Trabajo de Grado para optar por el título de Especialistas en Gerencia de TI

Título

“EL ANÁLISIS FORENSE COMO PROTOCOLO PARA INVESTIGACIÓN DE INCIDENTES INFORMÁTICOS EN LOS SISTEMAS DE INFORMACIÓN DE EMPRESAS COMERCIALES”

Por

JASMIN RODRIGUEZ POSADA

Correo electrónico: jasminrp@interlan.com.co

MONICA BETANCUR RESTREPO

Correo electrónico: monicabr@interlan.com.co

Curso: trabajo de grado

Asesor temático: ANA MARIA MESA ELNESER

Asesor metodológico: JORGE MARIO GAVIRIA HINCAPIE

**FUNDACIÓN UNIVERSITARIA LUIS AMIGO
FACULTAD DE INGENIERIAS**

**MEDELLÍN
2012**

NOTA DE ACEPTACIÓN

Asesor temático

Asesor metodológico

Medellín, Febrero de 2012

TABLA DE CONTENIDO

GLOSARIO DE TERMINOS	2
RESUMEN.....	9
ABSTRACT	11
INTRODUCCIÓN.....	13
1. INFORMACIÓN GENERAL	15
1.1 ANTECEDENTES	15
1.1.1 Los protocolos y estándares del manejo y la evidencia digital	16
1.2 JUSTIFICACIÓN	21
1.3 OBJETIVOS.....	23
1.3.1 Objetivo General	23
1.3.2 Objetivos Específicos	23
1.4 DESCRIPCIÓN DEL PROBLEMA	24
2. REFERENCIA TEÓRICA.....	27
2.1 Incidente de seguridad informática.....	28
2.1.1 Consideraciones Generales política de gestión de incidentes	29
2.1.1 Responsabilidades.....	30
2.1.2 Clasificación de los incidentes.....	32
2.1.3 Procesos de planificación de incidentes	35
2.1.4 Prevención del incidente.....	37
2.2 ANÁLISIS FORENSE.....	45
2.2.1 Procedimiento para la recolección de la evidencia	47
2.2.2 Desarrollo de plan de adquisición:	49
2.2.3 Adquisición de datos	50
2.3 PROTOCOLO FORENSE	54
2.3.1 Fases básicas	55
2.3.2 Uso de herramientas Forenses	58
3. METODOLOGÍA	63
4. CONCLUSIONES Y RECOMENDACIONES	64
5. BIBLIOGRAFÍA	66

GLOSARIO DE TERMINOS

Se hace importante la descripción de estos términos dado que no son conceptos muy conocidos y por tal razón se hace necesario su descripción para la mayor comprensión de este proyecto.

AMENAZAS: las amenazas son agentes capaces de explotar los fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa, afectando el negocio. (Academia Latinoamericana de Seguridad Informática, 2011)

ATAQUE: es la materialización de una amenaza: acción que puede violar los sistemas y mecanismos de seguridad de un sistema de información. Puede ser pasivos (únicamente se leen los datos transmitidos, sin modificarlos). (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

ANÁLISIS FORENSE INFORMÁTICO: Se denomina análisis forense informático al proceso resultante de aplicar métodos científicos de los sistemas informáticos con la finalidad de asegurar, identificar ,preservar analizar y presentar la evidencia, de manera que esta sea aceptada en un proceso judicial. (Jordi Serra, 2009)

CADENA DE CUSTODIA: La cadena de custodia es el conjunto de pasos o

Procedimientos seguidos para preservar la prueba digital que permita convertirla y usarla como evidencia digital en un proceso judicial. (AGESIC, 2010)

CONFIDENCIALIDAD DE INFORMACION ELECTRÓNICA: se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente e en la comunicación de los datos. (Academia Latinoamericana de Seguridad Informática, 2011)

CIENCIA FORENSE: La aplicación de prácticas científicas dentro de un proceso legal, la ciencia forense abarca tanto la rama civil como la penal del derecho.

CONTROL DE ACCESO: servicio de seguridad que previene el uso no autorizado de un recurso. El control se realiza limitando el acceso a recursos físicos o de información mediante una tabla de acceso, que describe las acciones y recursos permisibles a cada usuario. (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

DISPONIBILIDAD: servicio de seguridad que garantiza que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada. (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

ESTENOGRAFÍA: es la disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que

no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible a través de portador, para que pueda pasar desapercibida. (Jordi Serra, 2009)

EVIDENCIA: Cualquier elemento que proporcione información de la que se puede inferir alguna conclusión, o bien constituya un hallazgo relacionado con un hecho que se investiga. (Jordi Serra, 2009)

FORENSE: Tareas propias asociadas con la evidencia digital, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso. (Jordi Serra, 2009)

HACKER: se llama hacker a una persona habilidosa con los ordenadores que trata de sobrepasar las barreras de seguridad informática establecidas por empresas y organizaciones. Un hacker puede tener distintos objetivos: robar datos, solo curiosear, hacer daño (por ejemplo borrando datos), enriquecerse, chantajear, demostrar su capacidad o simplemente hacerse el gracioso. (KRALL, 2011)

INFORMACIÓN: según Idalberto Chiavenato, información "es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de

reducir el margen de incertidumbre con respecto a nuestras decisiones" (Ciberculturahoy, 2011)

INTEGRIDAD: servicio de seguridad que garantiza que los datos no han sido alterados o destruidos de modo no autorizado. Cuando se aplica sobre ficheros, son técnicas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus). (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares. (ISO27000, 2009)

JURISPRUDENCIA: se entiende por jurisprudencia a los informes dictados por los órganos jurisdiccionales del estado. Esto significa que para conocer el contenido completo de las normas vigentes, hay que considerar cómo han sido aplicadas en el pasado. En otras palabras, la jurisprudencia es el conjunto de sentencias que han resuelto casos iguales o similares de la misma manera o en el mismo sentido. (UNAM Instituto de Investigaciones Jurídicas, s.f)

realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos. (BORGHELLO, 2009)

MALWARE: El malware es un término general que se le da a todo aquel software que perjudica a la computadora. La palabra malware proviene del término en inglés malicious software, y en español es conocido con el nombre de código malicioso. (UNAM)

NORMAS: Acuerdos documentados que contienen especificaciones técnicas o criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, asegurando de esta forma que los materiales, productos, procesos y servicios son apropiados para lograr el fin para el que se concibieron. (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

PHISHING: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. (Seguridad PC, s.f)

PROCEDIMIENTO: un procedimiento es el modo de ejecutar determinadas acciones que suelen realizarse de la misma forma, con una serie común de pasos claramente definidos,

que permiten realizar una ocupación, trabajo, investigación, o estudio, se puede aplicar a cualquier empresa. (Universidad Complutense Madrid, 1997)

PROTOCOLO FORENSE: El proceso forense, el apoyo pericial y las herramientas forenses informáticas garantizan que la identificación, obtención y análisis forense no alterará la evidencia, permitiendo a la empresa poder avanzar en la identificación del crimen informático y ubicar responsables, permitiendo dar inicio a la formalización legal de los hechos a través de denuncia o querrela en lo Penal, Civil o Laboral, con la certeza que la evidencia permanece inalterable y con el apoyo de un informe forense informático que avala en una exposición y análisis técnico los dichos legales conforme a derecho. (L., 2008)

RIESGOS: Es la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: la confidencialidad, la integridad y la disponibilidad de la información. (Academia Latinoamericana de Seguridad Informática, 2011)

SALVAGUARDA: Mecanismo capaz de reducir el riesgo. (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

SEGURIDAD: se puede entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. (TUXTENO, 2011)

SEGURIDAD DE LA INFORMACIÓN: la seguridad de la información es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recurso humano integrado para proveer toda la protección debida y requerida a la información y a los recursos informáticos de una empresa, institución o agencia gubernamental (RUBIO, 2005)

VISHING: el término "vishing" significa "phishing de voz", o sea una clase de estafas realizadas a partir de llamadas telefónicas. (Seguridad PC, s.f)

VULNERABILIDAD: fallos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar. Estos errores de programación y/o diseño permiten que un tercero se aproveche de ellos para realizar acciones tales como ataques, intrusiones o cualquier otro uso indebido. (Centro Tecnológico de Telecomunicaciones De Catalunya, 2011)

RESUMEN

Las organizaciones se enfrentan a diferentes ataques a la información como el robo de datos, fraudes y estafas, siendo estos cada vez novedosos y difíciles de detectar.

Cuando las organizaciones han sido víctimas de un incidente informático, es importante para la demostración del hecho, que exista una evidencia digital, obtenida bajo protocolos forenses digitales, y a su vez que la persona ejecutora del protocolo sea un experto forense digital (sea o no certificado por una entidad certificadora), el cual pueda emitir un informe forense donde pueda indicar:

Su concepto pericial, la pertinencia y validez del protocolo aplicado, e indique su experiencia profesional (por certificación de estudios) y/o su experiencia empírica (por certificación de casos exitosos), con la finalidad de otorgarle un elemento material probatorio para su presentación en juicio en la etapa de control de garantía y finalmente pueda obtener una prueba digital para la demostración de tipo probatoria sobre la ocurrencia del incidente informático, con la indicación del posible sujeto activo de la conducta.

Los protocolos forenses digitales aplicables para la obtención de una evidencia digital 1, se cuentan con estándares internacionales de carácter privado y público y a su vez de uso exclusivo por los gobiernos y otros de uso para cualquier persona.

En Colombia no existe protocolo forense digital, a su vez se acogen protocolos internacionales reconocidos y certificados como los de SANS y NIST, sin embargo en Colombia existen normas que permiten la aplicación adecuada de éstos protocolos para la obtención de la evidencia digitales.

En el ordenamiento jurídico colombiano se encuentran varias regulaciones que permiten dar aplicación en conjunto con la finalidad de dar protección a la información, así: constitución política 1991 art. 15 y 20, código penal art. 269 A al 269i o ley 1273 de 2009, La ley 527 de 1999, decreto reglamentario 1747 de 2000, ley 1266 del 2008 habeas data, además de todas las disposiciones emitidas por las diferentes superintendencias que exigen el cumplimiento de seguridad y preservación de la información.

ABSTRACT

The organizations face different attacks on the information such as data theft, fraud and scams, these being each novel and difficult to detect. Where organizations have been victims of a computer incident, it is important for the demonstration of the fact, that there is a digital evidence obtained under digital forensic protocols, and in turn that the person executing the protocol is a forensic expert digital (whether or not certified by a certifying entity), which can issue a forensic report where you can indicate:

His expert concept, the relevance and validity of the applied Protocol, and indicate your professional experience (for certification) and/or its empirical experience (for certification of successful cases), with the purpose of providing an evidentiary material element for presentation at trial in the stage of guarantee control and can finally obtain a digital test for demonstration of evidentiary type on the occurrence of the computer incident, with an indication of the possible active subject of the conduct.

The applicable digital forensic protocols for obtaining digital evidence, have international standards of private and public character and in turn for exclusive use by Governments and others use to anyone.

In Colombia there is no digital forensic Protocol, in turn benefiting international protocols recognized and certified as SANS and NIST, however there are rules to enable the proper implementation of these digital protocols for obtaining evidence in Colombia.

In the system legal Colombian are several regulations that allow implementation in conjunction with the purpose of giving protection to information, thus: Constitution 1991 arts. 15 and 20, penal code art. 269 to the 269i or 1273 law of 2009, law 527 of 1999, regulatory decree 1747 of 2000, law 1266 of 2008 habeas data, as well as all the provisions issued by the different superintendence's requiring compliance with security and preservation of the information.

INTRODUCCIÓN

El trabajo de análisis forense, permite explorar el tratamiento y el manejo de la evidencia digital de carácter probatorio información cuando se presume la comisión de delito informático existe un delito informático.

Para este análisis, es necesario un estudio de los elementos que toda prueba digital debe tener : autenticidad , integridad, originalidad ,confidencialidad y no repudio que son de importancia evaluar para que la evidencia se mantenga elemento material probatorio y que esta pueda ser llevada a un juicio para determinar o considerar que se presentó una violación a una política de seguridad de la información, en las organizaciones puede ser necesario afrontar una serie de contratiempos relacionados con la violación al sistema, que pone en peligro el buen nombre de una organización.

Además, teniendo en cuenta que la organización tiene en sus manos la fiabilidad de los datos, sean de terceros o de la organización y que deben propender por la conservación, es necesario que establezcan planes administrativos, políticas de seguridad y reglamentación de sus procesos a través de mecanismos confiables y de fácil manejo y que existan protocolos para el manejo de la información.,

El objetivo es plasmar la situación legal de la informática en las organizaciones , junto con el manejo que se le debe dar a la información cuando esta ha sido vulnerada y se han violado los parámetros de accesos de la información a la comprensión de lo que está permitido y contemplado en la legislación Colombiana, lo que se puede y no se puede hacer, lo que es delito informático y lo que no, lo vulnerables de nuestros sistemas de información, que debemos proteger y las formas en que debemos actuar en cualquiera de estas situaciones.

1. INFORMACIÓN GENERAL

1.1 ANTECEDENTES

Las ciencias forenses tienen por objeto la aplicación de prácticas científicas dentro de un proceso legal, la información es un valor en sí mismo y por tanto un objeto codiciado por los nuevos delincuentes y una vía para provocar cuantiosos daños a la organización. (Jordi Serra, 2009). [1]

Con el advenimiento de nuevas tecnologías como Internet, se ha vuelto necesario evolucionar este principio para un mundo completamente virtualizado, dado que gracias a la naturaleza intangible del software y de la dificultad que presentaría bajar al nivel de granularidad para encontrar evidencia a nivel atómico y molecular, se requiere el desarrollo e implementación de mecanismos que permitan registrar eventos en instantes de tiempo particulares, donde se genere evidencia de transacciones, movimientos o acciones en general dentro de un sistema informático, abarcando no solo esquemas de almacenamiento y procesamiento sino también las redes telemáticas por las cuales fluyen los datos de manera electrónica. A lo largo de la historia de las redes teleinformáticas y más concretamente, de Internet se ha hecho evidente la carencia de mecanismos que permitan encontrar evidencia acerca de incidentes de seguridad informática, lo cual ha hecho que varios frentes criminales como el narcotráfico hayan tomado como lugar favorito la frontera digital **Fuente especificada no válida..** [2]

Para disminuir los niveles de impunidad y hacer justicia a partir de evidencia en un lugar que por naturaleza no deja evidencia, se han desarrollado un conjunto de mecanismos tanto técnicos como legales para extraer información en la escena del crimen o siniestro informático, dando lugar a protocolos de tratamiento de información que permitirán esclarecer los hechos. A continuación se muestran los protocolos y normas más encontrados, los cuales, presumiblemente son los más utilizados a nivel mundial y que servirán como alimentación principal para el buen término de la investigación.

1.1.1 Los protocolos y estándares del manejo y la evidencia digital

1.1.1.1 Computer Security Incident Handling Guide

Este documento contiene las recomendaciones del instituto nacional de estándares y tecnología norteamericano. Este es uno de los estándares más completos a nivel mundial acerca de manejo de incidentes y recolección de información en un incidente **Fuente especificada no válida.**[3]

1.1.1.2 RFC 3227: Guidelines for Evidence Collection and Archiving

Este Request For Comments (RFC) consiste en establecer los principios durante la recolección de evidencia, el procedimiento de recolección, la cadena de custodia y algunas referencias a herramientas (Brezinski, 2002).[4]

1.1.1.3 Electronic Crime Scene Investigation: A Guide for First Responders

Es una Guía del Departamento de Justicia Norteamericano, y de la oficina de programas de justicia, en el cual se define cual deberá ser los procedimientos para los equipos de respuesta a incidentes. Dentro de los elementos que trata están: Dispositivos electrónicos, Equipos y herramientas para la investigación, Aseguramiento y evaluación de una escena, Documentación de una escena, recolección de evidencia, empaquetado, transporte y almacenamiento, Examen forense por categoría del crimen. **Fuente especificada no válida.**[5]

1.1.1.4 Searching And Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

Este documento del Departamento de Justicia norteamericano pretende ser usado por fiscales federales para propósitos de entrenamiento y ejecución. Comprende un conjunto de leyes de delitos informáticos, espionaje y otros crímenes relacionados con tecnología. Consiste en la búsqueda y aprovechamiento de la información en un computador con o sin una orden judicial. También trata los asuntos legales acerca de la vigilancia en redes de comunicaciones y el tratamiento de evidencia digital. **Fuente especificada no válida.**[6]

1.1.1.5 RFC 2350: Expectations for Computer Security Incident Response

Este documento especifica las actuales mejores prácticas para la comunidad de Internet en cuanto a las expectativas frente a los equipos de respuesta a incidentes. Posiblemente no se defina todos los requisitos apropiados para cualquier tipo de equipo. **Fuente especificada no válida.**[7]

1.1.1.6 Prosecuting Computer Crimes

Este documento del Departamento de Justicia norteamericano pretende ser usado por fiscales federales para propósitos de entrenamiento y ejecución. Comprende un conjunto de leyes de delitos informáticos, espionaje y otros crímenes relacionados con tecnología. En los apéndices incluye las mejores prácticas para respuesta a incidentes, reporte de incidentes y recursos para crímenes en redes telemáticas. **Fuente especificada no válida.**[8]

1.1.1.7 Computer Forensics: Digital Forensic Analysis Methodology

Este artículo del departamento de justicia norteamericano, ofrece una metodología clara en cuanto al manejo de evidencia digital. Dicha metodología comprende los siguientes ítems: Preparación/Extracción, Identificación y Análisis. **Fuente especificada no válida.**[9]

1.1.1.8 Perfil sobre los Delitos informáticos en el Ecuador

Este documento es una guía para la VI Reunión del Grupo de Trabajo en Delito Cibernético de la REMJA, que se realizará el 21 y 22 de Enero del 2010 en Washington D.C. **Fuente especificada no válida.** En el contenido del documento se puede encontrar los tipos de delitos informáticos existentes en la legislación ecuatoriana, el Manual de manejo de evidencias digitales y entornos informáticos, principios básicos en otros.

1.1.1.9 Medios de Prueba Electrónicos: Estado de avance en la legislación Argentina

Esta ponencia analiza las distintas normas procesales en lo referente al grado de aceptación que presentan respecto del uso de medios electrónicos en Argentina, tanto para la gestión diaria de la administración de Justicia y funcionamiento interno de los tribunales, como para el diligenciamiento de notificaciones, así como también para el tratamiento de los medios de prueba digitales. **Fuente especificada no válida.**[10]

1.1.1.10 HB 171—2003 Guidelines for the Management of IT Evidence

Este manual, es el estándar australiano para el manejo de evidencia digital, establecido en el año 2003. Es un documento de referencia y en ningún momento se espera que el cumplimiento con estas recomendaciones sean suficientes para la admisibilidad evidencia electrónica **Fuente especificada no válida.**, solo es un enunciado de las mejores prácticas. Los temas principales que incluye son: Principios para el manejo de evidencia de TI, Ciclo de vida de la gestión de evidencia de TI.

1.1.1.11 Manual de Manejo de Evidencias Digitales y Entornos Informáticos

Este manual ecuatoriano define el procedimiento de operaciones estándar para la recolección de evidencia digital, cual es son los principios básicos y principios de peritaje, que aparatos electrónicos y herramientas se deben tener y como rastrear correo electrónico

Fuente especificada no válida..[11]

1.1.1.12 Manual Único de Procedimientos para Cadena de Custodia

Este manual creado por la Fiscalía General de la Nación en Colombia establece los procedimientos para el manejo de evidencia general en un caso de investigación criminal. Sin embargo, no se especifica cual es el manejo particular a evidencia digital o electrónica

Fuente especificada no válida..[12]

1.1.1.13 Manual Único de Policía Judicial

Este manual establece las funciones correspondientes a la Policía Judicial en Colombia, cuales son los organismos adjuntos a esta y cuales son los procedimientos que deben seguir en un caso de investigación criminal. En este documento se considera únicamente la evidencia digital en el caso de navegación en Internet, dejando por fuera elementos críticos como los de comunicaciones y almacenamiento **Fuente especificada no válida..[13]**

Después de haber encontrado los estándares y procedimientos más utilizados tanto a nivel nacional como internacional, es necesario analizar cuáles de estos procedimientos se adaptan adecuadamente al conjunto de principios de la ley Colombiana para el tratamiento de evidencia digital.

1.2 JUSTIFICACIÓN

Se plantea para el desarrollo del trabajo de grado la realización de un objetivo específico que permita dar parte de la solución en el desarrollo e investigación del objetivo general del proyecto, la elección del objetivo específico fue dado bajo la pertinencia temática, en correlación con el tiempo para su realización y el cumplimiento de los fines del curso.

La temática planteada en el objetivo específico permite hacer un análisis a los protocolos forenses como medios de investigación científica forense que permiten involucrar el trabajo de las ciencias forenses en la investigación de incidentes informáticos, permitiendo la recolección de evidencia digital que a su vez revele la existencia o no de una vulneración a sistema informático y si ésta a su vez permite o no el fundamento para probar la existencia de un delito informático, en los términos de la ley 1273 de 2009.

El 15 de mayo de 2005 se emitió la nueva versión internacional de la norma ISO/IEC 17025 la cual fue aprobada y adoptada como norma técnica colombiana por el Instituto Colombiano de Normas Técnicas ICONTEC el 26 de octubre de 2005, y cuya versión sustituye y anula la NTC ISO/IEC 17025:2001.

En el año 2008 la comunidad científica en materia de ciencias forenses decreto los laboratorios forenses y el procesamiento forense digital como una disciplina de las ciencias forenses, lo cual permite fortalecer la validez de los diferentes protocolos existentes a nivel mundial del campo público (estos desarrollados por instituciones privadas del campo académico e investigativo) y del campo privado (desarrollados por entidades estatales a

través de sus dependencias encaradas y/o de instituciones educativas con dedicación exclusiva a los estados).

1.3 OBJETIVOS

Para el desarrollo investigativo que se presenta en esta investigación, se ha elegido un objetivo específico, que permita, en un futuro, en articulación con los otros objetivos, dar respuesta y solución complementaria al objetivo general, sin embargo, para las competencias que se obtienen con el estudio de formación posgraduada, el objetivo específico indicado a continuación, es el mas pertinente, así:

1.3.1 Objetivo General

Definir el protocolo de análisis Forense y como se aplica de acuerdo a las normas y regulaciones para determinar la evidencia digital dado un incidente informático.

1.3.2 Objetivos Específicos

- Protocolos del Análisis Forense digital como herramienta para preservar la evidencia digital respecto de un incidente informático.

1.4 DESCRIPCIÓN DEL PROBLEMA

En Colombia el estatuto penal ley 906 de 2004 y la legislación complementaria no regula en específico la ciencia forense digital, en consecuencia existe el principio de libertad probatoria art. 272 del mismo estatuto, con el cual se fundamenta que toda investigación forense debe ser dada bajo parámetros rigurosos y garantizando tres aspectos fundamentales: el protocolo exista y haya tenido aplicabilidad en casos similares en especial sea un protocolo reconocido a nivel internacional por alguna entidad sea pública o privada; segundo que el perito se encuentre certificado o en su defecto que demuestre la experiencia en la ciencia forense informática a través de la solución de casos, esto única y exclusivamente en materia del campo privado, pues en el campo público todo investigador adscrito a una unidad de delitos informáticos es obligatorio que se encuentre certificado para la labor forense que vaya realizar y tercero, que el laboratorio forense en el que se encuentre realizada la investigación y obtención de la prueba digital cumpla con los parámetros establecidos para todo laboratorio forense, tal y como lo indica la norma ISO 17025.

Los sistemas informáticos han brindado alternativas que anteriormente se veían como un sueño, igualmente estas alternativas en conexiones de red externas e internas, se exponen a peligros potenciales con respecto a la vulnerabilidad de la información. No hay conciencia que los malos hábitos en seguridad de acceso, publicación de documentos, uso del correo electrónico entre otros, adicional al desconocimiento sobre el valor de la

información que se maneja, pueden traer consecuencias graves tales como la pérdidas de información o peor aún, llegar a las manos menos indicadas.

Para las organizaciones colombianas, debería implementar estándares de seguridad para el manejo de la información, que les provea tranquilidad para afrontar los retos que presenta la visión actual de los negocios, la tecnología y el comercio. Es por ello que deben buscar obtener los mejores elementos de seguridad legal, física y tecnológica para ser competitivos y crecer como organizaciones.

El problema no es solo técnico y tecnológico, los mecanismos de concientización cultural, relacional y comprensivo, de procesos y de control que permitan fortalecer el acceso, manejo y utilización con relación a la información; la solución no está solo en lo económico está en la atención y desarrollo de las actividades de seguridad.

El problema de la seguridad de la información en las empresas tiene en esencia dos matices, el primero el tecnológico y el segundo el organizacional.

Cualquier organización que se plantee la implantación de alguna medida de seguridad en sus sistemas de información (ya sea de carácter tecnológico u organizativo), deberá pretender alcanzar objetivo tales como: evitar los incidentes de seguridad y reducir las consecuencias de los que no puedan evitar.

Lo adecuado es que las organizaciones se planteen cómo actuar ante un incidente, dado que a través de la gestión de los incidentes permite a las organizaciones estructurar un

protocolo de actuación ante una incidencia para minimizar su impacto y el tiempo y el tiempo de resolución. (Huguet, 2009)[14]

2. REFERENCIA TEÓRICA

La actividad diaria de una organización, está fuertemente basada en los sistemas informáticos, el valor de los datos almacenados en estos sistemas es cada vez más importantes, convirtiéndose en los que se denomina “Activos Informáticos”, el crecimiento de las redes en los sistemas informáticos y las interconexiones de estas. Se ha creado entonces un nuevo reto para los administradores de sistemas, la prevención, el control y la respuesta a incidentes de seguridad en las redes de las organizaciones.

Sin embargo, muchos de los incidentes son intencionados y provocan daños de distinta índole. Una gestión como den eficaz de los incidentes, así como de su resolución, permitirá un rápido regreso a la normalidad, a la par que una recolección de evidencias digitales con valor probatorio ante un tribunal. (Huguet, 2009)[14]

2.1 Incidente de seguridad informática

Un incidente de seguridad informática es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita.

También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).

Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática. [NIST800-61, ISO 18044]. (AGESIC, 2010).[15]

Como ejemplos de incidentes de seguridad podemos enumerar:

- Acceso no autorizado
- Robo de contraseñas
- Robo de información
- Denegación de servicio

✓ **Incidentes de Denegación de Servicios (DoS):** Son un tipo de incidentes cuya finalidad es obstaculizar, dañar o impedir el acceso a redes, sistemas o aplicaciones mediante el agota-miento de sus recursos. (AGESIC, 2010)[15]

- ✓ **Incidentes de código malicioso:** Cualquier tipo de código ya sea, virus, gusano, “caballo de Troya”, que pueda ejecutarse en un sistema e infectarlo. (AGESIC, 2010). [15]

- ✓ **Incidentes de acceso no autorizado:** Se produce cuando un usuario o aplicación accede, por medio de hardware o software, sin los permisos adecuados a un sistema, a una red, a una aplicación o los datos. (AGESIC, 2010). [15]

- ✓ **Incidentes por uso inapropiado:** Se dan cuando los usuarios se “saltan” la política de uso apropiado de las sistemas (por ejemplo ejecutando aplicaciones P2P en la red interna de la organización para la descarga de música). (AGESIC, 2010). [15]

- ✓ **Incidente múltiple:** Se produce cuando el incidente implica varios de los tipos anteriores. (AGESIC, 2010). [15]

2.1.1 Consideraciones Generales política de gestión de incidentes

La gestión de estos incidentes se puede definir como un conjunto de acciones y procesos que brindan a las organizaciones fortalezas y capacidades para dar respuesta de forma adecuada al incidente de seguridad informática.

La política de gestión de incidentes de seguridad de la información está dirigida a toda persona que tenga legítimo acceso a los sistemas informáticos de la organización, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

Tanto la Dirección como el personal de toda la Organización tienen responsabilidades. (AGESIC, 2010). [15]

2.1.1 Responsabilidades

De la Dirección:

- ✓ Disponer los recursos necesarios a fin de brindar una apropiada gestión de los incidentes de seguridad de la información, mediante la designación de un equipo responsable por la gestión de incidentes de seguridad de la información.

- ✓ Difundir la presente política a todo el personal del Organización, independiente del cargo que desempeñe y de su situación contractual.

Del personal

- ✓ Dar cumplimiento a la presente política, independiente del cargo que desempeñe y de su situación contractual.

- ✓ Reportar los eventos de seguridad que detecte al equipo responsable de gestión de incidentes de seguridad de la información, siguiendo los procedimientos operativos establecidos para tal fin.

Es muy importante que la dirección de la Organización reconozca el valor significativo de gestionar los incidentes de seguridad de la información y que se declare el cumplimiento con la normativa y legislación vigente con aspectos de gestión de incidentes de seguridad de la información.

Esta Política de Gestión de Incidentes de Seguridad de la Información se integrará a la normativa básica de la Organización, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a esta.

Es política de la Organización:

- ✓ Adoptar medidas de seguridad eficientes para proteger sus activos de información críticos.
- ✓ Analizar los eventos de seguridad informática para determinar si se trata de un incidente de seguridad de la información.
- ✓ Ejecutar procedimientos de repuesta a incidentes para contener y mitigar el incidente.
- ✓ Documentar y clasificar los incidentes

- ✓ Responder por la integridad de la información generada o en su poder.
- ✓ Aprender de los incidentes de seguridad de la información, para prevenir nuevas ocurrencias.
- ✓ Reparar las consecuencias de los incidentes de seguridad de la información.
- ✓ Empezar actividades pos incidente, como ser mejoras a los procesos operativos de gestión de incidentes de seguridad de la información o asegurar la retención de evidencias. (AGESIC, 2010). [15]

2.1.2 Clasificación de los incidentes

El esquema de clasificación de incidentes de seguridad, deberá estar definido por las políticas de gestión de incidentes, esto permitirá tener estadísticas a mediano y largo plazo, a tener planes de contingencia y a la toma de decisiones.

Dentro de la clasificación es importante contemplar los siguientes aspectos de incidentes:

Tipo: en este se clasifica el incidente en categorías funcionales como:

- ✓ Acceso no autorizado a sistemas
- ✓ Denegación de servicios

✓ Divulgación de información sensible

✓ Infección del Malware

Severidad: En este se clasifica el impacto real o potencial del incidente, dependiente del caso se podrá clasificar en escalas monetarias o en escala de impacto de servicios como: alta, media, baja. (AGESIC, 2010). [15]

Existen multitud de ataques distintos, y por ello resulta muy importante poder clasificarlos de alguna manera, estos se pueden agrupar según el modo de actuar, así como en función de quien lo origina.

Según cómo actúa: Los ataques que pueden sufrir el Hardware y software y de una manera muy especial los datos, se clasifican en cuatro grandes grupos

- Interrupción: Este ataque es contra la disponibilidad en el cual se destruye o queda no disponible el recurso del sistema, un ejemplo de esta es un ataque de denegación de servicio. (Huguet, 2009)
- Intercepción: Ataque contra la **confidencialidad**, en el cual un elemento no autorizado consigue el acceso a un recurso, en este tipo de ataque, no se refiere únicamente a posibles usuarios que actúen como espías entre emisor y receptor. (Huguet, 2009)[14]

- **Modificación:** Ataque contra la **integridad** en el que, además de conseguir en acceso no autorizado a un recurso, también se consigue modificarlos, borrarlos o alterarlo de cualquier manera, los ataques hechos por los intrusos, por ejemplo los borrados de bases de datos, alteración a páginas web. (Huguet, 2009)[14]
- **Fabricación:** Ataque contra la **Integridad** en la que el elemento consigue crear o insertar objetos falsificados en el sistema. Por ejemplo añadir, de una manera no autorizada un nuevo usuario y la contraseña. (Huguet, 2009)[14]

Según quien lo origina: Pueden ser una o varias personas las que, con diferentes objetivos, originan un ataque a un sistema informático con el fin de intentar acceder a la información confidencial, destruirla o simplemente conseguir el control absoluto del sistema atacado. Conocer los objetivos de los atacantes y sus motivaciones resulta, pues, esencial para prevenir y detectar las acciones. (Huguet, 2009)[14]

Los ataques provenientes de personas se pueden clasificar en dos grandes grupos:

- **Ataques pasivos :** El atacante no destruye ni modifica ningún recurso del sistema informático, simplemente lo observa, normalmente con la finalidad de obtener alguna información confidencial, a menudo este tipo de ataque se produce sobre la información que viaja por la red
- **Ataques activos:** El atacante altera o destruye algún recurso del sistema, algunos ejemplos de ataques activos son: suplantación de identidad, restauración decir que uno o varios mensajes legítimos son interceptados y reenviados diferentes veces

para producir un efecto no deseado, degradación fraudulenta de un servicio, se trata cuando el espía evita el funcionamiento normal del sistema, por ejemplo eliminar los mensajes que se dirigen a un usuario determinado, Modificación del mensaje, se modifica una parte del mensaje interceptado y se reenvía la persona a la cual iba dirigido originalmente.

2.1.3 Procesos de planificación de incidentes

El proceso de planificación de incidentes, deberá incluir todas las actividades de tipo proactivo para estar más preparados, responder y enfrentar incidentes de seguridad. Dichas actividades deben contener

- ✓ Análisis de alertas y amenazas

- ✓ Actividades de sensibilidad

- ✓ Actividades de entrenamiento

- ✓ Ensayos y evaluaciones de seguridad.

- ✓ Definición de procedimientos

- ✓ Análisis y mejora continuo del proceso

En el proceso de atención de incidentes, se deben agrupar todas las actividades de respuesta de tipo reactivo

- ✓ Recepción de reportes de incidentes
- ✓ Clasificación y valoración de impacto
- ✓ Relevamiento de sistemas y procesos de negocio afectados así como sus responsables
- ✓ Elaboración de un plan de respuesta al incidente con medidas de contención y mitigación recomendadas.
- ✓ Obtención de avales para ejecución del plan de respuesta, si este lo requiere
- ✓ Ejecución de las medidas de contención y mitigación
- ✓ Elaboración de un informe final de cierre

(AGESIC, 2010)[15]

2.1.4 Prevención del incidente

Detectar un ataque a los sistemas informáticos antes de que se produzca, o en el peor de los casos en el instante en el que comienza, siempre será mejor que tener que recuperar el sistema recurriendo a sus copias de seguridad. (AGESIC, 2010)[15]

Existe múltiple información sobre cómo asegurar los sistemas en las organizaciones comerciales, en este proyecto se expondrá de forma breve algunas recomendaciones para asegurar los sistemas, redes, aplicaciones y datos.

- ✓ Disponer de una correcta gestión de parches y actualizaciones de su hardware y software, ya que gran parte de los ataques se basan en explotar un número reducido de vulnerabilidades en sistemas y aplicaciones.

- ✓ Asegurar los servidores basándose en el concepto de privilegio mínimo, esto es, configurarlos para que proporcionen un número limitado de servicios y con un nivel de acceso restringido según el tipo de usuario. Además deben evitarse configuraciones por defecto, como claves predefinidas, recursos compartidos, etc. También sería interesante disponer de medios de notificación al administrador cuando se produzcan accesos a niveles de privilegio no autorizados. (AGESIC, 2010).[15]

- ✓ Mantener la seguridad de la red, configurando un filtro perimetral en modo “paranoico”, esto es, denegando cualquier tipo de acceso no autorizado expresamente, y manteniendo sólo el tráfico necesario para la actividad diaria normal. Esto incluirá instalación de cortafuegos, detectores de intrusos (IDS), monitores de red, uso de redes privadas virtuales (VPNs), uso de protocolos seguros (IPSec, SSL). (AGESIC, 2010). [15]

- ✓ Prevenir la ejecución de código malicioso (malware), utilizando programas antivirus capaces de parar este tipo de código como virus, caballos de Troya, gusanos y además “especies”. (AGESIC, 2010). [15]

- ✓ Formar e informar a los usuarios de las organizaciones para que conozcan, acepten y sean capaces de aplicar las directrices de su política de seguridad. Hacerles saber hechos ocurridos en otras organizaciones o entidades, cómo han “aprendido la lección”, cómo ha afectado un incidente a sus actividades (y a sus sueldos). Informando y formando a los usuarios reducirá la frecuencia de los incidentes, sobre todo aquellos que impliquen la ejecución de código malicioso, o el saltarse la política de uso adecuado de los sistemas. (AGESIC, 2010). [15]

Es importante que las organizaciones incluyan dentro de su política de seguridad un Plan de Respuesta ante Incidentes. Estos planes dependen en gran medida de las características y

políticas de las organizaciones, y dentro de los cuales es importante que contengan los siguientes puntos:

Backup: Una buena política de copias de seguridad es la clave para tener segura la información de la organización, algunos motivos para hacer copias de seguridad son los siguientes:

- Proteger la información contra el fallo del sistema o algún desastre natural
- Proteger la información de los usuarios contra los borrados accidentales
- Proteger la información de los usuarios y de la organización, contra ataques por parte de terceros
- Duplicar la información de los usuarios por seguridad, dado que se pueden dar casos de uso incorrecto que la dejen inconsistente o la modifiquen incorrectamente.
- Posibilidad de un traspaso de la información cuando se utiliza o reinstala el sistema.

La estrategia de cómo hacer las copias de seguridad es crítica para asegurar que se haga todo correctamente y que se pueda restaurar la información cuando se requiera.

(Huguet, 2009)[14]

Monitorización de la Red: Es un elemento clave para asegurar que no se presente una incidencia de seguridad. Así el control de red puede darnos las primeras indicaciones de actividades anómalas. Las siguientes indicaciones permiten monitorizar la red y pueden ayudar a detectar un incidente, algunos de estos mecanismos pueden automatizarse con scripts y software. (Huguet, 2009). [14]

- Documentar la actividad normal de un sistema o red. De este modo, se detectan anomalías con mayor facilidad.
- Centralizar registros de un sistema de detención de intrusión, facilitan el estudio de incidentes y por tanto su detención.
- Correlacionar eventos, a partir de los registros, para poder ser centralizados.
- Utilizar Sniffers para obtener información que permita detectar anomalías en el tráfico de red.
- Mantenerse al día en materia de seguridad, esto se puede llevar a cabo mediante suscripciones a listas de correo, visitas regulares a portales de seguridad, participación en foros entre otros. (Huguet, 2009). [14]

Creación de un equipo de respuesta a incidentes: el hecho de reunir un equipo, antes de que se produzca cualquier incidente, es muy importante para la organización, e influirá positivamente en la manera de tratar el incidente, los miembros del equipo deben tener definidas claramente sus tareas, para asegurar que no quede ningún área de la respuesta sin cubrir. Deberían tener la formación y responsabilidades para acometer los incidentes que ocurran.

Para determinar una estructura ideal, depende el tipo de la organización y de la estrategia de administración de riesgo que esta tenga establecida, no obstante la CSIRT (computer security incident response team), el equipo principalmente esta compuesto por profesionales responsables de coordinar una respuesta ante cualquier incidente, el número

de miembros del CSIRT, dependerá del tamaño y la complejidad de la organización, pero debe asegurarse que cuente con los suficientes miembros para cubrir adecuadamente todas las tareas de equipo en cualquier momento. El equipo realizara las siguientes tareas:

- Supervisar el sistema en búsqueda de infracciones de seguridad
- Servir como punto central de comunicación, tanto para recibir los informes de incidentes de seguridad como ara difundir la información esencial de los incidentes y sobre las entidades correspondientes.
- Documentar y catalogar los incidentes de seguridad
- Aumentar el nivel de conciencia sobre la seguridad dentro de la compañía
- Posibilitar la auditoria de sistemas y redes mediante procesos de evaluación de vulnerabilidades y pruebas de penetración
- Investigar acerca de nuevas versiones de software
- Analizar y desarrollar nuevas tecnologías para minimizar el riesgo
- Ofrecer servicios de consultoría en seguridad. (Huguet, 2009)[14]

Para la preparación del equipo se deben seguir unas pautas mínimas como:

- Formación en el uso adecuado y la ubicación e las herramientas de seguridad critica, además de aprovisionar los recursos físicos para mejor aprovechamiento del tiempo.
- Reunir toda la información de comunicación pertinente, contar con toda la información del equipo de trabajo , detalles de Informacion de proveedor, asesoría

legal para contactar con las autoridades locales pertinentes antes de que se produzca el incidente.

- Establecer toda la Información del sistema de emergencia en la ubicación central y sin conexión, como carpetas físicas o equipos sin conexión, esta Información de emergencia incluye: contraseñas de los sistemas, direccionamiento IP, Información sobre configuraciones de router, firewall, copias de las claves de las entidades emisoras de certificados, números y nombres de personas de contacto, esta Información debe estar disponible con facilidad pero debe permanecer en un ambiente seguro, esto podría ser mantenerla de manera cifrada en un equipo y guardada en una caja fuerte con acceso limitado. (Huguet, 2009). [14]

Los miembros del equipo:

- Gerente o líder del equipo
- Personal para el manejo de incidentes y vulnerabilidades
- Personal de análisis de equipos
- Administradores de red o sistema
- Relaciones con los medios
- Representantes legales (Huguet, 2009)

Plan de contingencia: Planificar todos los pasos necesarios para permitir una recuperación ante desastre o una situación de crisis. Los desastres son inevitables, en la mayoría de los casos impredecibles, y varían de tipo y de magnitud.

Con el fin de minimizar las pérdidas provocadas por los desastres, es muy importante establecer un buen plan de recuperación, para cada organización, departamento y operación.

(Huguet, 2009). [14]

De manera general se puede determinar que un sistema informático es fiable si satisfacen las tres propiedades siguientes:

- **Confidencialidad:** Los recursos que integran el sistema, solo pueden ser accedidos por los elementos autorizados hacerlo, por recursos del sistema no solo se entenderá la información, si no cualquier recurso en general, como impresora, procesador entre otros.
- **Integridad:** Los recursos del sistema solo pueden ser modificados o alterados por los elementos autorizados hacerlo, como borrado creación entre otros.
- **Disponibilidad:** Los recursos del sistema deben permanecer accesibles a los elementos autorizados. (Huguet, 2009).[14]

De acuerdo a lo que dice Miguel Colobran Huguet en el apartado de conceptos básicos de análisis forense en sistemas de información *“el primer paso para la correcta detección de*

*un incidente consiste en verificar que realmente ha sucedido en caso afirmativo
determinar su tipo y magnitud”*

La correcta detección de incidente se realiza mediante diferentes fuentes como : alarmas de detención de incidentes, alarmas de sistemas de antivirus, análisis de registro (log), intercambio de información, aviso de incidentes con miembros de la propia organización.

Contención: Pará minimizar el riesgo deberían llevarse a cabo las siguientes actividades:

- Proteger la seguridad de las personas
- Proteger la información secreta y confidencial
- Proteger la información como dato científico sobre la propiedad de ámbito directivo
- Proteger software y hardware sobre un ataque, pérdida o modificaciones de archivos, contra daños físicos de hardware.
- Minimizar la interrupción de recursos informáticos

Resolución de incidente: Se puede realizar devolviendo el sistema afectado por el incidente al estado operativo, mejorar la seguridad para futuros incidentes, recuperación de pruebas del incidente , se debe organizar la Información cronológicamente, comprobar que está completa y firmarla y revisarla con las directivas y los representantes legales, se debe proteger las pruebas recopiladas en la fase de protección de pruebas, es importante contar con la presencia de personas para que puedan aprobar los pasos, esto permite reducir la probabilidad de que las pruebas se consideran no admisibles y que se modifiquen después.

2.2 ANÁLISIS FORENSE

Con el incremento del número de delitos informáticos presentados en todo el mundo, gran cantidad de países se han visto obligados a tener en cuenta este concepto en sus Legislaciones y a reglamentar la admisión de la evidencia digital en una corte. Colombia no es la excepción y, en consecuencia, los equipos nacionales de atención a incidentes informáticos deben trabajar con técnicas rigurosas que garanticen la admisibilidad legal de la evidencia digital en situaciones judiciales.

La evidencia digital es única, cuando se le compara con otras formas de “evidencia documental”. A comparación de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación genera problemas con respecto al robo de información comercial “secretos Industriales”.

Se debe tener en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque automáticamente se invalidaría la evidencia. Es por esta razón que los investigadores deben revisar constantemente sus copias, y que sean exactamente igual a la original. CHECKSUM ó HASH

Como normativa en Colombia en la Ley 527 de 1999, los mensajes de datos toman fuerza probatoria,

- **ART. 10.** *“Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original”.*
- **ART. 11.** *“Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente”.* (Echeverry, 2008). [16]

Según expertos como Miguel Lopez Delgado quien dice *que para la recopilación de evidencia se puede tomar siguiendo el orden de mayor a menor volatilidad. Este proceso se describe muy bien en el RFC 3227.*

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.

- Estado de los procesos en ejecución.
- Contenido del sistema de archivos y de los discos duros.
- Contenido de otros dispositivos de almacenamiento.

2.2.1 Procedimiento para la recolección de la evidencia

Los primeros pasos para identificar posibles fuentes de datos y obtener información para que las organizaciones se puedan apoyar en la recolección continua de datos con fines forenses, se debe llevar unos procesos y procedimientos los cuales son el apoyo sustentable para los procedimientos legales disciplinarios. Todo esto de acuerdo a las recomendaciones de la NIST 800-86 (Karen Kent, 2012)[17]

Identificación de recursos:

El uso cada vez más generalizado de la tecnología digital con fines personales como profesionales da lugar a una gran proliferación de los datos, las fuentes más comunes de datos son los computadores de escritorio, servidores, dispositivos, almacenamiento de red, estos sistemas como tal también puedes tener unidades internas que aceptan medios de comunicación como DVD,CD, puertos como USB, tarjetas; para almacenamiento de datos externos en los cuales se puede conectar unidades flash, tarjetas de memoria, discos ópticos y magnéticos, otras fuentes son los datos volátiles que están disponibles temporalmente , es decir que están hasta que el sistema se apaga o se reinicia y otros tipos de dispositivos como PDA, teléfonos celulares, cámaras , grabadoras digitales entre otros. (Karen Kent, 2012)[17]

Los analistas deben con ello identificar el área física y reconocer las posibles fuentes de datos, pero sin olvidar con ello otras posibles fuentes de datos en otros lugares. La información también puede ser registrada por otras organizaciones tales como proveedores de internet (ISP). (Karen Kent, 2012)[17]

Es de gran importancia que los analistas deben tener el conocimiento de cada fuente y de los efectos que podría tener en la recolección de los datos, por ejemplo recolectar para obtener copias de registros del ISP se requiere de una orden judicial, así como las consideraciones legales, por ejemplo considerar temas como propiedad externa más cuando se está involucrando fuentes que no están en la ubicación local.

Las organizaciones pueden tomar medidas proactivas para el curso de recopilación de datos que pueden ser útiles en los fines forenses por ejemplo:

- La mayoría de los sistemas operativos están preparados para auditar y registrar ciertos tipos de eventos, se puede extraer información de cómo ocurrió el evento. Y el origen del evento.
- Aplicación de registro centralizado ciertos sistemas y aplicaciones envían copias de registro para asegurar los servidores centrales. El registro centralizado impide que los usuarios no autorizados de la manipulación de registros anti-forenses.

- Realizar copias de seguridad periódicas de los sistemas como lo fueron en un tiempo determinado

Después de identificar las fuentes potenciales de datos, la adquisición se debe realizar mediante un proceso de tres pasos: el desarrollo de un plan para adquirir los datos, la adquisición de los datos y verificar la integridad de los datos adquiridos. Para los pasos dos y tres varían de acuerdo a la función de tipo de datos (Karen Kent, 2012). [17]

2.2.2 Desarrollo de plan de adquisición:

El desarrollo del plan es el más importante en la mayoría de los casos dado que determina las fuentes de datos posibles, al analista debe crear un plan de prioridad para las fuentes de datos, establecer un orden de los datos y como van hacer adquiridos y estos factores de importancia para priorizar incluyen lo siguiente:

Valor probable: Esta basado en la comprensión y análisis de la situación y la experiencia previa con situaciones similares, el analista debe ser capaz de estimar el valor relativo probable de cada fuente de datos

La Volatilidad: Se refiere a los datos que existen en un sistema temporal, y que se pierden cuando una computadora se apaga o se reinicia, estos datos deben tener prioridad sobre datos no volátiles. Sin embargo los datos no volátiles pueden ser un poco naturaleza dinámica por ejemplo archivos de registro que se sobrescriben en nuevos eventos

Cantidad de esfuerzo requerido: la cantidad requerida para adquirir las fuentes puede variar ampliamente, implica no solo el tiempo que requiere los analistas y otros en la organización como los asesores legales, sino también los el costo de los equipos y servicios, por ejemplo un enrutador de red requiere menos esfuerzo que la adquisición de datos de un proveedor de internet.

Teniendo en cuenta estos tres factores para cada fuente potencial de datos los analistas pueden tomar decisiones de acuerdo a la prioridad de adquisición del origen de datos, así como la determinación de la fuente de datos adquirir.

Las organizaciones deben considerar las complejidades de adquisición de datos y dar la prioridad a las fuentes de datos y con ello desarrollar planes escritos y procedimientos que pueda ayudar al analista a realizar y priorizar de manera eficaz. (Karen Kent, 2012). [17]

2.2.3 Adquisición de datos

Si los datos no han sido adquiridos por las herramientas de seguridad, herramientas de análisis u otros medios, el proceso general para la adquisición de los datos implican el uso de herramientas forenses, para recopilar los datos volátiles, no volátiles, esta se puede realizar de manera local o en una red. Aunque es preferiblemente local dado que hay un mayor control del sistema y los datos ,aunque la recopilación local muchas veces no es factible , por ejemplo cuarto cerrado, sistema ubicado en otro espacio físico etc, (Karen Kent, 2012)[17]

Cuando la adquisición de datos se da a través de una red, las decisiones deben tomarse con respecto al tipo de datos y la cantidad de esfuerzo para su uso. Por ejemplo podría ser necesario para la adquisición de datos tomarse desde varios sistemas y diferentes conexiones de red o podría ser suficiente para copiar un volumen lógico desde un mismo sistema.

Verificación de la integridad:

Después de que los datos han sido adquiridos, su integridad debe ser verificada. Es particularmente importante para un analista de demostrar que los datos no se han manipulado si podría ser necesario, la verificación de la integridad consiste en el uso de herramientas el resumen del mensaje de los datos originales y la copia. (Karen Kent, 2012)[17]

Examinación

Luego de que los datos fueron recolectados, se continúa con la fase de examinación de los datos, la cual implica evaluación y extracción de la información relevante., para este proceso es importante utilización de las herramientas de manera óptima , identificar la información pertinente con relación al incidente , la búsqueda de documentos que se relacionan con el tema , los registros de email, es importante la utilización de herramientas que permitan identificar contenido de archivos, tales como texto, gráficos ,música formatos

comprimidos, El conocimiento de tipos de archivos permiten identificar los archivos que puedan contener la Información más relevante y excluir los archivos que no sean de interés. (Karen Kent, 2012). [17]

Examinar archivos de datos

Después de una copia de seguridad de lógica la copia de seguridad o de imagen puede tener que ser restaurada en cualquier otro medio, antes de que los datos sean examinados, esto depende las herramientas forenses utilizadas, algunas herramientas pueden analizar la Información desde la copia imagen directamente, y otras deben pueden ser restauradas a una medio, los datos solo pueden accederse como de solo lectura esto para asegurar que los datos no sean modificados.

Después de restaurar la copia de seguridad si es necesario, el analista empieza analizar los datos y realiza una evaluación de todos los datos localizados en los archivos, incluyendo archivos borrados, es importante tener en cuenta que la Información o datos puede estar contenidos en archivos encriptados o protegidos por contraseñas. (Karen Kent, 2012)[17]

Extraer el dato

Los analistas requieren saber los tipos de datos que contiene el archivo, este lo pueden identificar mirando las cabeceras de los archivos, el cual contiene la Información que identifica un archivo metadatos. En el tema de cifrado de la información es un tema que le

complica notablemente el trabajo a los analistas, dado que se pueden encontrar con la encriptación (proceso para volver ilegible información considera importante) de archivos individuales, carpetas, volúmenes o particiones, aunque la identificación de que el archivo esta encriptado es fácil, el tema de desencriptar (descodificación de encriptacion) no lo es, otros de los temas difíciles de detectar es la estenografía que son los datos contenidos en otros datos, es decir es el ocultamiento de los datos, Una vez seguro de que los datos stegged existe, según los analistas podría ser capaz de extraer los datos incorporados y luego encontrar la clave de Stego, o mediante el uso de la fuerza bruta y ataques criptográficos para determinar un password. Los analistas también pueden necesitar acceder a no stegged archivos que están protegidos por contraseñas. Las contraseñas se almacenan a menudo en el mismo sistema que los archivos que ellos protegen, pero en un formato codificado o cifrado. Varias utilidades están disponibles que puede crackear contraseñas colocados en archivos individuales. (Karen Kent, 2012). [17]

2.3 PROTOCOLO FORENSE

Una vez que la información relevante ha sido extraída, el analista debe estudiar y analizar los datos para sacar conclusiones. El fundamento de la ciencia forense está utilizando un enfoque metódico para llegar a conclusiones sobre la base de los datos disponibles o determinar que no hay ninguna conclusión todavía se pueden extraer. El análisis debe incluir la identificación de las personas, lugares, objetos, eventos, y la determinación de cómo estos elementos se relacionan de manera que una conclusión se puede llegar. A menudo, este esfuerzo va a incluir los datos que correlacionan entre múltiples fuentes. Por ejemplo, una intrusión en la red Detection System (IDS) de registro puede enlazar un evento a un host, los registros de auditoría de acogida puede vincular el caso a una cuenta de usuario específica, y el registro de Host IDS puede indicar lo que las acciones que realiza el usuario. Herramientas como el registro centralizado y el software de seguridad de gestión de eventos puede facilitar este proceso de forma automática la recolección y correlación de los datos. Comparación de las características del sistema de líneas de base conocidos pueden identificar varios tipos de cambios realizados en el sistema.

Basados en el organismos internacionales intervinientes en el tratamiento y regulación de delitos **informáticos** y computación forense **,trabajamos la definición de este protocolo basado en NIST (Computer Security Division)** El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en Inglés), es una AGENCIA norteamericana, encargada de la definición y el mantenimiento de estándares y recomendaciones que promueven la innovación y la competencia industrial dentro de los Estados Unidos. La división de

seguridad computacional fue creada gracias a la ley de gobierno electrónico donde se reconoce la importancia de la seguridad de la información para la seguridad económica y la seguridad nacional. Su trabajo incluye proveer especificaciones para los requisitos mínimos de seguridad para los sistemas de información y la información federal utilizando una aproximación basada en el análisis de riesgos, entre otras tareas relacionadas con la seguridad de la información, incluyendo el manejo de evidencia digital. (Karen Kent, 2012). [17]

2.3.1 Fases básicas

Colección:

La primera fase del proceso consiste en identificar, etiquetar, registrar y obtener datos de las posibles fuentes de datos relevantes, mientras que siguiendo los lineamientos y procedimientos que permiten preservar la integridad de los datos. La recolección se realiza normalmente en el momento oportuno debido a la probabilidad de pérdida de datos dinámicos, como las conexiones de red actuales, así como la pérdida de datos de dispositivos con pilas (por ejemplo, teléfonos celulares, PDAs).

Durante la recolección de datos, el analista debe hacer varias copias de los archivos relevantes o file Systems por lo general una copia maestra y un grupo de trabajo continuación, el analista puede utilizar la copia de trabajo sin afectar a los archivos originales o la copia maestra. A través de técnicas y herramientas para copiar archivos y los datos residuales de archivos de los medios de comunicación. Se analiza la importancia

de mantener la integridad de los archivos y proporciona orientación sobre hardware y software que pueden ayudar en la preservación y la verificación de la integridad del archivo. A menudo es importante recoger no sólo los archivos, sino también marcas de tiempo para los archivos importantes, como cuando los archivos fueron modificados por última vez, o acceder a ella. Se describen las marcas de tiempo y se explica cómo se puede conservar. Otras cuestiones técnicas relacionadas con archivo de colección, tales como la búsqueda de archivos ocultos y copiar archivos de matriz redundante de discos independientes (RAID) puestas en práctica. (Karen Kent, 2012)[17]

Todos los pasos que se tomaron para crear la copia de la imagen debe ser documentado. Si lo hace, debe permitir que cualquier analista para producir un duplicado exacto de los medios de comunicación originales utilizando los mismos procedimientos. Además, la documentación apropiada, puede usarse para demostrar que las pruebas no se manejan adecuadamente durante el proceso de recolección. Las medidas que se tomaron para grabar la imagen el analista debe documentar la información complementaria, como el modelo de disco duro y número de serie, la capacidad de almacenamiento de medios, e información sobre el software de imágenes o hardware que se utiliza (por ejemplo, nombre, número de versión, información sobre licencias). Todas estas acciones apoyan el mantenimiento de la cadena de custodia. (Karen Kent, 2012)

Examinar:

Los exámenes consisten en análisis forense procesar grandes cantidades de datos recogidos mediante una combinación de métodos manuales y automatizados para evaluar y extraer datos de especial interés, preservando la integridad de los datos.

Análisis:

La siguiente fase del proceso consiste en analizar los resultados del examen, utilizando métodos y técnicas jurídicamente justificables, para obtener información útil que responda a las preguntas que fueron el impulso para realizar la recolección y el examen.

Presentación de informes:

La fase final es informar sobre los resultados del análisis, que puede incluir la descripción de las acciones utilizadas, explicando cómo las herramientas y los procedimientos fueron seleccionados, para determinar qué otras acciones deben llevarse a cabo (por ejemplo, examen, forense de las fuentes de datos adicionales, asegurando las vulnerabilidades identificadas, mejorar la los controles de seguridad existentes), y formular recomendaciones para la mejora de las políticas, directrices, procedimientos, herramientas y otros aspectos del proceso forense. La formalidad de la presentación de informes paso es muy variable dependiendo de la situación. (Karen Kent, 2012)[17]

2.3.2 Uso de herramientas Forenses

En la actualidad existen múltiples herramientas para recopilación de la evidencia, son la base esencial de los análisis de las evidencias digitales sin embargo es importante que los investigadores o analistas tengan un conocimiento y formación para utilizarlas adecuadamente de tal forma que los resultados sean confiables. El uso de estas herramientas se hace necesario debido a que hay cantidad de datos almacenados en los equipos, la variedad de formatos de los archivos, tanto la recopilación de la información y las copias generadas deben ser exactas, por la gran cantidad de información el tiempo que tomaría en analizarla, pueden borrarse archivos fácilmente, pueden existir sistemas de encriptación o contraseñas.

Los analistas deben tener acceso a diversas herramientas que les permitan llevar a cabo el análisis de datos, así como algunas actividades de recolección. Muchos de los productos permiten a los analistas forenses llevar a cabo una amplia gama de procesos para analizar archivos y aplicaciones, así como la recolección de los archivos, la lectura de imágenes de disco, y la extracción de datos de archivos. La mayoría de los productos de análisis también ofrecen la posibilidad de generar informes y registrar todos los errores que se produjeron durante el análisis. Aunque estos productos son muy valiosos en la realización de análisis, es fundamental entender los procesos que deben ejecutarse para responder a preguntas específicas sobre los datos.

Un analista que tenga que proporcionar una respuesta rápida o simplemente responder a una sencilla pregunta sobre los datos recogidos. En estos casos, una evaluación forense completa no puede ser necesario o factible incluso. El conjunto de herramientas forense debe contener aplicaciones que pueden lograr el examen y análisis de datos de muchas maneras y se puede ejecutar de forma rápida y eficiente de los disquetes, CD, o una estación de trabajo forense. Los siguientes procesos están entre las que un analista debe ser capaz de realizar con una variedad de herramientas:

- **Usando Visores de Archivos:** Varias herramientas están disponibles para ver los tipos comunes de archivos, y también hay herramientas especializadas exclusivamente para la visualización de gráficos. Los archivos disponibles no son compatibles con un formato de archivo en particular, la aplicación de la fuente original debe ser utilizado, si esto no está disponible, entonces puede que sea necesario para investigar el formato
- **Descompresión de archivos:** Los analistas deben descomprimir los archivos, esta tarea debe realizarse al principio del proceso forense para garantizar el contenido de los archivos comprimidos, sin embargo es importante que los analistas tengan en cuenta que los archivos comprimidos pueden contener , contenidos maliciosas, u bombas de compresión que significa que son archivos que han sido repetidamente comprimidos o contener malware u otras , Aunque no existe una forma definitiva para detectar bombas de compresión antes de descomprimir un archivo, hay

maneras de minimizar su impacto. Se debe crear una imagen del sistema de exploración debe ser creada de modo que, si es necesario, el sistema puede ser restaurado.

- **Gráficamente viendo la estructura de directorios:** esta práctica hace que sea fácil y rápido para los analistas obtener información general sobre el contenido de los medios de comunicación, como tipo de software instalado.
- **Identificación de los archivos conocidos:** Es importante la selección de la información altamente importante para el análisis y por tanto se debe eliminar los archivos que no posea información importante en el análisis.
- **Como realizar las búsquedas de cadenas y coincidencias de patrón:** Varias herramientas de búsqueda están disponibles que puede usar la lógica booleana y difusa, sinónimos y conceptos, derivados y otros métodos de búsqueda. Ejemplos de búsquedas comunes incluyen la búsqueda de varias palabras en un solo archivo y la búsqueda de versiones incorrectas de ciertas palabras.
- **Acceso a los metadatos del archivo:** Metadatos del archivo proporciona detalles acerca de cualquier archivo. Por ejemplo, la recolección de los metadatos de un archivo gráfico puede indicar la fecha de la Gráfica su creación, la información y la descripción, y los metadatos ,los gráficos generados por una cámara digital podría incluir la marca y el modelo de la cámara digital que se utiliza para tomar la

imagen, así como F-stop, flash y ajustes de apertura. Para los archivos de procesamiento de textos, los metadatos podrían especificar el autor, la organización que la licencia del software, cuándo y por quién se realizaron las ediciones pasada, y definidos por el usuario comentarios. Servicios especiales se pueden extraer los datos.

- **Herramientas como ENCASE** es un producto forense de software utilizado por muchos profesionales de la seguridad de la información. Desde su desarrollo en curso a partir de 1998, es uno de los pocos totalmente integrados basados en Microsoft Windows productos para análisis forense investigaciones. EnCase es un descendiente directo del software Perito previamente distribuido por ASR de datos (pre-1998) y las primeras versiones de EnCase eran muy similares a los testigos expertos.

El entorno integrado EnCase significa que el software EnCase adquiere las pruebas en su verificables, propiedad de flujo de bits de la imagen (llamado Presentar pruebas, FE), monta la imagen EF como una unidad virtual de sólo lectura, y reconstruye la estructura del sistema de archivo de la utilización de los datos lógicos en la imagen.

Este procedimiento integrado elimina la secuencia de tiempo de pasos que normalmente se asocian con la tradicional línea de comandos basada en imágenes y asegura que todos los datos y meta-datos (por ejemplo, marcas de tiempo) sigue siendo

forense inalterada. El adquirida está disponible como una pérdida menor. (George Mohay, 2003). [18]

3. METODOLOGÍA

El proyecto está enfocado en el desarrollo debido a que se aborda un tema nuevo o poco explorado, por comparativo con las demás ciencias y disciplinas del campo de la informática y la ciencia forense en su esencia, es por ello que se realiza la presente investigación con el mayor grado de carácter original.

Este análisis permite hacer un análisis detallado, de la necesidad que tienen las organizaciones de velar por la protección de la información, desde la perspectiva teórica y práctica, conociendo cada uno de los fundamentos, elementos, factores, amenazas, riesgos, metodologías y controles a la seguridad de la información, conociendo cada una por separado e identificando la relación que hay entre las mismas y conociendo el protocolo que puede llevar en el momento que encuentre un caso de violación a una política de información de la organización.

El proceso análisis contempla el desarrollo metodológico a partir de los siguientes puntos:

- Levantamiento de la información conceptual con relación a Incidentes, análisis forense y protocolo forense.
- Comprensión y documentación de las normas y protocolos aplicados internacionales y revisión de políticas en Colombia.

4. CONCLUSIONES Y RECOMENDACIONES

- Es importante que las organizaciones vean la informática forense como una herramienta importante en sus políticas de seguridad, teniendo en cuenta el proceso respuesta a incidentes.
- Aunque es destacable la comunidad de desarrollo que se ha encontrado en el análisis forense, en la actualidad existe diversos criterios al de definir estándares en los procesos utilizados para esta disciplina.
- Es importante que los profesionales, a pesar de su capacitación y aportes, se especialicen mas en las herramientas del análisis forense informático con el fin de que las evidencias digitales sean confiables y puedan ser utilizadas como evidencia probatoria en los juicios.
- De acuerdo a lo que menciona *Jeimy J. Cano, Ph.D.* en el artículo Consideraciones técnicas y jurídicas para su manejo evidencia digital, En Colombia el Estado debería empezar a fijar su atención en la creación de equipos, debidamente entrenados, para atender incidentes informáticos, ya que estos son indispensables en el desarrollo de la investigación de delitos informáticos, los cuales con el crecimiento de Internet son cada vez más frecuentes.

Si la inseguridad informática es la constante en el mundo digital, los procedimientos forenses en informática deberían ser la norma que confirma la existencia de la constante. Sin una adecuada respuesta a los incidentes de seguridad, la detección y el seguimiento de los intrusos no tendría sentido.

- Para que la evidencia digital sea confiable, es importante que se cuente con equipos de atención de incidentes, con estándares y procedimientos bien definidos, claros y justificables.
- Se debe pensar en formar unidades de investigación que estén debidamente entrenados para atender incidentes informáticos, ya que son piezas indispensables en el progreso de la informática forense en Colombia

5. BIBLIOGRAFÍA

Documento de la norma -ISO -IEC-27002. (2008). *ISO -IEC-27002* .

Academia Latinoamericana de Seguridad Informática. (2011). <http://www.piramidedigital.com>. Recuperado el 22 de 10 de 2011, de <http://www.piramidedigital.com/Documentos/ICT/pdictseguridadinformaticainroduccion.pdf>

AGESIC, I. A. (septiembre de 2010). *guia de procesos de gestion de incidentes*. Recuperado el 15 de 11 de 2011, de http://www.agesic.gub.uy/innovaportal/file/1217/1/Guia_de_procesos_en_gestion_de_incidentes.pdf

Best Management Practice. (s.f.). *Official Sites: Best Management Practice*. Obtenido de Official Sites: Best Management Practice: <http://www.best-management-practice.com/publications-library/it-service-management-til/til-version-2/security-management/online-subscription/>

BON, J. V. (2005). *Google Books*. Recuperado el 1 de 11 de 2011, de Gestión de servicios TI: una introducción a ITIL: http://books.google.com.co/books?id=HUaDV0SSJbwC&printsec=frontcover&hl=es&redir_esc=y

BORGHELLO, C. (13 de 04 de 2009). *ESET*. Obtenido de http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

Brezinski, D. (febrero de 2002). *Guidelines for Evidence Collection and Archiving*. Recuperado el 15 de 02 de 2012, de <http://www.ietf.org/rfc/rfc3227.txt>

CA. (2004). *Gestión de Proyectos y Soporte de TI*. Buenos Aires: Proyecto Pegasus.

CASTELLS. (2008). *La era de la información "Nuevo sistema tecnológico, económico y social. Una economía en la que el incremento de productividad no depende del incremento cuantitativo de los factores de producción(capital,trabajo, recursos)"*.

- Centro Tecnológico de Telecomunicaciones De Catalunya. (2011). <http://www.cttc.es/>. (C. CTTC, Ed.) Recuperado el 24 de 08 de 2011, de <http://www.cttc.es/resources/doc/080122-glosario-48230.pdf>
- Ciberculturahoy. (2011). <http://ciberculturahoy.wordpress.com/>. Recuperado el 13 de 09 de 2011, de <http://ciberculturahoy.wordpress.com/>: <http://ciberculturahoy.wordpress.com/glosario/>
- Citibank Colombia. (2010). *Colombia sostenible 2010*. Obtenido de https://www.citibank.com.co/common/pdf/Inf_sost2010.pdf
- COLL, F. M. (s,f). *Rediris*. Obtenido de Recomendaciones de Seguridad. Definición de una Política de Seguridad. : http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html
- CONFINAL. (2011 de ENERO de 2011). *Consultoria Financiera Nacional*. Recuperado el 02 de Diciembre de 2011, de Consultoria Financiera Nacional: <http://cofinalsas.blogspot.com/2011/01/centrales-de-informacion.html>
- CONGRESO DE LA REPUBLICA. (31 de diciembre de 2008). *secretaria del senado*. Recuperado el 17 de Noviembre de 2011, de secretaria del senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
- CONGRESO DE LA REPUBLICA. (05 de enero de 2009). *secretaria del senado*. Recuperado el 25 de Noviembre de 2011, de secretaria del senado: http://www.secretariasenado.gov.co/basedoc/ley/2009/ley_1273_2009.html
- Cuervo, J. (04 de 01 de 1998-2011). *Informatica Juridica*. Recuperado el 02 de 04 de 2012, de http://www.informatica-juridica.com/anexos/Ley_527_Mensajes_de_Datos_Comercio_Electronico_y_Firma_Digital_18_agosto_1999.colombia.asp
- Cuervo, J. (11 de septiembre de 2000). *informatica y juridica*. Recuperado el 03 de 04 de 2012, de http://www.informatica-juridica.com/anexos/Decreto_1747_reglamenta_parcialmente_Ley_527_certificados_y_firmas_digitales_colombia.asp
- Echeverry, J. j. (2008). *procedimiento policiales de colombia*. Recuperado el 12 de marzo de 2012, de <http://procedimientospolicialescolombia.blogspot.com/2008/11/evidencia-digital-como-medio-de-prueba.html>
- FALFÁN, J. B. (2 de Septiembre de 2007). *Seguinfo*. Recuperado el 5 de 11 de 2011, de Seguridad Informática:

<http://seguinfo.wordpress.com/2007/09/02/administracion-de-la-seguridad-en-til-2/>

George Mohay, C.-O. G.-A.-B. (2003). *computer and intrusion forencics*. British Library Cataloguing in Publication Data.

Gestión Calidad Consulting. (2009). *Gestión Calidad* . Obtenido de Gestión Calidad : <http://www.gestion-calidad.com/iso-27000.html>

GMV . (s.f.). *GMV*. Recuperado el 3 de 02 de 2012, de <http://www.gmv.com/es/Seguridad/>

HERNÁNDEZ, J. L. (s.f). *La Gestión de la información en las organizaciones: Una disciplina Emergente*.

Huguet, M. C. (2009). *Analisis Forense de sistemas de Informacion*. Barcelona: Eureka Media.

IBARRA, J. Á. (10 de 2011). *CACS*. Obtenido de <http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/111.pdf>

informacion, A. d. (septiembre de 2010). Recuperado el 12 de febrero de 2012, de www.sgsi.com.

Instituto Nacional de Tecnologías de la Información. (09 de 2011). <http://cert.inteco.es/>. Recuperado el 16 de 10 de 2011, de <http://cert.inteco.es/>: http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/?jsessionid=FB464276F5E6DBDC271780F0CE609687

Inter Prom Usa. (2002). *Enterprise Service Management Excellence. What is ITIL*, 3.

ISACA. (2005). *Juan de Dios BEL*. Ciudad de Panamá, Panamá: CACS.

ISO27000. (2009). *The ISO 27000 Directory*. Obtenido de The ISO 27000 Directory: <http://www.27000.org/>

IT Governance Institute. (s.f.). ITSM, ITIL. En E. I. Gubernamental, *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*.

ITIL CENTRAL. (2007). *ITIL CENTRAL*. Recuperado el 24 de 11 de 2011, de News and Information for ITIL: <http://itsm.fwtk.org/>

ITIL, G. (s,f). *Glosario de Términos ITIL®, Definiciones y Acrónimos*. Recuperado el 1 de 2 de 2012

- Jordi Serra, M. C. (2009). *Analisis Forense de sistemas de Informacion*. Barcelona: Eureka media.
- JRJ. (13 de enero de 2009). *Cosntitucion y Cuidadania*. Obtenido de <http://blogjus.wordpress.com/2009/01/13/ley-1266-de-2008-habeas-data/>
- Karen Kent, S. C. (28 de 02 de 2012). *CSRC.NIST*. Recuperado el 2012, de Guide to Integrating Forensic Techniques into Incident Response : <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
- KRALL, C. (2011). <http://www.aprenderaprogramar.com/>. Recuperado el 02 de 12 de 2011, de <http://www.aprenderaprogramar.com/>: http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=160:seguridad-informatica-hacking-a-los-hackers-iy-nuestros-datos&catid=45:tendencias-programacion&Itemid=164
- L., V. C. (2008). protocolo Informatico Forense.
- LANDEIRA PRADO, R. A. (2006). *Books.google.com*. Recuperado el 03 de Diciembre de 2011, de [Books.google.com](http://books.google.com.co/books): <http://books.google.com.co/books>
- MARQUIS, H. (5 de ABRIL de 2006). *Itsmsolutions*. Obtenido de VOL. 2.14: <http://www.itsmsolutions.com/newsletters/DITYvol2iss14.htm>
- MOLINA FOCAZZIO, L. A. (2007). *Channel Planet*. Obtenido de ITIL y la auditoria de TI y COBIT: <http://www.channelplanet.com/>
- NAVARRO, E. d. (2001). *Peritajes informáticos*. Madrid: Díaz de Santos S.A.
- Osiastis. (s.f.). *Osiastis*. Recuperado el 1 de 11 de 2011, de Itil Gestión de servicios TI: http://itil.osiastis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php
- OVIEDO, O. (12 de 2009). <http://oswaloviedosport.blogspot.es>. Recuperado el 23 de 10 de 2011, de <http://oswaloviedosport.blogspot.es>: <http://oswaloviedosport.blogspot.es/1263058380/>
- PACHAJOA, C. (s,f). *Gestión de la Seguridad*. (Getronics, Intérprete)
- Pink Elephant Inc. (2002). Benefits of ITIL. *White Paper*, 15.
- RINCON RIOS, J. (enero de 2009). *issuu.com*. (D. d. Economicas, Ed.) Recuperado el 26 de Noviembre de 2011, de issuu.com: <http://issuu.com/dialtec/delitoelectronico>

- ROUYET, J. I. (05 de 11 de 2007). *CIO España*. Obtenido de CIO España: <http://www.idg.es/cio/mostrarArticulo.asp?id=304068052&seccion=management>
- RUBIO, R. J. (2005). <http://profesores.is.escuelaing.edu.co>. Recuperado el 20 de 07 de 2011, de <http://profesores.is.escuelaing.edu.co>: <http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%200Y%20MATERIAL%20DE%20ESTUDIO/Introducci%F3n%20a%20los%20conceptos%20de%20Seguridad.pdf>
- SAGARRA, S. (11 de Julio de 2011). *Security at work*. Obtenido de <http://www.securityartwork.es/2011/07/11/5745/>
- Seguridad PC. (s.f). *Seguridad PC*. Obtenido de <http://www.seguridadpc.net/phishing.htm>
- Standardization, i. o. (02 de 03 de 2012). http://www.iso.org/iso/catalogue_detail.htm?csnumber=35396. Obtenido de http://www.iso.org/iso/catalogue_detail.htm?csnumber=35396
- Superfinanciera. (27 de Julio de 2011). *Conceptos Superintendencia Financiera de Colombia*. Obtenido de Boletín Jurídico: <http://www.superfinanciera.gov.co/Normativa/PrincipalesPublicaciones/boletin3311/seguridadycalidad.html>
- TORRES NIETO, A. (2007). *Telecomunicaciones y telemática: de las señales de humo a las actividades por Internet*. Bogotá D.C, Colombia: Escuela Colombiano de Ingeniería.
- TUXTENO. (2011). <http://www.tuxteno.net>. Recuperado el 15 de 08 de 2011, de <http://www.tuxteno.net>: <http://www.tuxteno.net/servicios/seguridad.html>
- UNAM Instituto de Investigacions Juridicas. (s.f). *Biblioteca Jurídica Virtual del Instituto de Investigacions Juridicas de la UNAM*. Recuperado el 04 de 12 de 2011, de <http://www.juridicas.unam.mx/publica/librev/rev/posder/cont/1/cnt/cnt6.pdf>
- UNAM, D. d. (s.f). *seguridad unam*. Recuperado el 9 de 04 de 2012, de <http://www.seguridad.unam.mx/descarga.dsc?arch=1736>
- Universidad Complutense Madrid. (11 de 09 de 1997). *ucm*. Obtenido de <http://www.ucm.es/info/Psyap/taller/procedimientos/sld002.htm>
- Universidad EAFIT. (s.f). *Sarbarnes Oxley*. Obtenido de <http://www.forodeseguridad.com/artic/segcorp/7217.htm>

Visa International Service Association. (2010). *VISA*. Obtenido de Seguridad de la Información: <https://www.visa.com.co/visa-colombia/comercios/seguridad-de-la-informacion.aspx>

[4] Documento de la norma -ISO -IEC-27002. (2008). *ISO -IEC-27002* .

Academia Latinoamericana de Seguridad Informática. (2011). <http://www.piramidedigital.com>. Retrieved 10 22, 2011, from <http://www.piramidedigital.com/Documentos/ICT/pdictseguridadinformaticainroduccion.pdf>

AGESIC, I. A. (2010, septiembre). *guia de procesos de gestion de incidentes*. Retrieved 11 15, 2011, from http://www.agesic.gub.uy/innovaportal/file/1217/1/Guia_de_procesos_en_gestion_de_incidentes.pdf

Best Management Practice. (n.d.). *Official Sites: Best Management Practice*. Retrieved from Official Sites: Best Management Practice: <http://www.best-management-practice.com/publications-library/it-service-management-til/til-version-2/security-management/online-subscription/>

BON, J. V. (2005). *Google Books*. Retrieved 11 1, 2011, from Gestión de servicios TI: una introducción a ITIL: http://books.google.com.co/books?id=HUaDV0SSJbwC&printsec=frontcover&hl=es&redir_esc=y

BORGHELLO, C. (2009, 04 13). *ESET*. Retrieved from http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

Brezinski, D. (2002, febrero). *Guidelines for Evidence Collection and Archiving*. Retrieved 02 15, 2012, from <http://www.ietf.org/rfc/rfc3227.txt>

CA. (2004). *Gestión de Proyectos y Soporte de TI*. Buenos Aires: Proyecto Pegasus.

CASTELLS. (2008). *La era de la información "Nuevo sistema tecnológico, económico y social. Una economía en la que el incremento de productividad no depende del incremento cuantitativo de los factores de producción(capital,trabajo, recursos)"*.

Centro Tecnológico de Telecomunicaciones De Catalunya. (2011). <http://www.cttc.es/>. (C. CTTC, Ed.) Retrieved 08 24, 2011, from <http://www.cttc.es/resources/doc/080122-glosario-48230.pdf>

- Ciberculturahoy. (2011). <http://ciberculturahoy.wordpress.com/>. Retrieved 09 13, 2011, from [http://ciberculturahoy.wordpress.com/glosario/](http://ciberculturahoy.wordpress.com/http://ciberculturahoy.wordpress.com/glosario/)
- Citibank Colombia. (2010). *Colombia sostenible 2010*. Retrieved from https://www.citibank.com.co/common/pdf/Inf_sost2010.pdf
- COLL, F. M. (s,f). *Rediris*. Retrieved from Recomendaciones de Seguridad. Definición de una Política de Seguridad. : http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html
- CONFINAL. (2011, ENERO 2011). *Consultoria Financiera Nacional*. Retrieved Diciembre 02, 2011, from Consultoria Financiera Nacional: <http://cofinalsas.blogspot.com/2011/01/centrales-de-informacion.html>
- CONGRESO DE LA REPUBLICA. (2008, diciembre 31). *secretaria del senado*. Retrieved Noviembre 17, 2011, from secretaria del senado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
- CONGRESO DE LA REPUBLICA. (2009, enero 05). *secretaria del senado*. Retrieved Noviembre 25, 2011, from secretaria del senado: http://www.secretariasenado.gov.co/basedoc/ley/2009/ley_1273_2009.html
- Cuervo, J. (1998-2011, 01 04). *Informatica Juridica*. Retrieved 04 02, 2012, from http://www.informatica-juridica.com/anexos/Ley_527_Mensajes_de_Datos_Comercio_Electronico_y_Firma_Digital_18_agosto_1999.colombia.asp
- Cuervo, J. (2000, septiembre 11). *informatica y juridica*. Retrieved 04 03, 2012, from http://www.informatica-juridica.com/anexos/Decreto_1747_reglamenta_parcialmente_Ley_527_certificados_y_firmas_digitales_colombia.asp
- Echeverry, J. j. (2008). *procedimiento policiales de colombia*. Retrieved marzo 12, 2012, from <http://procedimientospolicialescolombia.blogspot.com/2008/11/evidencia-digital-como-medio-de-prueba.html>
- FALFÁN, J. B. (2007, Septiembre 2). *Seguinfo*. Retrieved 11 5, 2011, from Seguridad Informática: <http://seguinfo.wordpress.com/2007/09/02/administracion-de-la-seguridad-en-itol-2/>
- George Mohay, C.-O. G.-A.-B. (2003). *computer and intrusion forencics*. British Library Cataloguing in Publication Data.

- Gestión Calidad Consulting. (2009). *Gestión Calidad* . Retrieved from Gestión Calidad : <http://www.gestion-calidad.com/iso-27000.html>
- GMV . (n.d.). *GMV*. Retrieved 02 3, 2012, from <http://www.gmv.com/es/Seguridad/>
- HERNÁNDEZ, J. L. (s.f). *La Gestión de la información en las organizaciones: Una disciplina Emergente*.
- Huguet, M. C. (2009). *Análisis Forense de sistemas de Información*. Barcelona: Eureka Media.
- IBARRA, J. Á. (2011, 10). CACS. Retrieved from <http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/111.pdf>
- informacion, A. d. (2010, septiembre). Retrieved febrero 12, 2012, from www.sgsi.com.
- Instituto Nacional de Tecnologías de la Información. (2011, 09). <http://cert.inteco.es/>. Retrieved 10 16, 2011, from http://cert.inteco.es/Formacion/SGSI/Conceptos_Basicos/?jsessionid=FB464276F5E6DBDC271780F0CE609687
- Inter Prom Usa. (2002). Enterprise Service Management Excellence. *What is ITIL*, 3.
- ISACA. (2005). *Juan de Dios BEL*. Ciudad de Panamá, Panamá: CACS.
- ISO27000. (2009). *The ISO 27000 Directory*. Retrieved from The ISO 27000 Directory: <http://www.27000.org/>
- IT Governance Institute. (n.d.). ITSM, ITIL. In E. I. Gubernamental, *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*.
- ITIL CENTRAL. (2007). *ITIL CENTRAL*. Retrieved 11 24, 2011, from News and Information for ITIL: <http://itsm.fwtk.org/>
- ITIL, G. (s,f). Glosario de Términos ITIL®, Definiciones y Acrónimos. Retrieved 2 1, 2012
- Jordi Serra, M. C. (2009). *Análisis Forense de sistemas de Información*. Barcelona: Eureka media.
- JRJ. (2009, enero 13). *Cosntitucion y Cuidadania*. Retrieved from <http://blogjus.wordpress.com/2009/01/13/ley-1266-de-2008-habeas-data/>

- Karen Kent, S. C. (2012, 02 28). *CSRC.NIST*. Retrieved 2012, from Guide to Integrating Forensic Techniques into Incident Response : <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
- KRALL, C. (2011). <http://www.aprenderaprogramar.com/>. Retrieved 12 02, 2011, from <http://www.aprenderaprogramar.com/>: http://www.aprenderaprogramar.com/index.php?option=com_content&view=article&id=160:seguridad-informatica-hacking-a-los-hackers-iy-nuestros-datos&catid=45:tendencias-programacion&Itemid=164
- L., V. C. (2008). protocolo Informatico Forense.
- LANDEIRA PRADO, R. A. (2006). *Books.google.com*. Retrieved Diciembre 03, 2011, from Books.google.com: <http://books.google.com.co/books>
- MARQUIS, H. (2006, ABRIL 5). *Itsmsolutions*. Retrieved from VOL. 2.14: <http://www.itsmsolutions.com/newsletters/DITYvol2iss14.htm>
- MOLINA FOCAZZIO, L. A. (2007). *Channel Planet*. Retrieved from ITIL y la auditoria de TI y COBIT: <http://www.channelplanet.com/>
- NAVARRO, E. d. (2001). *Peritajes informáticos*. Madrid: Díaz de Santos S.A.
- Osiastis. (s.f.). *Osiastis*. Retrieved 11 1, 2011, from Itil Gestión de servicios TI: http://itil.osiastis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php
- OVIEDO, O. (2009, 12). <http://oswaloviedosport.blogspot.es>. Retrieved 10 23, 2011, from <http://oswaloviedosport.blogspot.es>: <http://oswaloviedosport.blogspot.es/1263058380/>
- PACHAJOA, C. (s,f). *Gestión de la Seguridad*. (Getronics, Performer)
- Pink Elephant Inc. (2002). Benefits of ITIL. *White Paper*, 15.
- RINCON RIOS, J. (2009, enero). *issuu.com*. (D. d. Economicas, Ed.) Retrieved Noviembre 26, 2011, from *issuu.com*: <http://issuu.com/dialtec/delitoelectronico>
- ROUYET, J. I. (2007, 11 05). *CIO España*. Retrieved from CIO España: <http://www.idg.es/cio/mostrarArticulo.asp?id=304068052&seccion=management>
- RUBIO, R. J. (2005). <http://profesores.is.escuelaing.edu.co>. Retrieved 07 20, 2011, from <http://profesores.is.escuelaing.edu.co>: <http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%2>

0Y%20MATERIAL%20DE%20ESTUDIO/Introducci%F3n%20a%20los%20c
onceptos%20de%20Seguridad.pdf

SAGARRA, S. (2011, Julio 11). *Security at work*. Retrieved from
<http://www.securityartwork.es/2011/07/11/5745/>

Seguridad PC. (s.f). *Seguridad PC*. Retrieved from
<http://www.seguridadpc.net/phishing.htm>

Standardization, i. o. (2012, 03 02).
http://www.iso.org/iso/catalogue_detail.htm?csnumber=35396. Retrieved
from http://www.iso.org/iso/catalogue_detail.htm?csnumber=35396

Superfinanciera. (2011, Julio 27). *Conceptos Superintendencia Financiera de
Colombia*. Retrieved from Boletín Jurídico:
[http://www.superfinanciera.gov.co/Normativa/PrincipalesPublicaciones/bolet
inej/boletin3311/seguridadycalidad.html](http://www.superfinanciera.gov.co/Normativa/PrincipalesPublicaciones/boletin3311/seguridadycalidad.html)

TORRES NIETO, A. (2007). *Telecomunicaciones y telemática: de las señales de
humo a las actividades por Internet*. Bogotá D.C, Colombia: Escuela
Colombiano de Ingeniería.

TUXTENO. (2011). <http://www.tuxtено.ne>. Retrieved 08 15, 2011, from
<http://www.tuxtено.ne>: <http://www.tuxtено.net/servicios/seguridad.html>

UNAM Instituto de Investigacions Juridicas. (s.f). *Biblioteca Jurídica Virtual del
Instituto de Investigacions Juridicas de la UNAM*. Retrieved 12 04, 2011,
from
<http://www.juridicas.unam.mx/publica/librev/rev/posder/cont/1/cnt/cnt6.pdf>

UNAM, D. d. (n.d.). *seguridad unam*. Retrieved 04 9, 2012, from
<http://www.seguridad.unam.mx/descarga.dsc?arch=1736>

Universidad Complutense Madrid. (1997, 09 11). *ucm*. Retrieved from
<http://www.ucm.es/info/Psyap/taller/procedimientos/sld002.htm>

Universidad EAFIT. (s.f). Sarbarnes Oxley. Retrieved from
<http://www.forodeseguridad.com/artic/segcorp/7217.htm>

Visa International Service Association. (2010). *VISA*. Retrieved from Seguridad de
la Información: [https://www.visa.com.co/visa-colombia/comercios/seguridad-
de-la-informacion.aspx](https://www.visa.com.co/visa-colombia/comercios/seguridad-de-la-informacion.aspx)