ocurrir. Otro problema común es qué hacer con los gigabytes o terabytes de datos recolectados durante una investigación y cómo se pueden modificar los controles de seguridad (por ejemplo, auditoría, registro, detección de intrusiones) para registrar datos adicionales que serían útiles para futuras investigaciones. Los exámenes formales pueden ayudar a identificar maneras de mejorar estos procesos. Una vez que se implementan los cambios en las directrices y procedimientos, todos los miembros del equipo deben ser informados de los cambios y frecuentemente recordados de los procedimientos apropiados a seguir. Los equipos comúnmente tienen

mecanismos formales para rastrear los cambios e identificar las versiones actuales de cada proceso y procedimiento. Además, muchos equipos tienen carteles u otros documentos muy visibles montados en las paredes o las puertas que recuerdan los pasos claves a tomar, por lo que todo el mundo debe recordar constantemente de cómo se supone que las cosas se deben hacer.

Además de abordar los problemas identificados, se debe tomar otras medidas para mantener y aumentar las habilidades. Como por ejemplo certificarse o acreditarse, algunos examinadores forenses deben actualizarse periódicamente con las últimas herramientas y técnicas relacionadas con medios de almacenamiento informático, tipos de datos y formatos, y otros temas relevantes. Ya sea necesario o no, la renovación periódica de las habilidades a través de cursos, experiencia en el trabajo y fuentes académicas, esto ayuda a asegurar que los que realizan acciones forenses se mantengan al ritmo de las tecnologías en rápida evolución y las responsabilidades laborales. La revisión periódica de las políticas, directrices y procedimientos también ayuda a asegurar que la organización se mantenga al día con las tendencias de la tecnología y los cambios en la legislación.

Para la emisión del informe técnico se utilizará el formato del anexo “D”: Formato de Informe Técnico.

En caso de encontrarse un delito tipificado en el Código Integral Penal, COIP, este debería seguir su trámite de denuncia a la fiscalía, para que sea un perito calificado el que realice el proceso investigativo y quien deberá presentar un informe que contendrá como mínimo lo siguiente: lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas, las conclusiones y la firma [17].

4.6 HERRAMIENTAS COMUNMENTE UTILIZADAS

Actualmente existe gran cantidad de herramientas destinadas al análisis forense, tanto gratuita como licenciada y que trabajan sobre distintos aspectos de los equipos a analizar, por ejemplo, sobre las aplicaciones, las memorias, los dispositivos de almacenamiento, los protocolos de red, etc. También existen suites que ofrecen análisis sobre varios de estos puntos en conjunto, lo que facilita su uso. A continuación, se describe las herramientas gratuitas según el ámbito de trabajo:

- **Herramientas de análisis de red**
  - Snort: Es un programa de detección de intrusiones que trabaja en la red y es utilizado como analizador. Puede generar un registro de los sucesos que afecten al sistema analizado. Posee filtros los cuales deben ser configurados de acuerdo a las necesidades [17].

- Nmap: Es un analizador de puertos muy utilizado para auditorías de seguridad y para localizar evidencias en un proceso forense [18].
- Wireshark: Programa que puede analizar protocolos de red y el tráfico que existe en una red. Genera informes que pueden ser exportados a archivos de texto, para un posterior análisis forense [19].
- Xplico: Es una herramienta de análisis forense de red de código abierto, soporta una gran cantidad de protocolos. Esta herramienta genera la información capturada en formato PCAP, y la separa en función de los protocolos. Además, puede realizar el análisis de archivos de gran tamaño. Como una funcionalidad de apreciar es que puede pre visualizar las imágenes que han sido accedidas durante el periodo de captura [20].

Herramientas para tratamiento de discos

- Dcdd3: Software utilizado para trabajar en los discos de los equipos que van a ser analizados. Realiza copias a bajo nivel con la finalidad de proteger el disco original. Además, realiza copias de imágenes de gran tamaño en partes más pequeñas lo que ayuda en la manipulación y posterior análisis [21].
- Mount Manager: Es un programa para tratamiento de discos. Entre sus funcionalidades destaca: mostrar, montar y desmontar,

inspeccionar y gestionar unidades de almacenamiento conectadas. [22].

- Guymager: Programa que permite la copia bit a bit o réplicas de la imagen de un disco [23].
- FTK Imager: Herramienta que permite la obtención de imágenes de discos y posterior análisis de la información [24].

Herramientas para tratamiento de memoria

- Volatility: Es la plataforma de análisis forense de memoria más utilizada en el mundo. Es capaz de analizar volcados con datos en raw, crash dumps de sistemas operativos Windows, Linux etc. A partir de los datos se pueden extraer: tipo de sistema, fecha y hora, puertos abiertos, ficheros cargados por procesos, así como DLL, módulos del kernel, direccionamiento de memoria por procesos, claves de registro utilizadas en los procesos, etc. [25].
- Memoryze: Permite la captura de memoria RAM en equipos con sistemas operativos Windows y OSX [26].
- RedLine: Software que permite detectar signos de actividad maliciosa, mediante el análisis de memoria, archivos y el desarrollo de un perfil de la amenaza [27].

Herramientas para el análisis de aplicaciones

- OllyDbg: Esta aplicación permite desensamblar y depurar aplicaciones o procesos para Windows. Almacena y depua DLLs y

escanea toda clase de archivos. No requiere instalación lo que impide la creación de nuevas entradas en el registro de la máquina donde se trabaje [28].

- OfficeMalScanner: Es una utilidad utilizada para escanear archivos de Microsoft Office, busca códigos maliciosos, como, por ejemplo: macros, conectores OLE o ficheros encriptados [29].
- Radare: Aplicación que permite aplicar ingeniería inversa para analizar código de una aplicación maliciosa que se ha ejecutado en algún equipo [30].
- Process explorer: Programa que muestra información de los procesos que se encuentren abiertos en un equipo. Ayuda a localizar problemas de versión de DLL o pérdidas de identificadores. Ofrece también, detalles internos acerca del funcionamiento de Windows y aplicaciones [31].
- PDFStreamDumper: Aplicación que permite el análisis de código malicioso en archivos PDF. Tiene herramientas especializadas para tratar con JavaScript obscurecido, encabezados y objetos pdf de bajo nivel y shellcode [32].

Suites de aplicaciones

- DEFT: Es una distribución hecha para análisis forense, con el propósito de correr en directo en sistemas sin alterar o corromper dispositivos (discos duros, pendrives, etc. ...) conectados a la

computadora donde el proceso de arranque tiene lugar. Entre sus características esta, la recuperación de ficheros del sistema con el uso aplicaciones que facilitan la obtención de información asociada a usuarios y su actividad con el equipo. Además, mediante el uso de distintas herramientas se puede recuperar las contraseñas del sistema y generar informes y obtención de evidencias [33].

- Osforensics: Es una herramienta de investigación digital que permite extraer datos forenses o descubrir información oculta de una computadora. Ofrece una variedad de características de búsquedas avanzadas que permiten descubrir las actividades realizadas en el equipo o en Internet, archivos borrados, contraseñas almacenadas y otras informaciones forenses [34].
- CAINE (Computer Aided INvestigate Environment): Es un conjunto de herramientas que ofrece un entorno forense completo. Brinda entorno interoperable que apoya al investigador digital durante las cuatro fases de la investigación digital y con herramientas fáciles de usar, así como un proceso semiautomático para generar informes con los resultados obtenidos [35].
- Autopsy: Es un conjunto de herramientas de código abierto para el análisis de imágenes de discos. Esta suite actualmente se encuentra disponible también para OS X y Windows. permite analizar de forma eficiente discos duros y teléfonos inteligentes.

Tiene una arquitectura de plug-in que le permite encontrar módulos complementarios o desarrollar módulos personalizados en Java o Python. [36].

CAPÍTULO 5

IMPLEMENTACIÓN DE LA METODOLOGÍA

5.1 DESCRIPCIÓN DEL CASO

5.1.1 DESCRIPCIÓN

Para la implementación de la Metodología utilizaremos un caso hipotético de mal uso de información calificada luego de una fuga de información provocada supuestamente por parte de un miembro de la Institución

La Institución se encuentra regularmente inmersa en procesos contractuales, para la adquisición de servicios a los diferentes proveedores, sin embargo, en los tres últimos procesos realizados,

los representantes de algunas empresas han presentado su protesta porque indican que solamente una empresa ha ganado los concursos e indican que probablemente esta empresa ha recibido información privilegiada.

El departamento encargado de realizar las adquisiciones es el Administrativo-Financiero donde trabajan solamente dos funcionarios y que tienen acceso a toda la información de los procesos.

Se sospecha del Analista Financiero, quien en los últimos meses ha mostrado indicios de mantener problemas económicos, por lo cual se presume que la información haya sido enviada mediante correo electrónico.

El señor Director ha solicitado al departamento de Seguridad, que examine la estación de trabajo del Analista Financiero en busca de una evidencia que indique si ha existido mal uso de la información.

5.1.2 DETALLES TÉCNICOS DEL CASO

La computadora utilizada por el funcionario, funciona bajo el sistema operativo Windows, en la versión de Windows 7.

El tipo de sistema operativo usado por el equipo, constituye la realidad actual de uso de los sistemas operativos alrededor del mundo. Según Net Market Share[4], el sistema operativo con mayor penetración en el mercado en el año 2016, es el Windows 7. Como se lo puede observar la figura No. 5.1.

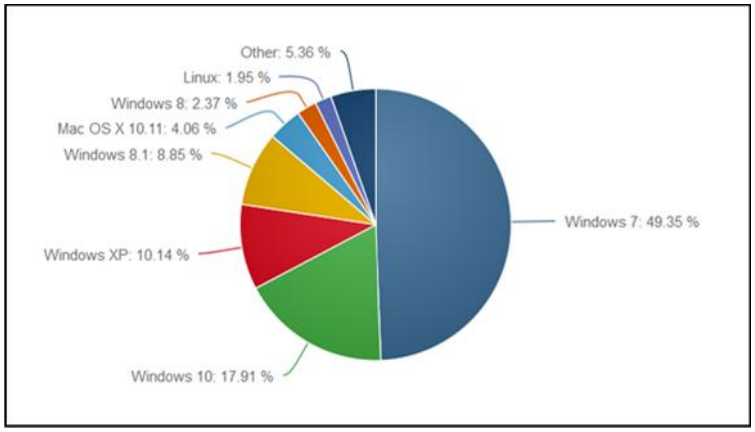


Figura 5.1 Distribución de los sistemas Operativos

A continuación, se muestra el detalle del software utilizado en el equipo utilizado en el caso.

Tabla 8: Software utilizado

Software Utilizado
Microsoft Windows 7

[4] Net Marquet Share es un sitio web dedicado a realizar estadísticas de tecnología de internet.

Microsoft Office 2010
Adobe Acrobat Reader
Firefox Mozilla
Microsoft Outlook

5.2 APLICACIÓN DE LA METODOLOGÍA

Para comenzar con la aplicación de la metodología propuesta, se requiere tener legalizado el requerimiento de la investigación mediante el llenado del formulario FOR-SIN-001 – Solicitud de análisis forense. (ver Anexo G).

5.2.1 ETAPA DE RECOLECCIÓN

De acuerdo a la metodología propuesta en este trabajo de investigación, el primer paso es la etapa de recolección, el cual consiste en tres fases:

1. Identificación de posibles fuentes de datos.

Para este paso vamos analizar las fuentes internas, por lo tanto, la fuente de la información es el disco duro del computador donde se presume hubo el incidente.

2. Adquisición de los datos.

En este paso procedemos a sacar una copia del disco duro y para lo cual procedemos a llenar el FOR-SIN-002 – Formato de Recolección de Información (ver Anexo G). También realizamos el llenado del FOR-SIN-003 – Formato de la Cadena de Custodia (ver Anexo G), para llevar un control del dispositivo que se va a realizar el análisis forense.

Para la realización de una copia del disco, utilizamos la herramienta FTK Imager y cuya pantalla la visualizamos en la figura No. 5.2.

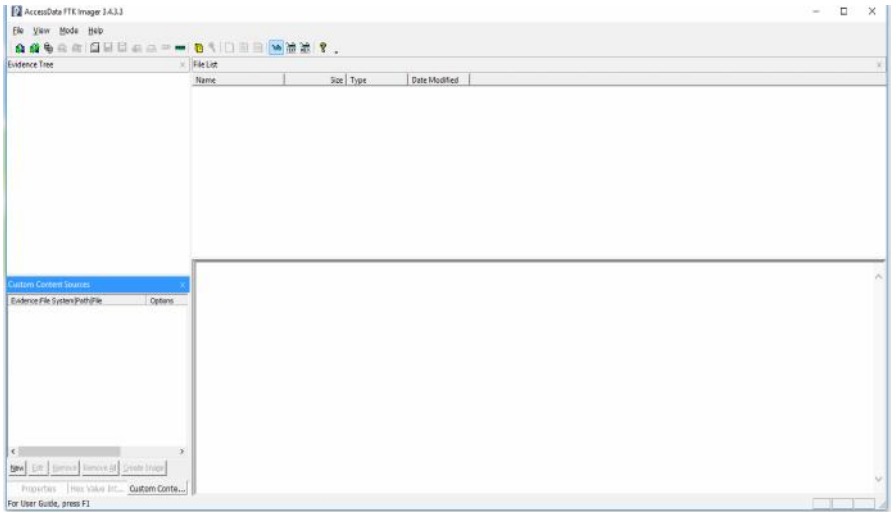


Figura 5.2 Pantalla del FTK Imager

Realizado el proceso de generación de la copia, procedemos a registrar la información generada.

Tabla 9 Información de la imagen Caso

Nombre de la Imagen	IMG- DIRTIC-AYF-002
Nombre del dispositivo del origen	DIRTIC-AYF-002
Identificador de la Cadena de custodia	FOR-SEG-003; No. 001
Identificador del dispositivo donde se almacena la imagen	Disco externo 1 TB
Herramienta usada	FTK Imager
MD5 de la herramienta	f7bb1825d22c1263f8983f85b05d0568
MD5 de la imagen generada	ef6a7ab2afb99dfdb3218f9d35998130

3. Consideraciones de respuesta a incidentes.

En este caso por ser una máquina de un usuario, mientras se desarrolla el análisis forense de la computadora se asignó otro computador al funcionario para que siga con sus labores normales.

5.2.2 ETAPA DE REVISIÓN

Para el desarrollo de esta fase, utilizaremos la herramienta FTK Imager, la cual luego del proceso de montado de la imagen nos permitirá observar todas las particiones existentes en la evidencia, como se lo muestra en la figura No. 5.3.

Para comprobar la teoría expuesta, es necesario ubicar los archivos del correo electrónico del Microsoft Outlook, los cuales se encuentran en el directorio C:\Users\Analista\Documents\Archivos de Outlook y utilizan la extensión “.pst”.

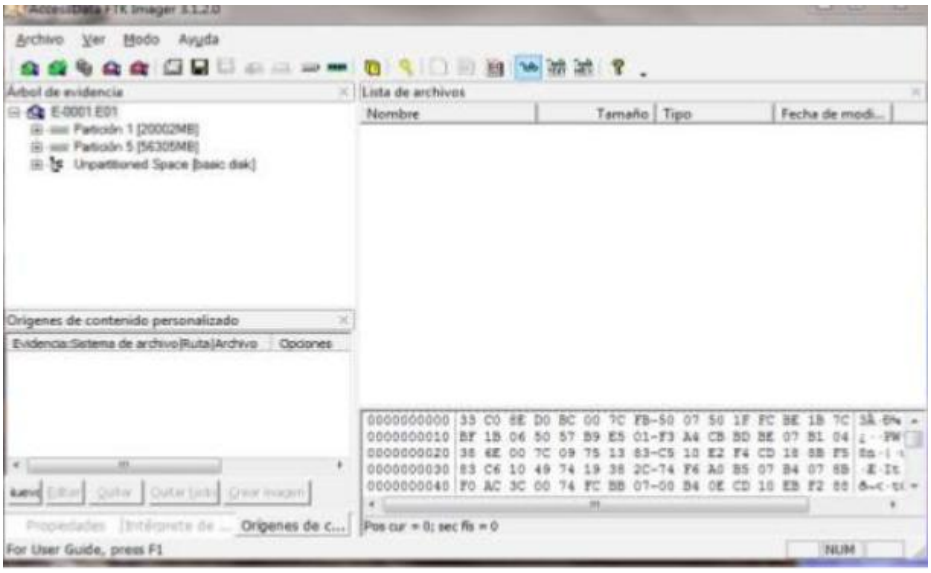


Figura 5.3 Directorio de ubicación del archivo .pst

Identificado el archivo, se procede a recuperarlo con la misma herramienta para su análisis posterior. Para esta exportación del archivo también se hace una comprobación mediante la función hash MD5.

Realizado el proceso de exportación del archivo, se procede a registrar la información generada.

Tabla 10: Información de archivo Outlook encontrado

Nombre de la Imagen	IMG- DIRTIC-AYF-002
Identificador del Hallazgo	HAL-01-DIRTIC-AYF-002
Nombre del archivo	Outlook.pst
Ubicación	C:\Users\Analista\Documents\Archivos de Outlook
Herramienta usada	FTK Imager
MD5 del archivo	220127f1f1b2bc8e268966a5fa152379
Descripción	Archivo que contiene el historial del correo electrónico utilizado por el Analista Financiero

Para acceder a los datos del archivo Outlook.pst y a fin de evitar garantizar la no alteración de la evidenciase utilizó la herramienta PSTViewer, con la cual se pudo obtener desde la bandeja de enviados un correo generado el día 12 de septiembre del 2016, donde el Analista Financiero remite un correo a la empresa ganadora con los términos de referencia del proceso, en el archivo “Terminos.docx”, antes de ser publicado el proceso.

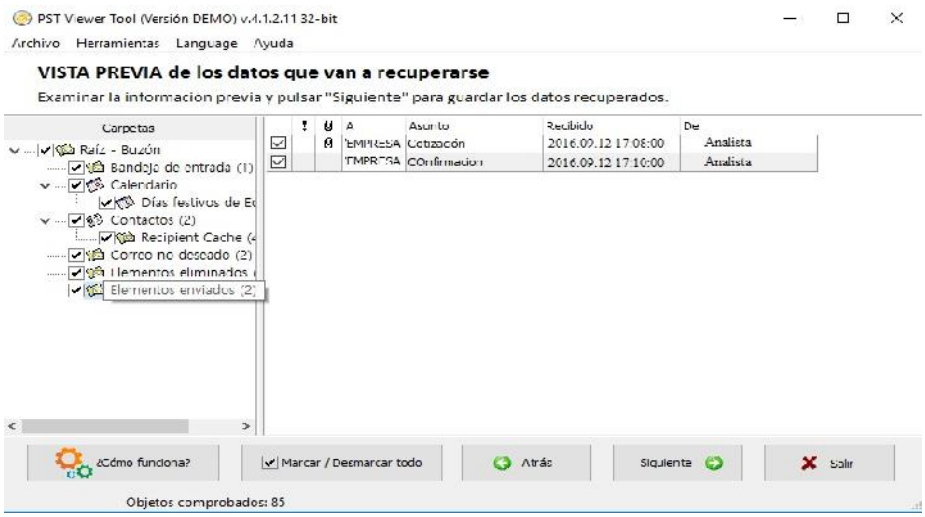


Figura 5.4 Información del archivo Termino.docx

Una vez realizado el proceso de acceder a los datos, se procede a registrar la información del archivo encontrado.

Tabla 11 Información del archivo .doc. encontrado

Nombre de la Imagen	IMG- DIRTIC-AYF-002

Identificador del Hallazgo	ARC-01-DIRTIC-AYF-002
Nombre del archivo	Terminos.docx
Ubicación	C:\Users\Analista\Documents\Archivos de Outlook
Herramienta usa	FTK Imager
MD5 del archivo	220127f1f1b2bc8e268966a5fa152379
Descripción	Archivo que contiene los términos de referencia enviados a la empresa ganadora

A fin de correlacionar el correo de la Empresa, se pudo constatar que en la bandeja de eliminados existía un correo de la Empresa hacia el funcionario, realizado el día 24 de agosto del 2016, a las 15:20.

Figura 5.5 Recuperación de correo enviado por la Empresa hacia el funcionario.

Posteriormente, procedemos a analizar el encabezado del correo para confirmar que las direcciones de origen y destino son las mismas. Encontrándose que el correo recibido desde empresa@outllok.es, el 24 de agosto del 2016 a las 15:20, es el mismo correo al cual se envió las especificaciones.

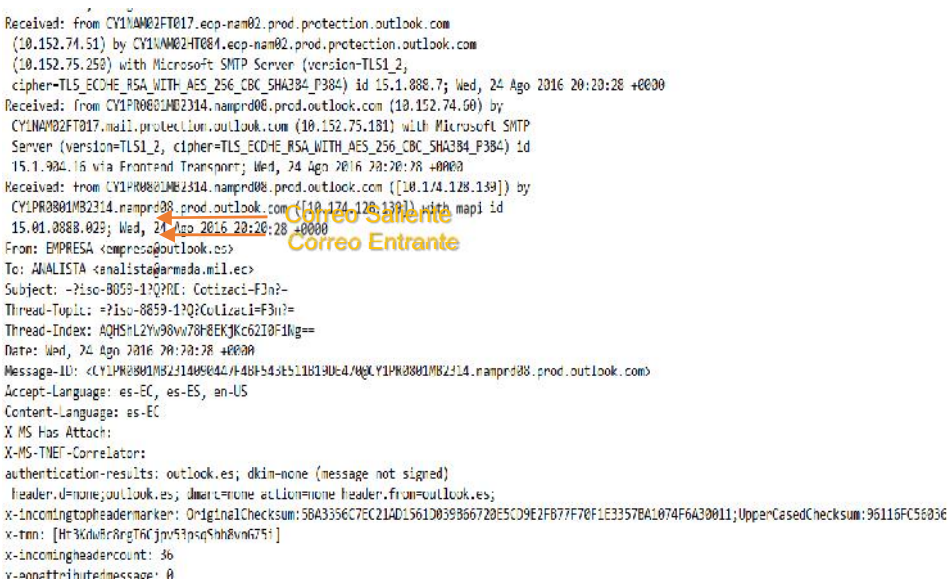


Figura 5.6 Análisis de cabecera de Correo entrante de la Empresa

5.2.3 ETAPA DE ANÁLISIS

La hipótesis planteada sobre mal uso de información confidencial en los procesos contractuales, que arrojaban como sospechoso al Analista Financiero, se puede presentar los siguientes aspectos:

Se obtuvo una imagen del disco de la máquina del analista Financiero, en esta imagen se pudo recuperar el archivo Outlook.pst en el cual se guardan el historial de los correos tramitados en la aplicación Microsoft Outlook. De la revisión del archivo .pst se evidenció la existencia de un correo del 12 de septiembre del 2016 dirigido a la empresa ganadora del proceso, cabe recalcar que este correo fue enviado 10 días antes de la publicación del proceso.

Esta situación deja en mal predicamento a la Institución debido que ha existido empresas externas que han presentado su reclamo, y a fin de evitar se continúe con este tipo de denuncias se deberán implementar mecanismos que eviten este tipo sucesos.

Para poder verificar los hechos acontecidos durante el caso, realizamos la línea de tiempo de acontecimientos, lo que nos permite recrear las actividades, relacionadas a la investigación forense.

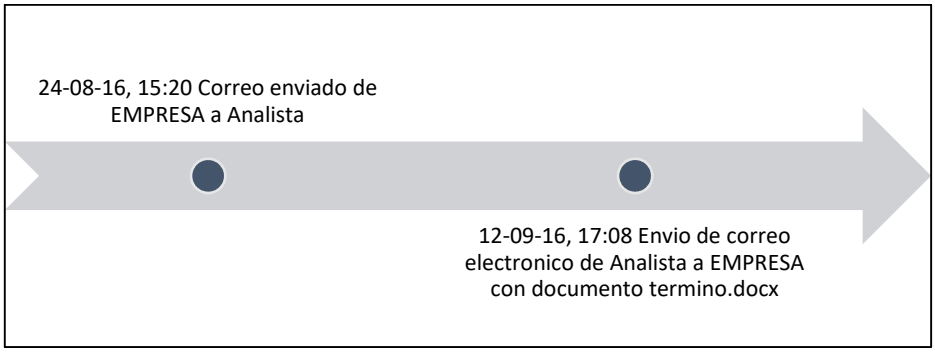


Figura 5.7 Línea de tiempo del análisis.

5.2.4 ETAPA DE PRESENTACIÓN

Esta etapa se contempla la presentación de los resultados obtenidos al finalizar la investigación. Incluye los procedimientos técnicos más relevantes, resultados y la interpretación de los mismos. Esta esta se define mediante la presentación del Informe técnico plasmado en el formato FOR-SIG-004 – Informe técnico. (ver Anexo G).

5.3 PLAN DE IMPLEMENTACIÓN

5.3.1 ORGANIZACIÓN

Como se pudo observar en el capítulo 4, la DIRTIC cuenta con un Departamento de Seguridad y Estandarización, donde existen dos divisiones Seguridad Informática y Estandarización, es necesario la creación de una sección de análisis forense dentro del departamento de Seguridad Informática, con sus respectivos

procesos y actividades. Por lo pronto se comenzará con un analista de seguridad y posteriormente dependiendo de la carga de trabajo se puede ir solicitando más personal para esta sección.

5.3.2 PERSONAL

La persona asignada a esta nueva sección, debe tener ciertas competencias para que pueda cumplir el trabajo encomendado, entre ellas debe tener un perfil de técnico informático con conocimientos de redes, sistemas operativos, usos de herramientas ofimáticas, entro otras.

5.3.3 CAPACITACIÓN

En virtud que es un campo nuevo, que no ha sido explotado en la DIRTIC, la persona asignada a este trabajo debe ser capacitado con al menos unos cursos de análisis forense y posteriormente una certificación que acredite este conocimiento.

5.3.4 EQUIPAMIENTO

En cuanto al equipamiento se puede establecer dos áreas a cubrir hardware y software. En cuanto al software se utilizará herramientas de uso libre descritas en el capítulo 4 y en cuanto al hardware se puede comenzar el trabajo con la PC de escritorio asignada al analista de seguridad y dos discos duros externos para

respaldo de las imágenes. Debido a que en el presente año no existe un presupuesto para adquirir equipamiento como: bloqueador de disco o licencias, se dejará estas necesidades para siguiente año.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 ANÁLISIS DE MÉTRICA

Como se puedo observar en el capítulo 3, los incidentes más comunes son los siguientes:

- Denegación de los servicios, por saturación en la red, DDOs
- Perdida de conectividad con los servicios.
- Saturación del Firewall
- Incidentes de código malicioso
- Mal uso de información confidencial
- Acceso no autorizado.

- Uso inapropiado de los recursos.

Luego del uso de la metodología en el caso presentado, el nuevo y reciente encargado de Análisis Forense del Departamento de Seguridad de la DIRTIC, presentó mayor confianza al momento de realizar el análisis forense del caso, pues el hecho se seguir los pasos en forma secuencial hizo que no perdiera el objetivo fijado.

Se espera que con el tiempo y la experiencia este tipo de análisis vaya mejorando y dando mejores resultados, especialmente en los tiempos de ejecución y en las exigencias de los análisis.

En la siguiente tabla podemos observar el tiempo que tomo hacer el Análisis Forense en sus distintas etapas y que serán la base para futuros trabajos. (ver Tabla 12).

Tabla 12 Tiempo de ejecución del caso de estudio

CASO DE ESTUDIO: Mal uso de información confidencial	
ETAPA	**TIEMPO CON LA METODOLOGÍA**
Etapa de recolección	3 HORAS

Etapa de revisión	12 HORAS
Etapa de análisis	3 HORAS
Etapa de presentación	3 HORAS

Sin embargo, conforme se vayan realizando nuevos casos estos deben ser considerados y registrado sus métricas como parte un mejoramiento continuo.

6.2 ANÁLISIS DE RIESGOS

Para el análisis de riegos vamos a considerar el control estadístico de la DIRTIC, sobre los incidentes más frecuentes que se desarrollan en la organización.

Tabla 13 Probabilidad de ocurrencia de incidentes

INCIDENTE	**PROBABILIDAD DE OCURRENCIA**
Perdida de conectividad con los servicios.	ALTA
Mal uso de información confidencial	ALTA

Uso inapropiado de recursos	ALTA
Denegación de los servicios, por saturación en la red, DDOs	MEDIA
Saturación del Firewall	BAJA
Incidentes de código malicioso	BAJA
Acceso no autorizado.	BAJA

Seguidamente debemos establecer a que equipos o servicios afectan estos incidentes y el impacto sobre ellos.

Tabla 14 Matriz de Impacto

		Impacto		
Equipos	**Incidentes**	**ALTO**	**MEDIO**	**BAJO**
Servidores	Perdida de conectividad con los servicios.	x		
	Uso inapropiado de recursos		x	
	Denegación de los servicios, por saturación en la red, DDOs	x		

	Incidentes de código malicioso		x	
	Acceso no autorizado	x		
Storage	Perdida de conectividad con los servicios.	x		
	Uso inapropiado de recursos		x	
	Acceso no autorizado	x		
Firewall	Denegación de los servicios, por saturación en la red, DDOs	x		
	Saturación del Firewall	x		
	Acceso no autorizado	x		
Equipos de redes	Perdida de conectividad con los servicios.	x		
	Acceso no autorizado	x		
Computadores	Mal uso de información confidencial		x	
	Uso inapropiado de recursos		x	
	Incidentes de código malicioso			x
	Acceso no autorizado			x

Dado que el cálculo del riesgo está dado a la probabilidad x el impacto, tenemos la siguiente matriz de riegos.

Tabla 15 Matriz de evaluación de riesgo

INCIDENTES	Servidores	Storage	Firewall	Redes	PC
Perdida de conectividad con los servicios.	ALTO	ALTO	BAJO	ALTO	BAJO
Mal uso de información confidencial	BAJO	BAJO	BAJO	BAJO	ALTO
Uso inapropiado de recursos	ALTO	ALTO	BAJO	BAJO	ALTO
Denegación de los servicios, por saturación en la red, DDOs	ALTO	BAJO	ALTO	BAJO	BAJO
Saturación del Firewall	BAJO	BAJO	ALTO	BAJO	BAJO

Incidentes de código malicioso	BAJO	BAJO	BAJO	BAJO	BAJO
Acceso no autorizado.	MEDIO	MEDIO	MEDIO	MEDIO	BAJO

A continuación, mostramos el mapa de calor de los riesgos presentes, en las computadoras siendo los de mayor criticidad: el mal uso de información calificada y uso inapropiado de los recursos.

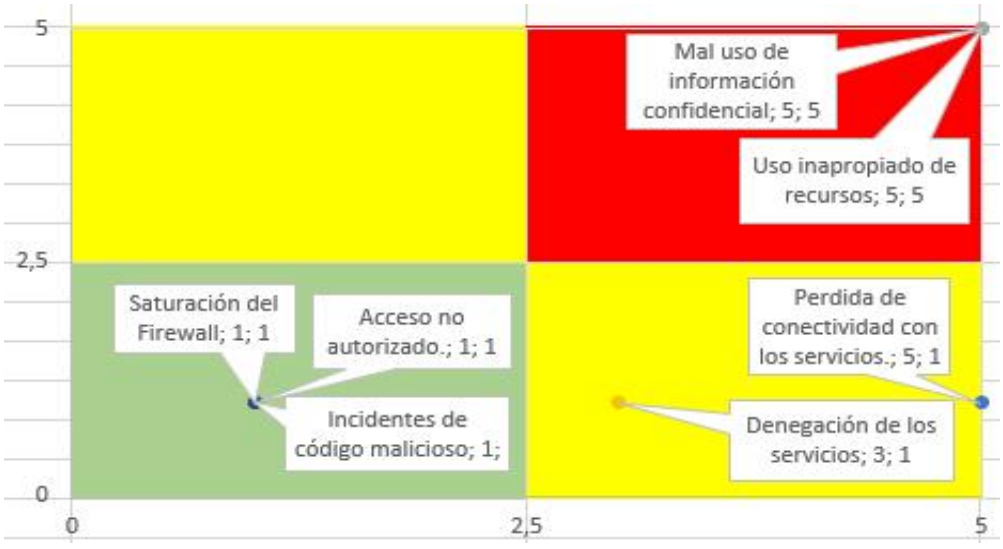


Figura 6.1 Mapa de calor de riesgos

Dentro de los controles preventivos que se pueden realizar para disminuir o minimizar los riesgos se podrían implementar algunas recomendaciones:

- Mantener actualizado todos los sistemas operativos de los servidores.
- Colocar antivirus a todas las computadoras bajo administración centralizada de su consola principal.
- Realizar de forma continua, recordatorios de las normas y procedimientos del uso de los sistemas y servicios.
- Establecer como política realizar un cambio periódico de claves a los diferentes sistemas
- Mantener una correcta configuración del Firewall, basado en estándares y mejores prácticas
- Crear acciones que permitan mitigar un ataque de DDOs.

6.3 ANÁLISIS DE IMPACTO EN EL CLIMA ORGANIZACIONAL

En la entrevista realizada a la persona encargada del análisis forense sobre la metodología que se empleó, se puede resumir en los siguientes resultados:

- El hecho de no existir un área para el análisis forense, hacía que los incidentes solo queden en un registro estadístico, sin el respectivo seguimiento y análisis.
- El contar con una metodología con los formatos establecidos, permite que el encargado pueda seguir paso las etapas del proceso, permitiendo que estos sean más agiles y efectivos.

- Aproximadamente el 70% de la DIRTIC considera que es necesario establecer el área de análisis forense para mejorar la seguridad informática, por lo que el uso de la metodología y el continuo trabajo en esta área mejorará la percepción de la seguridad.

CONCLUSIONES Y RECOMENDACIONES

1. El trabajo presentado cumple con los objetivos planteados al inicio. Se consiguió adaptar e implementar una metodología de análisis forense, que permita la investigación de incidentes de seguridad informática dentro de la Dirección de Tecnologías de Información y comunicaciones.
2. La metodología implementada ofrece una guía para realizar análisis forense a pesar de que cada caso es diferente, las etapas y los procesos estructurados, sirven de base para cualquier investigación forense dentro de la DIRTIC.

3. Debido a que la DIRTIC es una Institución del Estado y esta se rige en función de normas de Contraloría, para la Administración de los bienes, es necesario realizar una verificación a esta reglamentación.
4. Existen todavía vacíos dentro de la Institución, desde el punto de vista técnico y legal. Desde ámbito técnico es un área nueva que no ha sido explotada y no existía ningún proceso documentado con respecto al Análisis Forense, pero existe campo donde aplicarla. Desde el punto de vista legal se puede indicar que también no existe nada normado dentro de la Institución con respecto a la validez o no de un Análisis Forense.
5. Se debe realizar un plan de capacitación para el encargado de análisis forense con el objetivo de que pueda desempeñarse mejor en este nuevo trabajo y pueda brindar mejores resultados.
6. Luego de un tiempo de trabajo de la nueva área de análisis forense se debe generar una encuesta para conocer el impacto que ha tenido en la percepción de la seguridad informática

BIBLIOGRAFÍA

[1] National Institute of Standards and Technology, Glossary of Key Information Secutity Informations, Maryland, 2013.

[2] A. Toffler, La tercera Ola, Bogota: Plaza & Janes. S.A., 1980.

[3] Dicccionario Oxfort, «Dicccionario Oxfort,» 30 05 2016. [En línea]. Available: http://www.oxforddictionaries.com/definition/english/forensic..

[4] S. V. y. Lourens, A Control Framework for Digital Forensics, 2006.

[5] M. B. Cambrum, Análisis Forense Informático-Automatizacion del Proceso Digital, Montevideo, 2010.

[6] B. V. y. T. Florence, Model, The Enhanced Digital Investigation Process, Kampala, 2004.

[7] C. C. y. G. G. M. Reith, «An Examination of Digital Forensic Models,» *International Journal of Digital Ev,* 2002.

[8] National Institute of Standards and Technology, «Guide to Integrating Forenic Techniques into Incident Response,» 2006.

[9] National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response, Gaithersburg, 2006.

[10] S. Ciardhuáin, «An Extended Model of Cybercrime Investigations,» *Internation Journal of Digital Evidence,* vol. 3, nº 1, 2004.

[11] PwC, «Resusltado de la encuesta Global de seguridad de la Información 2015,» 2015.

[12] EY, «Encuesta Global de Análisis Forense de Datos 2016,» 2016.

[13] Armada del Ecuador, «Estatuto Orgánico de Gestión Orgnaizacional por Procesos,» Quito, 2015.

[14] Departament of Justice, «Justice,» 10 10 2016. [En línea]. Available: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf.

[15] Digital Forensics Research Workshop, «DFRWS,» 10 10 2016. [En línea]. Available: http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf.

[16] O. R. Almeida Romo, Metodologia para la implementacion de Informatica forense en sistemas operativos Windows y Linux, Ibarra, 2011.

[17] Ministerio de Justicia, Derechos Humanos y Cultos, Código Intergl Penal, Quito: Gráficas Ayerve, 2014.

[18] «Snort,» 10 10 2016. [En línea]. Available: https://www.snort.org/.

[19] «NMAP,» 10 10 2016. [En línea]. Available: https://nmap.org/.

[20] «Wireshark,» 10 10 2016. [En línea]. Available: https://www.wireshark.org/.

[21] «Xplico,» 10 10 2016. [En línea]. Available: www.xplico.org/.

[22] Sourceforge, «Sourceforge,» 10 10 2016. [En línea]. Available: https://sourceforge.net/projects/dc3dd/.

[23] «Linux-Apps.com,» 10 10 2016. [En línea]. Available: https://www.linux-apps.com/content/show.php/MountManager?content=76502.

[24] Sourforge, «Guymager,» 10 10 2016. [En línea]. Available: http://guymager.sourceforge.net/.

[25] «AccsessData,» 10 10 2016. [En línea]. Available: http://accessdata.com/product-download.

[26] «Volatility Foundation,» 10 10 2016. [En línea]. Available: http://www.volatilityfoundation.org/.

[27] «FireEye,» 10 10 2016. [En línea]. Available: https://www.fireeye.com/services/freeware/memoryze.html.

[28] «FireEye,» 10 10 2016. [En línea]. Available: https://www.fireeye.com/services/freeware/redline.html.

[29] «OllyDbg,» 10 10 2016. [En línea]. Available: http://www.ollydbg.de/.

[30] «Reconstructer,» 10 10 2016. [En línea]. Available: http://www.reconstructer.org/code.html.

[31] «Radare,» 10 10 2016. [En línea]. Available: http://www.radare.org/r/.

[32] Microsoft, «Technet,» 10 10 2016. [En línea]. Available: https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx.

[33] «Sandsprite,» 10 10 2016. [En línea]. Available: http://sandsprite.com/blogs/index.php?uid=7&pid=57.

[34] «Deft,» 10 10 2016. [En línea]. Available: http://www.deftlinux.net/.

[35] PassMark Software, «Osforensic,» 10 10 2016. [En línea]. Available: http://www.osforensics.com/.

[36] «CAINE,» 10 10 2016. [En línea]. Available: http://www.caine-live.net/.

[37] «Sleuthkit,» 10 10 2016. [En línea]. Available: https://www.sleuthkit.org/autopsy/.

[38] H. Rifa, J. Serra y J. Rivas, Análisis forense de sistemas infomáticos, Barcelona: Eureca Media, 2009.

[39] M. L. Delgado, Análisis Forense Digital, 2007.

[40] E. Casey, Digital Evidence and Computer Crime, Elsevier Academic Press, 2004.

[41] D. Brezinski y T. Killalea, RFC 3227: Guidelines for evidence Collection and Archiving, 2002.

GLOSARIO

Análisis forense: rama de la computación dedicada a la aplicación de técnicas científicas y analíticas para la captura, procesamiento, análisis e investigación de información almacenada en computadoras utilizando una metodología donde la evidencia descubierta es aceptable en un proceso legal.

Árbol de directorios: representación gráfica del conjunto de directorios en una unidad de almacenamiento.

Cadena de custodia: Procedimiento mediante el cual se busca garantizar la integridad de la evidencia digital mediante la documentación detallada de las interacciones y procesos a los que es sometida.

Ciencias forenses: conjunto de técnicas y procedimientos de investigación de los que está compuesta la criminalística.

DDoS: siglas en inglés para Denegación de Servicio Distribuido. Es un tipo de ataque en el que se utilizan diferentes equipos para hacer muchas peticiones a un recurso con el fin de bloquear las peticiones legítimas.

Evidencia digital: elemento de información que por su contexto puede ser considerada para ofrecer certeza clara y manifiesta de un evento ocurrido en un sistema de información.

Firma hash: cadena de longitud fija producto resultante de la aplicación de una función matemática irreversible a una cadena de longitud variable

FTK Imager: programa desarrollado por AccesData que permite realizar imágenes forenses desde diferentes medios.

Imagen forense: copia bit a bit del contenido de un dispositivo de almacenamiento.

ISP: Proveedor de Servicio de Internet.

Keylogger: dispositivo físico o programa diseñado para registrar todas interacciones de un usuario con un dispositivo de entrada, como un teclado.

Malware: cualquier software malicioso.

PSTViewer: programa desarrollado por Encryptomatic LLC que permite administrar contenidos de Microsoft Outlook.

ANEXOS

A. REPORTE DE INCIDENTES

B. ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN

C. VENTAJAS Y DESVENTAJAS DE LAS METODOLOGIAS FORENSES

D. FORMATO DE REQUERIMIENTO DE NALISIS

E. FORMATO DERECOLECCION DE INFORMACION Y CUSTODIA DE LA INFORMACION

F. FORMATO DE INFORME TECNICO

G. FORMATOS DEL CASO DE ESTUDIO

ANEXO “A”

ARMADA DEL ECUADOR

DIRECCION DE TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

REPORTE DE INCIDENTES INFORMÁTICOS

DEPARTAMENTO	PERIODO												
	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE	TOTAL
INFRAESTRUCTURA		1											1
REDES	1	2	3	2	1	1							10
SOPORTE			1		2	1							4
SEGURIDAD	3	3	3	2	1	1							13
TOTAL	4	6	7	4	4	3							28

ANEXO “B”

Encuesta de Seguridad de la Información

Esta encuesta tiene la finalidad de conocer la percepción interna sobre la seguridad de la información y la metodología de análisis forense.

BIENVENIDO.

Esperamos que sus respuestas sean lo más apegadas a la realidad del reparto.

Hay 11 preguntas en esta encuesta

SEGURIDAD DE LA INFORMACION

La escala a utilizarse es la siguiente:

1 Totalmente en desacuerdo

2 En desacuerdo

3 Neutral

4 De acuerdo

5 Totalmente de acuerdo

¿Se implementan controles de detección, prevención y recuperación de la información, para la protección contra código malicioso o virus? *

Por favor seleccione **sólo una** de las siguientes opciones:

- 1
- 2
- 3
- 4
- 5

¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información? *

Por favor seleccione **sólo una** de las siguientes opciones:

- 1
- 2
- 3
- 4
- 5

¿Han existido varios incidentes de seguridad de la información en la DIRIC en el último año? *

Por favor seleccione **sólo una** de las siguientes opciones:

- 1
- 2
- 3
- 4
- 5

¿Ha sido víctima de un ataque informático? *

Por favor seleccione **sólo una** de las siguientes opciones:

- Sí
- No

¿Considera que debe haber campañas de prevención de los delitos informáticos? *

Por favor seleccione **sólo una** de las siguientes opciones:

- 1
- 2
- 3
- 4
- 5

¿En su opinión considera suficiente la inversión en seguridad informática? *

Por favor seleccione **sólo una** de las siguientes opciones:

-) 1
-) 2
-) 3
-) 4
-) 5

ANÁLISIS FORENSE

¿Ha escuchado hablar sobre el análisis forense digital? *

Por favor seleccione **sólo una** de las siguientes opciones:

- Sí
- No

¿Conoce las ventajas del análisis forense? *

Por favor seleccione **sólo una** de las siguientes opciones:

- Sí
- No

¿Conoce si el departamento de seguridad realiza análisis forense?

Por favor seleccione **sólo una** de las siguientes opciones:

- Sí
- No
- No sabe

¿Conoce alguna metodología aplicada al análisis forense? *

Por favor seleccione **sólo una** de las siguientes opciones:

- Sí
- No

¿Considera que la implementación de una metodología de análisis forense contribuirá a la seguridad de la información?

Por favor seleccione **sólo una** de las siguientes opciones:

- Sí
- No

Agradecemos su colaboración

24/05/2016 – 08:24

Enviar su encuesta.

Gracias por completar esta encuesta.

ANEXO “C”

VENTAJAS Y DESVENTAJAS DE LAS METODOLOGIAS FORENSES

METODOLOGIA	VENTAJAS	DESVENTAJAS
DOJ	Tiene un procedimiento bien definido que proporciona los pasos a seguir en cada una de las etapas	No cubre las etapas generales necesarias para realizar una investigación forense
		Se enfoca a la investigación de equipos con sistema Windows
		No propone metodologías para realizar análisis en grandes volúmenes de información
		No se establece una cadena de custodia.
		No da resultados para mejorar el sistema.
DRFW	Cubre todas las etapas de la investigación forense	No propone un procedimiento específico para las actividades
	Define una gran gama de dispositivos y como pueden ser tratados	
	Da énfasis a preservar la integridad	

	Entrega técnicas para extracción de datos ocultos	
	Considera métodos para análisis de grandes volúmenes	
NIST	Entrega un listado de herramientas probadas	
	Tiene cuatro etapas claramente definidas	
	Es un estándar	
	Tiene el soporte de otros estándares del Instituto	
	Establece una prioridad de recolección de información volátil	
	Considera un listado de sitios de consulta	

AUTOR: Desarrollo Personal

ANEXO “D”

FORMATO DE SOLICITUD DE ANÁLISIS FORENSE

	SOLICITUD DE ANÁLISIS FORENSE	No.
		FOR-SIG-001
		FECHA:

DESCRIPCIÓN DEL INCIDENTE INFORMÁTICO	
1. Fecha de Incidente:	
2. Duración del incidente:	
3. Detalles del Incidente:	

INFORMACIÓN GENERAL	
4. Reparto:	
5. Departamento:	
6. Responsable del sistema afectado	Apellidos y Nombres:
	Cargo:
	E-mail:
	Teléfono:
	Celular

INFORMACIÓN SOBRE EL EQUIPO AFECTADO	
7. Dirección IP	
8. Nombre del equipo	
9. Marca y modelo	
10. Capacidad RAM	
11. Capacidad de disco duro	
12. Procesador	
13. Sistema Operativo	
14. Uso del equipo	
15. Tipo de información procesada por el equipo:	

FIRMAS DE RESPONSABILIDAD	
Solicitado por:	*Autorizado por:*
[Nombre y cargo del solicitante]	*[Nombre y Cargo de la persona que aprueba]*
16. Ingresado por:	*[Nombre y Cargo de la persona que registró los datos]*

Copia N° 1	Página 1 de 1

FUENTE: Autor

ANEXO “E”

FORMATO DE RECOLECCIÓN DE INFORMACIÓN

	RECOLECCIÓN DE INFORMACIÓN	No.
		FOR-SIG-001
		FECHA:

REFERENCIAS	
1. Solicitud de análisis:	

EQUIPO DE TRABAJO	
2. Líder de Equipo	
3. Analista 1	
4. Analista 2	

EQUIPOS A ANALIZAR	
5. Equipo:	
6. Características:	
5. Equipo:	
6. Características	
5. Equipo:	
6. Características:	

RECOLECCION DE DATOS	
7. Equipo:	
8. Procedimiento:	
9. Herramienta utilizada:	
7. Equipo:	
8. Procedimiento:	
9. Herramienta utilizada:	
7. Equipo:	
8. Procedimiento:	

	RECOLECCIÓN DE INFORMACIÓN	No.
		FOR-SIG-001
		FECHA:

9. Herramienta utilizada:	

FIRMAS DE RESPONSABILIDAD

Analista:	*Líder de Equipo:*
[Nombre y cargo]	*[Nombre y Cargo]*

FORMATO DE CADENA DE CUSTODIA

	CADENA DE CUSTODIA	No.
		FOR-SIG-003
		FECHA:

REFERENCIAS	
1. Solicitud de análisis:	

EQUIPO DE TRABAJO A CARGO DE LA PRUEBA O EVIDENCIA						
H	R	E	GRADO	APELLIDOS Y NOMBRES	CARGO	FIRMA

* Personas que: H-Hallo, R-Recolecto, E-Embalo

DESCRIPCIÓN DEL EQUIPO/COMPONENTE EN CUSTODIA	
2. Equipo/Componente	

MOVIMIENTOS DE LA PRUEBA O EVIDENCIA							
FECHA	HORA	GRADO	APELLIDOS Y NOMBRES	CARGO	PROPOSITO DE LA ENTREGA	OBSERVACIONES	FIRMA

ANEXO “F”

FORMATO DE INFORME TECNICO

	INFORME TÉCNICO	No.
		FOR-SIG-004
		FECHA:

1. ANTECEDENTES

2. ACTIVIDADES REALIZADAS

3. DESCRIPCION DE LAS HERRAMIENTAS UTILIZADAS

4. ANALISIS DE LA EVIDENCIA

5. CONCLUSIONES Y RECOMENDACIONES

6. REFERENCIAS

Analista: *Líder de Equipo:*

[Nombre y cargo] *[Nombre y Cargo]*

ANEXO “G”

CASO DE APLICACIÓN

	SOLICITUD DE ANÁLISIS FORENSE	No. 001
		FOR-SIG-001
		FECHA: 10-OCT-16

DESCRIPCIÓN DEL INCIDENTE INFORMÁTICO	
1. Fecha de Incidente:	*Por determinar*
2. Duración del incidente:	*desconocido*
3. Detalles del Incidente:	
Se presume un mal uso de información calificada.	

INFORMACIÓN GENERAL	
4. Reparto:	*DIRTIC*
5. Departamento:	*ADMINISTRATIVO FINACIERO*
6. Responsable del sistema afectado	Apellidos y Nombres: ANALISTA FINANCIERO
	Cargo: ANALISTA FINANCIERO
	E-mail: analista@outllok.com
	Teléfono: 2502240
	Celular:

INFORMACIÓN SOBRE EL EQUIPO AFECTADO	
7. Dirección IP	*10.128.37.46*
8. Nombre del equipo	*DIRTIC-AYF-002*
9. Marca y modelo	*Veriton M4630G*
10. Capacidad RAM	*6 Gb*
11. Capacidad de disco duro	*1 Tb*
12. Procesador	*Core i7 3.6 Ghz*
13. Sistema Operativo	*Windows 7*
14. Uso del equipo	*Trabajo*
15. Tipo de información procesada por el equipo:	*Documentación de Trabajo*

FIRMAS DE RESPONSABILIDAD	
Solicitado por:	*Autorizado por:*
SUBS-IF Jacinto Idrovo	*CPCB-TNC Alex Tapia*
16. Ingresado por:	*MARO-IF Anderson Hidalgo*

	RECOLECCIÓN DE INFORMACIÓN	No. 001
		FOR-SIG-002
		FECHA: 10-OCT-16

REFERENCIAS	
1. Solicitud de análisis:	*SOLICITUD DE ANALISIS FORENSE No 001*

EQUIPO DE TRABAJO	
2. Líder de Equipo	*CPCB-TNC ALEX TAPIA*
3. Analista 1	*MARO-IF ANDERSON HIDALGO*
4. Analista 2	

EQUIPOS A ANALIZAR	
5. Equipo:	*COMPUTADOR DE ESCRITORIO DIRTIC-AYF-002*
6. Características:	*COMPUTADOR VERITON M4630G, PROCESADOR CORE I7 3,6 Ghz, 6Gb RAM, 1Tb DISCO DURO, SISTEMA OPERATIVO WINDOWS 7*

RECOLECCIÓN DE DATOS	
7. Equipo:	*COMPUTADOR DE ESCRITORIO DIRTIC-AYF-002*
8. Procedimiento:	*MAL USO DE INFORMACIÓN CALIFICADA – EXTRACCION DE CORREO*
9. Herramientas utilizadas:	*FTK IMAGER* *PST VIEWER*

FIRMAS DE RESPONSABILIDAD	
Analista:	*Líder de Equipo:*
MARO-IF Anderson HIDALGO	*CPCB-TNC Alex Tapia*

	CADENA DE CUSTODIA	No. 001
		FOR-SIG-003
		FECHA: 10-OCT-16

REFERENCIAS	
1. Solicitud de análisis:	*No 001*

EQUIPO DE TRABAJO A CARGO DE LA PRUEBA O EVIDENCIA						
H	**R**	**E**	**GRADO**	**APELLIDOS Y NOMBRES**	**CARGO**	**FIRMA**
X	**X**	**X**		**MARO-IF ANDERSON HIDALGO**	**ANALISTA**	

- **Personas que: H-Hallo, R-Recolecto, E-Embalo**

DESCRIPCIÓN DEL EQUIPO/COMPONENTE EN CUSTODIA	
2. Equipo/Componente	*DISCO DURO DE 80 GB*

MOVIMIENTOS DE LA PRUEBA O EVIDENCIA							
FECHA	**HORA**	**GRADO**	**APELLIDOS Y NOMBRES**	**CARGO**	**PROPOSITO DE LA ENTREGA**	**OBSERVACIONES**	**FIRMA**
10-OCT-16	0800	CPCB	ALEX TAPIA	LIDER	OBTENER IMAGEN	PRESTAMO 4 HORAS	

	INFORME TÉCNICO	No. 001
		FOR-SIG-004
		FECHA:12-OCT-17

1. ANTECEDENTES

El día 10 de octubre de 2016 el Director de Tecnologías de Información y Comunicaciones, solicita una investigación basada en cómputo forense para identificar al responsable de la fuga de información relacionada a procesos contractuales

Se solicita la revisión del equipo de cómputo para identificar la actividad relacionada con la posible fuga de información, al inicio de la investigación el equipo se encontró apagado por lo que se procedió a la recopilación de la información.

2. ACTIVIDADES REALIZADAS

La investigación fue realizada por el analista de seguridad y toda la documentación correspondiente se encuentra en el expediente Caso SIN-001. Durante la investigación se realizaron las siguientes actividades:

- Autorización para iniciar el análisis forense
- Generación de una imagen forense del sistema afectado.
- Ubicación de los registros del correo electrónico.
- Análisis del archivo de correo electrónico.
- Ubicación del correo con la información confidencial
- Análisis y conclusiones de lo encontrado

3. DESCRIPCION DE LAS HERRAMIENTAS UTILIZADAS

Para este trabajo se utilizaron dos herramientas: FTK Imager y PSTViewer

- FTK Imager es la herramienta que permitió realizar la imagen del disco de la computadora perteneciente al Analista Financiero y posteriormente con esta misma herramienta se utilizó para la búsqueda de los archivos.

- PSTViewer es la herramienta que permitió visualizar el archivo de Outlook, a fin de no afectar a los registros del archivo.

4. ANALISIS DE EVIDENCIA

La hipótesis planteada sobre mal uso de información confidencial en los procesos contractuales, que arrojaban como sospechoso al Analista Financiero, se puede presentar los siguientes aspectos:

Se obtuvo una imagen del disco de la máquina del analista Financiero, en esta imagen se pudo recuperar el archivo Outlook.pst en el cual se guardan el historial de los correos tramitados en la aplicación Microsoft Outlook. De la revisión del archivo .pst se evidenció la existencia de un correo del 12 de septiembre del 2016 dirigido a la empresa ganadora del proceso, cabe recalcar que este correo fue enviado 10 días antes de la publicación del proceso.

También se realizó un análisis del encabezado de un correo entrante, del 24 de agosto del 2016, de la Empresa ganadora hacia el funcionario, con la finalidad de verificar la autenticidad del correo, encontrándose que el correo es el mismo al cual fue enviado los términos de referencia.

Esta situación deja en mal predicamento a la Institución debido que ha existido empresas externas que han presentado su reclamo, y a fin de evitar se continúe con este tipo de denuncias se deberán implementar mecanismos que eviten este tipo sucesos.

5. CONCLUSIONES Y RECOMENDACIONES

Después de analizar el sistema fue posible identificar que el mal uso de información calificada se llevó a cabo a través del servicio de correo electrónico. Se utilizó la cuenta "analista@outlook.com" para enviar el archivo "Terminos.docx", archivo que contiene los términos de referencia del proceso contractual adjudicado a la empresa ganadora. La información fue enviada a la

cuenta de correo "empresa@outlook.com", el día 12 de septiembre de 2016, a las 17:08.

De acuerdo a la información proporcionada al inicio de la investigación, la persona responsable de la cuenta de correo "analista@outlook.com" es la persona que labora como Analista Financiero dentro de la DIRTIC.

No hay evidencia del uso de algún otro mecanismo de extracción de información en el sistema. Tampoco existe evidencia de una posible intrusión no autorizada al sistema.

A fin de evitar que vuelven a ocurrir este tipo de acciones se debe seguir las siguientes acciones:

- Se debe realizar un recordatorio al personal sobre el manejo de la información confidencial y el uso del correo electrónico.
- Iniciar el proceso disciplinario al Analista Financiero, por mal uso de la información confidencial.

6. REFERENCIAS

- FOR-SIG-001 Solicitud de análisis forense No. 001
- FOR-SIG-002 Recolección de la información N0. 001
- FOR-SIG-003 Cadena de custodia N0. 001
- Reglamento de Disciplina Militar.

Analista:	*Líder de Equipo:*
MARO-IF Anderson Hidalgo	CPCB-TNC Alex Tapia