UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

"PROPUESTA DE GUÍA DE SEGURIDAD DE INFORMACIÓN DIGITAL DIRIGIDA A LA GERENCIA GENERAL DE UNA ORGANIZACIÓN"

Realizado por:

JOSÉ ADRIÁN PINO VERA

Como requisito para la obtención del título de INGENIERO DE SISTEMAS EN INFORMÁTICA

QUITO, MAYO DE 2009

DECLARACIÓN JURAMENTADA

Yo, José Adrián Pino Vera, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

……

José Adrián Pino Vera

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado

PROPUESTA DE GUÍA DE SEGURIDAD DE INFORMACIÓN DIGITAL DIRIGIDA A LA GERENCIA GENERAL DE UNA ORGANIZACIÓN

Realizado por el alumno

JOSÉ ADRIAN PINO VERA

como requisito para la obtención del título de

INGENIERO DE SISTEMAS EN INFORMÁTICA

ha sido dirigido por el profesor

Ing. ROBERTO LANDÁZURI

quien considera que constituye un trabajo original de su autor.

…….

Ing. ROBERTO LANDÁZURI

Director

Los profesores informantes

Ing. VIVIANA GUERRÓN, e

Ing. SANTIAGO MENA

después de revisar el trabajo escrito presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador.

…… ……..

Ing. VIVIANA GUERRÓN Ing. SANTIAGO MENA

Quito, a 11 de Mayo del 2009

DEDICATORIA

A MI FAMILIA: Que confió en mi anhelo, creyó incondicionalmente en mis sueños siendo mi guía, mi soporte y el más puro aliciente que ha inspirado la culminación de mi carrera, con amor profundo, mi triunfo es su triunfo. Gratitud inmensa por su fe inquebrantable, eterno amor para ellos.

AGRADECIMIENTO

A los señores profesores de la Facultad de Ingeniería de Sistemas en Informática, de la Universidad Internacional SEK, por la entrega de su valiosa enseñanza para la formación de profesionales honestos y correctos, así como a los Ings. Santiago Mena y Viviana Guerrón, quienes me supieron dirigir sin egoísmo, y que en forma incondicional me han participado de sus experiencias y conocimientos.

Agradezco a Dios, por su guía e iluminación en mi vida estudiantil.

RESUMEN EJECUTIVO

El presente proyecto puede ser considerado como una guía de Seguridad de la Información cuyo principal objetivo es brindar a la Gerencia General de una Organización una base de conocimiento que sea útil para evaluar e implementar un sistema integral de seguridad con la finalidad de controlar accesos a los activos de información digital, su forma de uso, divulgación, interrupción o destrucción.

La guía propuesta en este trabajo tiene una aplicación universal a cualquier organización, sin importar su tamaño o naturaleza. El método descrito es de fácil ejecución y permite que la Gerencia General implemente y gestione proyectos cuyo objetivo sea evitar que ciertos eventos de seguridad se conviertan en incidentes de seguridad.

ABSTRACT

The present project can be considered to be a Digital Information Security Guide which principal aim is to offer to the General Management of an Organization a base of knowledge that is useful to evaluate and to implement an integral system of safety with the purpose of controlling accesses to the assets of digital information, its form of use, publication, interruption or destruction

The guide proposed in this work, has a universal application to any organization, without importing its size or nature. The described method is of easy execution and allows that the General Management should implement and manages projects which goal is to prevent certain events of safety from turning into safety incidents.

CONTENIDO

1. DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN

1.1. INTRODUCCIÓN

En la actualidad, debido a los distintos niveles tecnológicos que cada una de las empresas adquiere, su gestión de la información también cambia, por ejemplo, anaqueles que contenían carpetas y documentos impresos o escritos han quedado casi obsoletos, ahora, toda esa infraestructura de oficina tiende a cambiarse por infraestructura tecnológica. De la misma forma los funcionarios de la organización ya no tienen acceso a estos documentos escritos sino a archivos digitales, de tal manera que si ellos quisieran transmitir este tipo de información a personas no autorizadas, podrían recurrir a mecanismos y técnicas simples para lograrlo, como por ejemplo, un teléfono celular, una memoria extraíble, un mensaje de correo electrónico, etc.

Dicho lo anterior y considerando una eventual fuga de información por parte los funcionarios, la organización debe estar decidida, concientizada, capacitada y preparada para afrontarlo:

- Decidida, porque aún no existe la cultura de la demanda informática, ya que la organización teme perder imagen ante sus clientes y ante la competencia.

- Concientizada, ya que debe haber una cultura de los funcionarios orientada a la fidelidad, seguridad, confianza y compromiso hacia la empresa, como a todos sus activos, tomando en cuenta que el activo más valioso es la información.

- Capacitada, ya que la capacitación individual, departamental y organizacional, tiende a ser la base de la seguridad de la información; y,

- Preparada ya que se requiere tener mecanismos tanto de prevención como de análisis del delito informático.

Todo lo anterior deberá ir de la mano con los distintos manuales y políticas internas de la organización, ya que cada departamento y área de la misma serán la base tanto para establecer responsabilidades y funciones, como también para determinar sanciones, las cuales podrían ser tanto a nivel interno, como a nivel judicial, dependiendo de la gravedad del delito, de las consecuencias del mismo y de la conveniencia de la empresa.

Con el objetivo de prevenir intrusiones a la información digital, a más de establecer los mecanismos técnicos ya conocidos (claves de acceso, firewalls, etc.) se debe considerar al personal, ya que una parte importante de la seguridad de la información es la capacitación de todo funcionario para no cometer errores, sean o no forzados y sobre todo de implementar una política de entrega de información a cualquier funcionario bajo requisitos previamente establecidos; además de tener personal especialista dentro de la organización para que se encargue de la seguridad de toda la información.

Considerando la investigación forense es necesario saber que, como toda investigación, ésta se basa en un proceso, el cual, si no es seguido adecuadamente puede entorpecer el camino del esclarecimiento del delito. Por ello se requiere de un especialista forense, quien apoyado en su conocimiento y con ciertas herramientas analizará toda evidencia digital, lo que permitirá no determinar quién es el culpable, sino, desde donde y en que momento se realizó el acto ilícito, para que la organización apoyándose en sus políticas decida a quién o quienes sancionar. Es por eso que las políticas deben ser robustas y consistentes, pero también realistas.

Finalmente, la Gerencia General debe saber lo que se hace en todo momento, el punto de partida y el punto de llegada, además de todo el procedimiento comprendido entre estos dos puntos, simplemente porque ellos son los encargados de tomar decisiones, y, para esto deben contar con ciertos conocimientos referentes al que hacer del personal técnico.

1.2. ANTECEDENTES

Al igual que en todas las ramas de la actividad humana, la tecnología ha significado evolución y mayor facilidad para realizar las distintas actividades, es así que, las varias formas de cometer fraudes han evolucionado en el sentido de que ya no es necesario ser usuario técnico para cometer delitos informáticos. El alcance de esta investigación se enmarca en proponer medidas de seguridad de información digital y lineamientos básicos de informática forense dirigidos a la Gerencia General de una organización a fin de conocer y prevenir sobre delitos informáticos internos de fuga de información.

1.3. SITUACIÓN ACTUAL

Las empresas en el Ecuador se encuentran en proceso de modernización e incluso implementando su infraestructura tecnológica, lo cual brinda mayores facilidades para que con la ayuda de técnicas y dispositivos, los funcionarios cometan ilícitos orientados a transmitir información de carácter confidencial sin la debida autorización, perjudicando a dicha organización en varios aspectos tales como ventajas competitivas, toma de decisiones, planes de marketing, datos de empleados, información de proyectos, etc.

1.4. JUSTIFICACIÓN

La necesidad de contar con una guía de contenido fundamentado, aprobado, aceptado y técnicamente válido que sirva como soporte a la Gerencia General de una organización para formar parte activa en la evaluación e implementación de un sistema de seguridad de información digital, justifica la elaboración del presente trabajo.

1.5. IMPORTANCIA

La importancia de este trabajo radica en que las Gerencias Generales de todas las organizaciones deben formar parte activa en proyectos de aseguramiento de activos, incluyendo proyectos de implementación y evaluación de sistemas de seguridad de información digital, de modo que, una guía servirá como base para salvaguardar dichos activos de una manera metódica, ordenada y eficaz.

1.6. DEFINICIÓN DEL TEMA

El tema de la presente investigación es Propuesta una Guía de Seguridad de Información Digital Dirigida a la Gerencia General de una Organización.

1.7. OBJETIVOS

1.7.1. Objetivo General

Diseñar y definir una guía de seguridad de información digital dirigida a la Gerencia General de una organización.

1.7.1. Objetivos Específicos

- Determinar razones por las cuales el área de Tecnología de una Organización, administrativamente debe subordinarse solamente de la Gerencia General para lograr que la implementación de un sistema de seguridad de información digital no enfrente oposición de ningún tipo proveniente de los funcionarios de la organización.
- Determinar los aspectos básicos de Seguridad de Información (Digital), Derecho Informático e Informática Forense.
- Indicar algunos de los aspectos más frágiles que forman parte de un sistema de seguridad de información digital.
- Recomendar prácticas administrativas de seguridad de información digital para prevenir delitos informáticos internos de fuga de información, estableciendo controles técnicamente definidos.

1.8. DISEÑO METODOLÓGICO

El presente trabajo se desarrolla en base a una investigación descriptiva de tipo aplicada, ya que se enfoca a estudiar una realidad dada por un problema específico el cual es la fuga de información digital de una organización por parte de su personal.

Para apoyar a la investigación, se utilizan técnicas de estudio tales como la investigación documental, la entrevista, y la observación:

La investigación documental será la base para trabajar con todos los documentos disponibles tales como libros de texto y documentos digitales, que, principalmente serán utilizados para sustentar el marco teórico de la presente investigación.

La entrevista y la observación serán utilizadas para obtener información de distintos profesionales que posean conocimientos relevantes para sustentar el presente tema de estudio.

Finalmente se analizarán los resultados obtenidos con la finalidad de emitir conclusiones y recomendaciones que evidencien que los objetivos planteados al inicio de la investigación han sido alcanzados de acuerdo a las expectativas.

2. MARCO TEÓRICO

2.1. SEGURIDAD INFORMÁTICA

Seguridad informática es un concepto amplio que engloba una serie de técnicas, procedimientos, estudios, estimaciones, análisis, interpretaciones, aplicaciones de herramientas, apoyo en experiencias pasadas, etc., con la finalidad de determinar qué activo requiere ser protegido y por qué, de qué debe ser protegido y cómo protegerlo. [1]

2.2. CONTRAMEDIDAS

Son un conjunto de técnicas y herramientas orientadas a la prevención de delitos informáticos, por ejemplo, equipos de control físico y electrónico con el objetivo de neutralizar elementos de escucha; una adecuada configuración de los parámetros de seguridad en un Directorio Activo de Windows, etc.

2.3. CARACTERÍSTICAS DE LA INFORMACIÓN SEGURA

Para que la información digital sea considerada como segura, debe reunir las siguientes características:

- Confidencialidad: Que la información esté protegida de personas no autorizadas. [2]
- Integridad: Que la información esté como se pretende, sin modificaciones inapropiadas. [2]
- Disponibilidad: Que los usuarios autorizados tienen acceso a la información cómo y cuando lo requieran. [2]
- Irrefutabilidad: Que nadie pueda negar la autoría de la información que ha proporcionado.[2]

[1] ALEXANDER, Alberto. 2007. Diseño y Gestión de un Sistema de Seguridad. Pág. 13
[2] VIEITES, Alexis. 2006. Enciclopedia de la Seguridad Informática. Pág. 67-68

2.4. ANÁLISIS DE RIESGOS

2.4.1. Concepto

Es el proceso de usar información obtenida, para identificar posibles fuentes y estimar los riesgos que pueden provenir de estas, con la finalidad de tomar medidas de manera anticipada para que en caso de que sucedan, no impacten de manera considerable a los distintos activos. [3]

La finalidad de hacer un análisis de riesgos es estimar posibles escenarios en los cuales una amenaza puede aprovecharse de una vulnerabilidad y generar fallas en la seguridad, ya que, sin amenazas no hay riesgos debido a que una vulnerabilidad por sí sola no causa daño pero si puede hacer que una amenaza se convierta en incidente.

2.4.2. Reducir Riesgos

Indica reducir la posibilidad de que la vulnerabilidad sea explotada por la amenaza, o, detectando eventos no deseables antes de que ocurran para reducir al máximo los riesgos que estos conllevan. [3]

2.4.3. Aceptar Riesgos

Esta decisión es tomada en caso de que la organización no pueda identificar el riesgo, o los costos para afrontarlo sobrepasen el presupuesto, o que simplemente el costo de las consecuencias no sean considerables, se puede tomar la decisión de aceptar el riesgo y asumir las consecuencias si este llega a ocurrir. [3]

2.4.4. Transferir Riesgos

Esta opción es la más idónea cuando se trata de una organización que carece de recursos para reducir o controlar el riesgo a un nivel aceptable, de manera que por ejemplo, optan por aseguradoras. [3]

2.4.5. Evitar Riesgos

Para evitar un riesgo, la organización debe estar en capacidad de saber tomar acciones sobre las actividades del negocio, para modificarlas a fin de evitar la ocurrencia del riesgo, para esto se puede: [4]

- No realizar dichas actividades
- Retirar los activos de la zona considerada riesgosa
- Decidir no trabajar con información sensible.

2.4.6. Riesgo Residual

Es el riesgo remanente que existe luego de que se ha analizado los posibles escenarios, sus amenazas y las vulnerabilidades, por eso debe estudiarse también en qué medida las decisiones reducirán el riesgo, así como el riesgo residual que va a quedar. [4]

2.5. AMENAZA

2.5.1. Concepto de Amenaza

Son todos los factores, características o circunstancias que se consideren un factor que en potencia cause un incidente no deseado o que haya declarando intención de hacer daño, es por eso que en el punto anterior se señaló que sin amenazas no hay riesgos. [5]

2.5.2. Orígenes de las Amenazas

Las amenazas pueden provenir de distintos orígenes, es por eso que tenemos:

- Desastres naturales (terremotos, inundaciones, etc.)
- Humanos (falta de personal, error de mantenimiento, errores de usuario, etc.)
- Tecnológico (tráfico sobrecargado, falta de actualizaciones, etc.)
- Amenazas deliberadas (terrorismo, robo, hurto, etc.)

[4] Apuntes Universitarios
[5] VIEITES, Alexis. 2006. Enciclopedia de la Seguridad Informática. Pág. 47

2.6. INCIDENTE DE SEGURIDAD INFORMÁTICA

2.6.1. Concepto

Se refiere a cualquier evento, real o sospechoso que pueda afectar a los sistemas o a las redes de información, por ejemplo, fallos en un sistema bancario, adulteración de información, daños en equipos de cómputo, etc. [6]

2.6.2. Gestión y Manejo de Incidentes

Son medidas que se toman tanto antes, como después de que se ha suscitado un incidente, las primeras son aquellas que ayudan a la prevención ya que proveen guías para mitigar posibles riesgos y sus causas, basándose en un plan de acción, un conjunto de procesos consistentes, medibles, repetibles y de alta calidad, pero que sobre todo, sean entendidos por el personal correspondiente. [6]

Las medidas a tomarse después de suscitado el incidente, se refieren a las fases y sus respectivas tareas que la organización cumplirá, todo esto incluye tres funciones que podrían variar dependiendo de la gestión interna de la organización: reporte del incidente, análisis del incidente y respuesta al incidente.

El reporte del incidente se orienta a realizar la recolección de toda la información relacionada a este para que sea revisada y correlacionada, esto con la finalidad de determinar las tendencias y los patrones de actividad usados para vulnerar la seguridad y llegar al incidente en cuestión, y estar en capacidad de brindar recomendaciones.

El análisis del incidente implica estudiar a profundidad el reporte del paso anterior para determinar el alcance, la prioridad, y la amenaza de dicho incidente, junto con la respuesta posible y estrategias de mitigación.

Respuesta al incidente es hacer recomendaciones para la recuperación, contención y prevención de componentes o sistemas de información y de red, también realizar los pasos propios en los sistemas afectados, además de gestionar el intercambio de

[6] Apuntes Universitarios

información y las lecciones aprendidas con equipos de respuesta y otras organizaciones pertinentes.

2.6.3. Estimación del costo de un incidente

Para la organización, al igual que los activos, los costos pueden ser tangibles e intangibles, los costos tangibles pueden ser cuantificados a manera de disminución de horas de productividad, esfuerzos de investigación y recuperación, pérdida de negocios o de recursos, mientras que los costos intangibles son difíciles de identificar y cuantificar ya que se orientan a daños en la reputación corporativa, pérdida de buena voluntad, daños psicológicos (dependiendo del grado de dureza del incidente), confiabilidad legal y efectos en los accionistas (retiros, represalias, etc.). [7]

2.6.4. Categorías de Incidentes

Los incidentes de seguridad informática pueden provenir de distintos orígenes y pueden causar distinto tipo de daños, es por eso que se los ha categorizado en tres niveles: [7]

2.6.4.1. Nivel Bajo

Son los menos severos de todos los incidentes, se recomienda manejarlos dentro del siguiente día hábil de ocurrido, y pueden ser identificados cuando:

- Hay pérdida de contraseñas del personal
- Se sospecha que se comparte información de la organización
- Existen pruebas fallidas de escaneo a la red
- Hay la presencia de cualquier virus o gusano

2.6.4.2. Nivel Medio

Estos incidentes son más serios, por lo tanto deben ser manejados el mismo día de su ocurrencia, pueden ser identificados cuando:

[7] Documentación Confidencial Auspiciada

- Se viole el acceso a una máquina o a un cuarto de máquinas.
- Se termine la relación laboral con un empleado en malos términos o en enemistad.
- Exista procesamiento o almacenamiento desautorizado de información.
- Si hay destrucción de la propiedad relacionada al incidente, donde el monto límite sea determinado por la administración de la empresa, aunque los expertos de EC-Council en sus cursos de certificación recomiendan que sea menos de $100.000
- Si hay robo de datos relacionados al incidente, cuyo monto, para la administración, es considerable pero no crítico.
- Gusanos o virus de mayor intensidad
- Acceso ilegal a edificios

2.6.4.3. Nivel Alto

Este es el nivel más grave de incidentes, son los más perjudiciales, razón por la cual deben ser manejados inmediatamente hayan ocurrido o hayan sido detectados, se puede presentar:

- Ataques de Denegación de Servicio (DoS)
- Sospecho de vulneración de seguridades
- Virus o gusanos de máxima intensidad
- Cambios en el hardware o software del sistema sin autenticación
- Destrucción de la propiedad o robos de montos críticos para la organización.
- Cualquier tipo de pornografía, apuestas o violaciones a cualquier ley.

2.7. DERECHO INFORMÁTICO

2.7.1. Concepto

Debido al creciente y actual desarrollo de la tecnología, el derecho informático ha sido analizado desde diversas perspectivas. Por una parte, este se define como un conjunto

de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Pero también hay definiciones que establecen que es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales. [8]

En términos generales, el derecho informático es considerado por algunos profesionales del Derecho como un punto de inflexión de este campo, puesto que todas sus áreas así como de casi todas las actividades humanas, se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos. Es aquí donde hace su aparición el derecho informático, no tanto como una rama sino como un cambio.

De manera general, el derecho informático constituye un conjunto de normas, jurisprudencias y doctrinas referidas a la informática en sus múltiples aspectos, además, abarca el estudio de dichas normas, relativas al control y regulación de la informática en dos aspectos:

- Regulación del medio informático en su expansión y desarrollo
- Aplicación idónea de los instrumentos informáticos.

2.7.2. Delito Informático

Delito informático es todo acto malicioso intencional, dependiente de un dispositivo o herramienta electrónica, en definitiva, son delitos en que los medios tecnológicos son el método, el medio o el fin de la conducta delictiva. [9]

Un delito informático además se puede manifestar en dos sentidos: como delito de resultado y como delito de medio.

2.7.2.1. Delito de Resultado

Se refiere a conductas que vulneran los sistemas que utilizan tecnologías de información, es decir, que lesionan el bien jurídico constituido por la información

[8] Universidad de El Salvador. 2000. Trabajo Sobre Delitos Informáticos. Pág. 29
[9] http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico

que los sistemas contienen, procesan, resguardan y transmiten, puesto que la información no es más que el bien que subyace en ellos.

2.7.2.2. Delito de Medio

Delito de medio, recoge las conductas que se valen del uso de las tecnologías de información para atentar contra bienes jurídicos distintos de la información contenida y tratada en sistemas automatizados, esto es, bienes como la propiedad, la privacidad de las personas o el orden económico. [10]

2.7.2.3. Sujeto Activo

Son personas que cometen los delitos informáticos y poseen ciertas habilidades para el manejo de los sistemas y generalmente se encuentran en lugares estratégicos donde se maneja información de carácter sensible, ya sea que tengan o no relación laboral. [10]

A través de diversas experiencias ha sido posible concluir que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos.

Las personas que optan por cometer delitos informáticos tienden a reunir características como: listos, decididos y motivados, además, tienen cierta preparación y conocimientos específicos, lo que exige que sean personas de apreciable nivel cultural y económico, o lo que se conoce como Delincuentes de Cuello Blanco.

2.7.2.4. Sujeto Pasivo

El sujeto pasivo en el caso de los delitos informáticos, pueden ser individuos, instituciones crediticias, órganos estatales, etc., que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. [10]

[10] Universidad de El Salvador. 2000. Trabajo Sobre Delitos Informáticos. Pág. 29

Para labores de prevención de estos delitos es importante el aporte de especialistas junto con los perjudicados ya que pueden ayudar en la determinación de las maniobras usadas por los delincuentes informáticos.

2.7.3. Evidencia Digital

Toda información almacenada o transmitida por dispositivos electrónicos (evidencia electrónica) capaz de relacionar un crimen con la víctima o con el perpetrador con la finalidad de ser recopilada para incorporarla a un proceso judicial a manera de prueba, o también utilizarla para establecer sanciones amparadas en procedimientos propios de la organización, simplemente como evidencia, algunos ejemplos pueden ser: [11]

- Registros generados por el sistema operativo
- Historial de correos electrónicos
- Fotografías digitales
- Documentos digitales
- Historial de navegación de un explorador de Internet
- Historial de documentos recientes
- Resultados arrojados por software de auditoría y software forense
- Reportes de aplicaciones
- Datos precargados en formularios con combos de sitios Web
- Nombres y direcciones de contactos

2.7.4. Informática Forense

2.7.4.1. Concepto

Es la ciencia de capturar, procesar y analizar evidencia digital utilizando una metodología con la finalidad de preservar, identificar, extraer, interpretar y documentar dicha evidencia, bajo reglamentaciones de manejo y mantenimiento de integridad de evidencia, procedimientos legales, forma de reportar la información obtenida, además de proveer una opinión experta en una corte de justicia o en ciertos procesos administrativos. [11]

[11] Documentación Confidencial Auspiciada

2.7.4.2. Objetivos

La informática forense, se enfoca a objetivos claramente definidos que son:

- Recuperar, presentar y analizar material computacional de manera que pueda ser presentado como evidencia en una corte o ante autoridades competentes.
- Identificar la evidencia en un aceptable periodo de tiempo (para la administración)
- Estimar el potencial impacto que la actividad maliciosa causa a la víctima
- Evaluar el intento de intrusión
- Identificar al perpetrador

2.7.4.3. Investigador Informático Forense

Es un profesional de la informática con los suficientes conocimientos y experiencias que le permitan alcanzar los objetivos de la informática forense, apegándose a todas las reglas y consideraciones establecidas para llevar a cabo un proceso investigativo perfecto desde todo punto de vista con la finalidad de que su trabajo sea admisible en una corte de justicia. [12]

Por ser un profesional, el investigador forense debe tener una conducta que lo identifique como tal, ya que esta determinará su credibilidad; incluso la vestimenta dice mucho de él por lo tanto es recomendable que vista formal.

Además, siempre debe mostrar los niveles más altos de ética e integridad moral, así como confidencialidad, siempre debe hablar del caso tratado, solamente con la o las personas que tienen derecho de saberlo.

También un investigador informático forense debe estar preparado para afrontar con todos los obstáculos que puedan presentarse durante la investigación, por ejemplo, tecnología, conflictos con el personal, socios, clientes e inversionistas, disputas comerciales, etc.

[12] Apuntes Universitarios

2.8. EQUIPO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.8.1. Concepto

Grupo de personal capacitado para responsabilizarse de prevenir, recibir, revisar y responder a incidentes informáticos.

Estos profesionales deben trabajar en base a objetivos orientados a gestionar incidentes problemas de seguridad informática, tomando medidas preactivas ante las diferentes vulnerabilidades, y, respondiendo efectivamente ante potenciales incidentes de seguridad, minimizando y controlando daños brindando así respuestas adecuadas que ayuden a la prevención de eventos futuros no deseados. [13]

Debido a que una organización por lo general abarca a un grupo importante de personas que no necesariamente se encuentran en una misma ubicación geográfica, este equipo de repuesta a incidentes, así como todo el personal administrativo debe regularse a estrategias de trabajo que sirven para agilitar los procedimientos de respuesta, de modo que la organización debe contar con un solo punto de contacto para reportar problemas internos para que inmediatamente los especialistas identifiquen y analicen lo sucedido, incluyendo el impacto y la amenaza y proporcionen la respuesta al incidente de manera óptima.

2.8.2. Integrantes

Un equipo de gestión de incidentes debe conformarse de una serie de profesionales distribuidos de la siguiente manera: [13]

- Administrador o líder del equipo
- Asistentes, supervisores o líderes de grupos
- Help desk (Mesa de ayuda – punto único donde se receptan notificaciones de incidentes)
- Administrador de incidentes

[13] http://www.cert.org/cert/information/managers.html

- Administrador de vulnerabilidades
- Personal de análisis de dispositivos
- Especialistas de las distintas plataformas o sistemas operativos
- Capacitadores
- Personal de monitoreo de tecnología
- Personal de soporte
- Documentadores
- Administradores de red y sistemas
- Desarrolladores y programadores (propios del equipo)
- Relacionador público
- Asesor legal
- Auditores o aseguradores de calidad
- Personal de marketing

2.8.3. Servicios que Presta

Los servicios que un equipo de manejo de incidentes informáticos debe prestar se encuentran enmarcados en tres grupos:

2.8.3.1. Servicios Reactivos

Clase de servicios que se desencadenan por un evento o una solicitud, como por ejemplo un reporte de algún cliente, la propagación de un código malicioso, vulnerabilidades de software, y todo lo identificado por los sistemas detectores de intrusos y por los sistemas de validación de accesos. [14]

2.8.3.2. Servicios Proactivos

Este tipo de servicios provee asistencia e información para ayudar a preparar, proteger y asegurar los sistemas y sus componentes para anticiparse a ataques, problemas o eventos. Este servicio reducirá el número de incidentes futuros, este tipo de servicios se enfoca a implementar y publicar normas, políticas y controles de seguridad de información para todo el personal de la organización,

[14] Documentación Confidencial Auspiciada

donde se deben detallen todos los procedimientos de manejo, acceso y responsabilidades del personal para con los activos de información, los equipos donde se almacenan o podrían ser almacenados y todos los medios de acceso posibles tanto físicos como lógicos. [15]

2.9. TÉCNICAS Y DISPOSITIVOS PARA VULNERAR SEGURIDADES DE LA INFORMACIÓN DIGITAL

2.9.1. Intrusiones por Medio de Redes Inalámbricas

2.9.1.1. Concepto

Ataques que pueden ser llevados a cabo utilizando la red inalámbrica de la empresa, por ejemplo, un empleado puede hacer uso de su computador portátil para desde una ubicación cubierta por la señal de la antena sustraer información y transmitirla, incluso, algunas empresas acostumbran a tener varias redes inalámbricas, pero, no todas son aseguradas (asignan direcciones IP en forma dinámica y sin solicitar contraseña) lo cual puede originar que los recursos de la red de la organización sean utilizados por personas no autorizadas.

2.9.1.2. Ataque Pasivo

Un ejemplo claro de un ataque pasivo es el “escuchar” el tráfico de la red, lo cual consiste en, por medio de programas llamados “SNIFFERS” verificar los paquetes que son transportados a través de la red en cuestión.
Son ataques difíciles de detectar, de modo que una manera efectiva de detección sería verificando si existe alguna dirección MAC no autorizada, revisando los archivos logs del DHCP, donde es posible verificar la asignación dinámica de direcciones IP. [15]

La finalidad de los ataques pasivos es simplemente obtener información.

2.9.1.3. Ataque Activo

En caso de que un intruso obtenga la información necesaria por medio de un ataque pasivo, la red será mucho más vulnerable a ataques de DoS, Flood (repetición desmesurada de algún mensaje en un corto espacio de tiempo), MiTM (ataque man-in-the-middle, ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado), etc. [16]

2.9.2. Ataques Mediante Correo Electrónico

2.9.2.1. Concepto

Toda actividad en la cual el correo electrónico es utilizado para propósitos fraudulentos, por ejemplo:

- Spam (Correo Basura)
- Bombardeo de Correo (Saturar buzones de entrada)
- Acoso sexual
- Pornografía infantil
- Envío de información confidencial sin autorización

2.9.2.2. Obtención de Evidencia Digital

Es trabajo técnico conocer las localizaciones donde es posible adquirir evidencia digital que brinden información importante sobre utilización de correo electrónico.

Orientando el análisis a un Explorador de Internet, por si se sospecha el uso de correo comercial (Hotmail, Yahoo, etc.), la evidencia puede ser obtenida a partir de:

[16] Documentación Confidencial Auspiciada

- Cookies
- Favoritos
- Historial
- URLs escritos con anterioridad
- Archivos temporales de Internet
- Caché
- Información que se auto completa en los formularios de las distintas páginas

Además de lo anterior, importante información puede quedar registrada en los archivos de registros del servidor de correo electrónico, en caso de que la entidad utilice uno.

2.9.2.3. Herramientas de análisis forense para correo electrónico

Existen algunas herramientas que pueden ser utilizadas para investigar delitos mediante correo electrónico, aunque su uso dependerá de cada investigador, según su capacidad y su experticia en cada una de estas, además, dependerá también de que si la administración las proporciona; a continuación posibles herramientas especializadas en análisis forense de correo electrónico que podrían ser adquiridas por la gerencia de una organización: [17]

- FTK (Forensic ToolKit)
- FINALeMail
- R-Mail
- Spam Punisher
- E-Mail Examiner

[17] http://www.delitosinformaticos.com/seguridad/clasificacion.shtml

2.9.3. Ataques Mediante Esteganografía

2.9.3.1. Definición de Esteganografía Digital

Es la ciencia que se encarga del estudio y la aplicación de conocimientos con la finalidad de ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia; se lo considera también como una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido. [18]

2.9.3.2. Esteganografía vs. Criptografía

Si bien la Esteganografía suele confundirse con la criptografía, por ser ambas parte de los procesos de protección de la información, son disciplinas bastante distintas, tanto en su forma de implementar como en su objetivo mismo. [18]

Mientras que la criptografía es utilizada para cifrar o codificar información de manera que sea ilegible para un probable intruso, a pesar del conocimiento de su existencia, la Esteganografía oculta la información en un portador de manera que no sea advertido el hecho mismo de su existencia y envío. De esta última manera un probable intruso ni siquiera sabrá que se está transmitiendo información sensible, por un lado, o por otro, el dueño de cierta información no sabrá que esta está siendo fugada.

Sin embargo, la criptografía y la esteganografía pueden complementarse, dando un nivel de seguridad extra a la información, es decir, es muy común (aunque no imprescindible) que el mensaje a esteganografiar sea previamente cifrado; de tal modo que a un eventual intruso no sólo le costará advertir la presencia misma de la mensajería oculta, sino que si la llegara a obtener, la encontraría cifrada.

[18] http://www.kriptopolis.org/esteganografia-doble-uso

2.9.3.3. Uso Inadecuado de Esteganografía

Los siguientes son ejemplos de uso no ético de esteganografía, los mismos que pueden darse en cualquier tipo de organización:

- Comunicaciones criminales
- Fraude
- Sobornos electrónicos
- Apuestas o pornografía digitales
- Acoso
- Ofensas a la propiedad intelectual
- Transmisión de código malicioso

2.9.3.4. Detección de Esteganografía

El investigador forense debe estar familiarizado con los nombres de las distintas herramientas de esteganografía, así como con los términos relacionados, incluso con los distintos sitios que tratan sobre el tema.

Para realizar el análisis, el investigador debe realizar un análisis en el explorador de Internet a nivel de historial, cookies, mensajes de correo, archivos de logs de charlas, así como toda información enviada o recibida por el sospechoso que podría estar asociada a esteganografía.

El análisis de lo anterior, podría proveer evidencia digital que agilite el proceso investigativo, debido a que el análisis a nivel interno de una organización es más factible puesto que se es propietario de toda la infraestructura.

Además existe software que puede proveer información en caso de que llegue a detectar un archivo dentro de otro.

Para detectar esteganografía, existen herramientas como Siego Siute, My Secrets, Pretty Good Envelope, Steganos, etc. [19]

[19] De PLATTINI, Mario. 2007. Gobierno de las Tecnologías y Sistemas de Información. Pag. 47

El investigador debe saber manejar o estar familiarizado con al menos una herramienta de detección de esteganografía, además de tener la habilidad de saber en que tipos de delitos puede el infractor haber utilizado esta técnica, en este caso de estudio, la esteganografía sería una técnica muy útil para fugar información empresarial.

2.9.4. Ataques Mediante PDA

2.9.4.1. Definición de PDA

PDA, del inglés Personal Digital Assistant (Asistente Digital Personal), es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura. Hoy día se puede usar como una computadora doméstica (ver películas, crear documentos, juegos, correo electrónico, navegar por Internet, reproducir archivos de audio, etc.). [20]

2.9.4.2. Análisis Forense de un PDA

Administrativamente, el personal interesado puede formar parte activa en los siguientes pasos, para lo cual no se necesitan conocimientos técnicos de análisis forense ya que el objetivo del Gerente General es brindar facilidades y planificar objetivos, más no hacer el trabajo técnico. [20]

- Asegurar la evidencia: Asegurar físicamente el PDA, sus accesorios y sus tarjetas de memoria externa

- Obtener la evidencia: Crear una imagen exacta del disco del dispositivo para evitar pérdida de información. Además de asegurar y almacenar todos los dispositivos y periféricos, manuales y todos los componentes aunque estén dañados.

[20] Documentación Confidencial Auspiciada

- Examinar la evidencia: Indagar en los datos digitales, buscando datos o aplicaciones sospechosas, algunas fuentes de evidencia pueden ser el dispositivo, su cable de electricidad y demás dispositivos periféricos asociados a este.

- Presentar la evidencia: Documentar los resultados , para esto es necesario grabar todos los datos visibles, todos los identificadores del dispositivo (número de serie), además deben constar fotografías de todos los componentes de hardware, una descripción del estado del equipo mientras duró la investigación, siempre manteniendo la documentación en un sitio seguro.

- Mantener la evidencia: Mantener el equipo en un lugar seguro, siempre asegurándose de mantenerlo con baterías cargadas, lo importante es evitar que se apague.

Además es recomendable que un administrador tenga conocimientos básicos de manejo de este tipo de equipos con la finalidad de no entorpecer el análisis, por ejemplo:

Si el equipo está encendido:

- Mantener el equipo siempre con la batería cargada o conectado a la corriente
- Tomar una fotografía del equipo

Si el equipo está apagado:

- Dejarlo apagado
- Conectarlo a la corriente
- Fotografiarlo

Si el equipo está sincronizado con un PC (conectado):

- Evitar todo tipo de comunicación a partir de ese momento
- Desconectar el cable USB (o la conexión Serial) del computador
- Incautar el computador

Si está comunicado con una red inalámbrica:

- Evitar toda comunicación desde ese momento
- Guardar el equipo en una bolsa antiestática para eliminar posibilidades de que se vuelva a conectar a dicha red
- Sacar tarjetas de red inalámbricas

Si el equipo tiene acceso ranura de tarjeta de expansión de memoria:

- No hacer ninguna actividad dentro del equipo
- No quitar ninguna tarjeta ni periférico

Si no existe ranura de tarjeta de expansión:

- Incautar todos los dispositivos periféricos

Además de tener conocimientos elementales, un gerente también debe conocer al menos los nombres de ciertas herramientas que pueden ser de utilidad para apoyar al equipo de análisis, por ejemplo PDA Secure o Encase.

2.9.5. Ataques Mediante IPOD

2.9.5.1. Definición de IPOD

Dispositivo digital para reproducción de archivos multimedia, podría ser catalogado como un dispositivo de almacenamiento parecido a una memoria

extraíble o a un disco duro portable con una capacidad mayo los 60 Gb, de manera que un usuario puede almacenar: [21]

- Música con formato MP3.
- Fotografías o imágenes.
- Respaldos archivos.
- Direcciones, teléfonos y demás datos de contactos.
- Incluso para jugar videojuegos.

2.9.5.2. Análisis Forense de un Ipod

La Gerencia General, adecuadamente asesorada por personal técnico, debe asegurar la recolección de la evidencia, que se documente un informe descriptivo del dispositivo, se cree y se analice una copia exacta de la información contenida en este, además de tomar fotografías del sitio, así como del equipo.

Además, es necesario saber que cuando un Ipod se encuentre conectado a un computador, debe ser desconectado ademadamente, una vez desconectado debe ser almacenado adecuadamente en una bolsa antiestática identificando como "Evidencia", sin acercarlo a objetos magnéticos ya que podrían dañar la evidencia digital.

Una vez obtenida la evidencia física, es necesario realizar un análisis de laboratorio para obtener evidencia digital, el mismo que consiste en dejar constancia documentada de las características del computador o computadores que son enviados al laboratorio junto con el iPod para investigaciones, además, se obtienen copias del disco del Ipod. Todo lo anterior se realiza con la finalidad de vincular cualquier evidencia digital sospechosa encontrada tanto en el Ipod como en los computadores incautados y asociarlas a posibles usuarios.

[21] en.wikipedia.org/wiki/IPod

Para tratar físicamente a los equipos, así como su extracción de la bolsa antiestática, es necesario documentar y fotografiar el proceso, una vez encendidos hay que asegurarse que la batería se encuentra cargada.

Hasta lo especificado anteriormente, en ciertos casos y dependiendo del tipo de investigación, podrá estar involucrado personal de la administración ya que no existen aspectos técnicos de alto nivel, pero a partir de este punto el investigador hará uso de su conocimiento en herramientas de análisis forense para continuar con la investigación, pero, de igual forma la gerencia debe asegurarse de proporcionar al profesional todas las facilidades así como las herramientas de trabajo, como por ejemplo, EnCase, Recover My Ipod y Disk Internals Music Recovery

2.9.6. Ataques Mediante Blackberry

2.9.6.1. Definición de Blackberry

Es un dispositivo portátil inalámbrico introducido en 1999 que admite correo electrónico, telefonía móvil, mensajería de texto, navegación en Internet y otros servicios de información inalámbricos. Fue desarrollado por una compañía canadiense, Research In Motion (RIM), y transporta la información a través de las redes de datos inalámbricas de empresas de telefonía móvil, no es un teléfono celular. [22]

Este equipo puede funcionar a manera de:

- Dispositivo de envío y recepción de mensajes de texto.
- Teléfono celular.
- Dispositivo de acceso a redes inalámbricas.
- Módem
- Organizador
- Equipo de acceso a datos corporativos (correo y archivos)

[22] en.wikipedia.org/wiki/BlackBerry

2.9.6.2. Análisis Forense de un Blackberry

La forensia en equipos BlackBerry, ha redimensionado las investigaciones forenses en equipos PDA, debido a que tradicionalmente un PDA requiere ser sincronizado con un computador, mientras que un BlackBerry puede ser sincronizado vía inalámbrica.

Una vez encendido el BlackBerry, los archivos que se encuentran en espera serán enviados desde el computador inmediatamente.

Para obtener evidencia digital de un BlackBerry, es necesario recolectar los archivos de registro directamente del equipo, aunque esto viola una de las reglas del investigador, la cual consiste un nunca trabajar en el equipo directamente sino en una copia exacta de su disco. El motivo por el cual se obtienen los logs directamente del dispositivo, es que una vez hecha la copia, los logs son limpiados automáticamente. [23]

Una vez obtenidos los logs, se saca una copia exacta del disco del dispositivo.

Algo que debe considerarse al momento de analizar un BlackBerry, es que este tipo de dispositivo tiene características como bases de datos ocultas, espacios entre particiones y datos ofuscados, o sea, los datos podrían ser almacenados entre las particiones del sistema operativo y los espacios sobrantes luego de haber instalado las aplicaciones.

2.9.7. Ataques Mediante Ingeniería Social

2.9.7.1. Concepto de Ingeniería Social

La ingeniería social básicamente es una habilidad utilizada por un individuo, orientada a relacionarse con personas que conozcan cierta información, con la finalidad de adueñarse de esta y utilizarla en beneficio propio. [23]

[23] Documentación Confidencial Auspiciada

2.9.7.2. Prevención de Ataques de Ingeniería Social

Lamentablemente, no existen técnicas ni herramientas que ciertamente funcionen para contrarrestar este tipo de ataques, motivo por el cual es responsabilidad de las altas gerencias conocer y mantener informados a los empleados sobre esta modalidad, ya que fácilmente podrían ser influenciados, sea por amistad, intimidación, cargo que ocupan en relación al intruso, etc.

La base en este caso es la capacitación, ya que el punto clave en este tipo de ataques no es llegar a la información, sino a la persona que la posee o posee los medios para llegar a esta.

2.10. TÉCNICAS Y PROCEDIMIENTOS FORENSES

2.10.1. Aseguramiento de la Evidencia Digital

Es un proceso mediante el cual toda la información contenida en un equipo informático y cualquier dispositivo capaz de almacenar información digital es recuperada con el objetivo de ayudar en la investigación, a manera de que de esta forma no se comprometerán los datos originales. [24]

Es importante que al examinar, el investigador y todos sus colaboradores siempre trabajen de acuerdo a las “Mejores Prácticas”, ya que, en caso de no hacerlo podrían dar cualquier evidencia de fraude o de abuso inusual en los procedimientos subsecuentes.

Para lograr lo anterior, la administración de la organización que ha sufrido de fuga de información empresarial, debe asegurarse que el personal que investigará el delito tenga las capacidades profesionales adecuadas y suficientes, que disponga de un laboratorio para el manejo de los datos y de la evidencia, que trabaje bajo una metodología de trabajo, y que siempre exista una autoridad competente que vele por el proceso.

[24] DE SOLER, Joan. 2008. Preservación de los Documentos Electrónicos. Pág. 67

Una metodología podría abarcar los siguientes aspectos: [25]

a) Relevamiento del caso
b) Preparación de un diseño detallado
c) Determinación de los recursos que serán necesarios
d) Identificación de todos los riesgos envueltos en el caso
e) Recuperar la evidencia digital y analizarla
f) Documentar resultados
g) Exponer los resultados

Con todo lo anterior, la evidencia tanto física como digital no estará bajo riesgos significativos durante todo el proceso investigativo.

2.10.2. Preparación para la Recolección de Evidencia

Aunque un gerente general puede no tener los suficientes conocimientos técnicos para encabezar algunas actividades, es responsabilidad de él saber rodearse de gente capacitada y de confianza.

Todo delito informático necesariamente debe ser ejecutado mediante un equipo o dispositivo electrónico, de modo que, sin importar como se está gestionando la investigación, siempre, antes de incautar cualquier computador o dispositivo informático, es importante determinar si dicho equipo o alguna de sus partes, así como sus sistemas son factores preponderantes para determinar el rol del computador en el delito, por ejemplo, usualmente personal que fugaría información confidencial fuera de la compañía, tendría que utilizar su equipo de trabajo para hacerlo, ya que este sería la ruta de acceso a la información de la empresa.

Para el proceso de recolección de evidencia digital, se requieren los siguientes pasos:

- Buscar la evidencia
- Identificar la evidencia
- Determinar datos relevantes

[25] Documentación Confidencial Auspiciada

- Agruparlos en orden de volatilidad
- Eliminar toda posibilidad de influencia externa que genere riesgos de alteración
- Recolectar la evidencia
- Documentar los resultados

Además, toda la evidencia física del delito debe pasar (de darse el caso) por una cadena de custodia, en la cual, bajo un procedimiento definido se establezcan responsabilidades de todos los movimientos de dicha evidencia, indicando lugar a donde se encuentra, lugar a donde se dirige y todas las formas de responsabilidad.

En lo que corresponde al traslado y manipulación de la información, la cadena de custodia es una técnica de identificación de todos los individuos que han manipulado la evidencia por medio de un documento que contiene entre otros aspectos firmas de responsabilidad; un formato de documento de traslado de evidencia (cadena de custodia) podría ser: [26]

Fecha Investigación:	Tipo de Incidente:	Id. Caso:
EVIDENCIA		
No. Serie:	Descripción del Dispositivo:	
Modelo:		
CADENA DE CUSTODIA		
Lugar de origen	Lugar de destino	Razón de traslado
Firma Encargado	Firma Encargado	Fecha:
Lugar de origen	Lugar de destino	Razón de traslado
Firma Encargado	Firma Encargado	Fecha:
Lugar de origen	Lugar de destino	Razón de traslado
Firma Encargado	Firma Encargado	Fecha:
Lugar de origen	Lugar de destino	Razón de traslado
Firma Encargado	Firma Encargado	Fecha:
Situación Final de la Evidencia:		

Ejemplo de Formato de Formulario de Custodia de Dispositivos

[26] http://www.delitosinformaticos.com/seguridad/custodia.shtml

2.10.3. Proceso de Investigación Forense

El proceso investigativo forense, podría ser ejecutado por un equipo de especialistas contratados por la empresa, aunque, en caso de que esta haya optado por dar parte a las autoridades judiciales competentes, será el Ministerio Público el que se encargue de la investigación.

A continuación, se describen cinco tópicos que resultan necesarios para conducir una investigación informática forense a la interna de la empresa:

2.10.3.1. Desarrollo de Políticas y Procedimientos

Se refiere a establecer parámetros y procedimientos que guiarán las operaciones del equipo de investigación, es una parte muy importante en el proceso de creación de una unidad de investigación de delitos informáticos. [27]

En este punto se detallarán las funciones núcleo, las mismas que harán referencia a la investigación de crímenes tecnológicos, recolección de evidencia y análisis forense.

Un punto muy importante es que la evidencia original nunca debe ser utilizada para desarrollar procedimientos.

2.10.3.2. Evaluación de la Evidencia y del Caso

La evidencia digital debe evaluada con respecto al ámbito del caso, para así determinar el curso de la investigación, esto abarca actividades tales como garantías y autorizaciones legales, naturaleza del hardware y software, determinación de evidencia potencial y de todas las circunstancias que rodean a la adquisición de la evidencia. [27]

Además de evaluar los aspectos mencionados anteriormente, es necesario que el investigador realice una evaluación del ambiente en el cual resolverá el caso, debe determinar aspectos como:

[27] Documentación Confidencial Auspiciada

- Autoridad legal que dispone para hacer todos los requerimientos necesarios en su investigación.
- Asegurarse que dispone de todo el apoyo de la administración de la entidad.
- Determinar su equipo de trabajo, el cual no necesariamente debe estar constituido solamente por personal técnico.
- Solicitar autorización para obtener información de fuentes externas (proveedores de Internet, especialistas en estudios de huellas digitales, etc.)
- Considerar la relevancia de componentes ajenos a la propiedad de la entidad escáneres, cámaras fotográficas, etc.

2.10.3.3. Adquisición de la Evidencia

Debido a que la evidencia digital es muy natural, esta es frágil y puede ser alterada, dañada o destruida debido a manipulación o examinación inapropiada; en caso de que la evidencia sufra algún tipo de alteración es posible que la investigación se vea interrumpida o que los resultados obtenidos sean erróneos. [28]

Lo más importante en este punto es duplicar toda la información digital de los equipos obtenidos como evidencia física en equipos propios y exclusivos del laboratorio.

Otra fuente de información, podrían ser los mismos empleados de la empresa, motivo por el cual, el investigador debe tener la capacidad de poder determinar a quien se entrevistará, en base a los conocimientos adquiridos del paso anterior.

2.10.3.4. Examinación de la Evidencia

Al momento de examinar la evidencia digital, es necesario aplicar principios generales de forensia, técnicamente, este punto depende íntegramente del especialista puesto que hará uso de herramientas de análisis forense, debido a

[28] Documentación Confidencial Auspiciada

que se obtuvieron copias de toda la evidencia, la examinación debe hacerse sobre las copias, mas no sobre la evidencia original. [29]

2.10.3.5. Documentar y Reportar Resultados

A lo largo del proceso investigativo, se requiere acumular la siguiente documentación: [29]

- Notas tomadas durante el proceso investigativo.
- Documentación de solicitudes de asistencia de especialistas durante la investigación.
- Copias de la documentación generada por la cadena de custodia.
- La suficiente cantidad de documentación que permita conocer lo que se realizó en cada una de las actividades del análisis forense, incluyendo fechas, responsable, trabajo realizado y resultado obtenido.
- Documentación donde se detalle cualquier irregularidad ocurrida durante la investigación.
- Incluir documentación técnica, de darse el caso, como pueden ser diagramas de red, listados de usuarios de una aplicación determinada, etc.
- Documentación referente al sistema operativo (versión instalada, parches, antivirus).
- Descripción detallada de toda la información entregada al investigador (que no sea considerada como evidencia, sino que sea utilizada para realizar otro tipo de análisis tales como el de usuarios del sistema)

A más de los documentos anteriores, es necesario presentar un informe final, el cual debería contener como parte de su contenido: [29]

- Identificación detallada del caso en cuestión.
- Fecha en la que ocurrió el incidente.
- Fecha en la que el incidente fue reportado.
- Identificación detallada de todos quienes reportaron el incidente.
- Fecha en la cual el incidente fue asignado a los investigadores.

[29] Documentación Confidencial Auspiciada

- Descripción detallada de los archivos examinados.
- Descripción detallada de toda la evidencia digital analizada.
- Descripción detallada de todo lo que se observó durante la investigación, especialmente las anomalías
- Materiales de soporte.
- Glosario de términos
- Conclusiones.

En términos generales, otra información que podría agregarse al informe final podrían ser datos del responsable del delito, así como de qué, cómo, cuándo y dónde se dio el mismo. En este punto es necesario indicar que si la empresa no cuenta con políticas robustas, será muy complicado establecer responsabilidades.

2.10.4. Primer Procedimiento de Respuesta

El Primer Procedimiento de Respuesta, es lo que la organización debe hacer apenas ha descubierto un fraude informático, con la finalidad de la evidencia permanezca íntegra y no sufra daños por manipulación o acción de personal mal o bien intencionado. [30]

Lo primero que los jefes de la empresa deben asegurar al momento de detectar el delito, es mantener alejado de la escena a todo el personal ajeno o inadmisible dependiendo de que si se tomarán acciones legales o administrativas.

Haciendo referencia a la segregación de funciones que en toda organización debe existir, los responsables serían:

- Administradores del Sistema
- Administradores de la Organización
- Analistas forenses

Las acciones tomadas por los administradores de los sistemas envueltos en el delito, serán de vital importancia en la investigación; una vez que el administrador ha

[30] VIEITES, Alexis. 2006. Enciclopedia de la Seguridad Informática. Pág. 132

detectado un fraude, debe reportarlo inmediatamente siguiendo el procedimiento de reporte de incidentes con el que cuenta la entidad, o en su defecto, contactándose con sus superiores.

Una vez que el administrador del sistema ha reportado el incidente, no debe manipular el sistema, los únicos autorizados para hacerlo, son el Encargado de la Investigación o uno de sus subordinados.

Por otro lado, los Administradores de la Organización y el personal ajeno al área de tecnología o a la aplicación sujeto de fraude, debe mantenerse alejados de la escena; es responsabilidad de los jefes encargarse de que el personal no traspase los límites físicos del delito, de manera que no basta con asegurar el computador y sus sistemas, sino todo el ambiente físico donde estos se encuentran.

El primer procedimiento que debe ser ejecutado por el equipo de investigadores (internos, a nivel administrativo), se enfoca en asegurar y evaluar la escena del crimen, planificar entrevistas iniciales (obtener firmas de quienes comparten información, relevamiento de información, tomar fotografías, etc.), documentar la escena del crimen, obtener evidencia física y digital, empacarla y transportarla al laboratorio donde será analizada.

2.10.5. Testigo Experto

Un testigo experto, es un testigo que por virtud de su educación, profesión o experiencia tiene conocimiento especial o relevante en un asunto determinado en relación a otra persona, de manera que, legalmente es posible llegar a depender de su opinión. [31]

Un testigo experto es una persona que investiga un crimen, evalúa la evidencia, educa al público y a los interesados en los resultados de la investigación y está capacitado para testificar de manera compresible ante autoridades competentes.

[31] http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico

Pueden haber varios tipos de testigos expertos, por ejemplo, experto en informática forense, experto en medicina y psicología, experto en legislación civil, experto en construcción y arquitectura y expertos el litigios criminales.

Las declaraciones de un técnico frente a las de un experto, se diferencian en el ámbito del conocimiento, en las conclusiones que presenta, en la responsabilidad como profesional y en la preparación para exponer su trabajo adaptándose al tipo de auditorio.

Una de las cualidades del testigo experto, y, dependiendo de la organización donde se ha efectuado el delito, es saber tratar con los medios de prensa, motivo por el cual es importante que el equipo investigador se mantenga alejado durante todo el proceso investigativo debido a que nunca existe la seguridad acerca de lo que la prensa puede publicar, algunos comentarios podrían influenciar sobre el caso o las declaraciones pueden tornarse en contra del investigador, en caso de ser abordado por reporteros, debe ser muy cauto en sus declaraciones evitando comentar sobre los implicados o sobre las autoridades que trabajan en el caso.

3. ANÁLISIS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. INTRODUCCIÓN

El principal objetivo de la seguridad informática es proteger mediante medidas de prevención, monitoreo y recuperación los datos, la información y todos los procesos de obtención y gestión de la misma, así como todo lo que directa o indirectamente se relaciona con ella, tales como, personal, equipos, dispositivos de almacenamiento, etc., además de gestionar todos los riesgos relacionados con cada uno de estos, que puedan vulnerar a los activos de información digital, por ejemplo, un empleado con falta de capacitación o el uso de equipos obsoletos.

Un adecuado proceso de análisis de dichos riesgos brinda como resultado final un plan de tratamiento del cada riesgo, que contemplará detalladamente todas las actividades necesarias para poder asignar responsabilidad a individuos, saber de los recursos necesarios, posibles obstáculos, formas de monitoreo y los entregables, además, brindará una perspectiva que permita el establecimiento de controles para mitigar cada riesgo identificado.

Aunque una organización identifique y trate a cada riesgo asociado con los elementos del sistema de seguridad de la información, es posible que sucedan incidentes, lo cual básicamente indica que una amenaza se aprovechó de una vulnerabilidad, en este caso, es necesario tomar medidas correctivas.

Los encargados de la seguridad de la información deben realizar tareas periódicas que permitan detectar incidentes, algunas técnicas recomendables son:

- Implementar una alarma de una herramienta de detección de intrusos, que indique una alerta de seguridad.
- Verificar entradas sospechosas a la red.
- Verificar intentos de autentificación fallidos.
- Validar a los nuevos usuarios o nuevos archivos injustificados.
- Buscar alteraciones injustificadas de archivos de sistema.
- Buscar modificaciones o eliminaciones injustificadas de datos.
- Monitorear actividades que se encuentran fuera de los permisos concedidos según el perfil de los usuarios.

3.2. CONTROLES DE SEGURIDAD DE INFORMACIÓN DIGITAL

El éxito o fracaso de un sistema de seguridad de información digital, depende de la implementación y eficacia de controles, ya que estos están orientados a mitigar los riesgos que pueden afectar a los activos de información digital.

Todo sistema de seguridad de información debe contar con controles técnicos y con controles administrativos, ya que algunas actividades pueden controlarse automáticamente, por ejemplo, utilizando contraseñas, asignando cuentas de usuario restringidas, bloqueando accesos a ciertos sitios de Internet o utilizando lectores biométricos, mientras que otras actividades deben ser reguladas por políticas, por ejemplo, para la utilización de equipos y dispositivos tanto de la empresa como de uso personal, para el uso apropiado de información a la cual cada empleado tiene acceso, para obtener respaldos periódicos de información sensible, etc.

Una adecuada gestión de un sistema de seguridad de información, implica evaluar periódicamente los controles que han sido implementados, con la finalidad de determinar su eficacia operativa, lo cual permitirá conocer si existe alguna falla en el diseño del control o en el personal que debe cumplir con el mismo.

La parte más importante y crítica, está en el establecimiento de controles internos, ya que es aquí donde se deben contemplar todos los componente físicos y lógicos relacionados con el almacenamiento y custodia de la información, por ejemplo, políticas internas de

accesos físicos, de traslado de equipos, de posesión de dispositivos, de horas de trabajo, de visitas de personas externas, de mantenimiento a equipos, de funciones y responsabilidades, además de técnicas de seguridad lógica, tales como, configuración de parámetros de las políticas de seguridad de las distintas plataformas existentes (AS400, Windows, AIX, etc.), contraseñas de acceso, identificadores únicos de usuario, gestión de usuarios, autorización de accesos (físicos y lógicos), seguimiento y monitoreo del estado de los accesos a las aplicaciones y equipos, adecuada segregación de funciones, etc.

3.3. ANÁLISIS DIGITAL FORENSE

La informática forense, como parte de la seguridad informática, ha ido evolucionando como rama formalmente adoptada por varios profesionales de la computación, debido a los beneficios que puede presentar para cualquier organización ya que en caso de detecciones de delitos informáticos, toda la evidencia encontrada puede ser utilizada con la finalidad de hacerla actuar en defensa de la empresa en caso de cualquier controversia legal, o en caso de un incidente mayor, se puede realizar una investigación rápida y eficiente cuyas acciones interrumpan de forma mínima al negocio haciendo que el análisis del delito pase de forma desapercibida tanto para clientes como para empleados, además de extender el objetivo de seguridad de información a un campo más amplio que la fuga de información, por ejemplo protección a la propiedad intelectual, protección ante fraudes corporativos, extorsión, acoso, apuestas, pornografía infantil, etc. [32]

3.3.1. Defectos y Riesgos

La informática forense en el Ecuador se encuentra en una etapa de desarrollo, motivo por el cual se encuentran algunas complicaciones, ya que se requiere algunas veces que el personal sea capacitado fuera del país, además, difiere de otras ciencias forenses en la forma de examinar la evidencia.

Para algunos profesionales de la informática, existe carencia de entrenamiento apropiado, lo cual implica una falta de estandarización de herramientas y en las metodologías de trabajo, lo cual ha generado que a nivel local sea complicado

[32] De PLATTINI, Mario. 2007. Gobierno de las Tecnologías y Sistemas de Información. Pág. 118

encontrar capacitación económicamente accesible para profesionales sin auspicio corporativo.

Los riesgos de no tener el personal capacitado tanto en cantidad como en calidad, podría generar falsos e incorrectos resultados en los distintos análisis que se realicen, además de complicaciones al momento de realizarlos, ya que podrían existir problemas de inexperiencia en el uso de determinadas herramientas, fallas en la interpretación de resultados, etc.

3.3.2. Consideraciones ante Delitos Informáticos

La Gerencia General de una organización, sin necesidad de tener conocimientos técnicos, puede estar en capacidad de conocer ciertos lineamientos que le permitan tener una acertada gestión de un proceso investigativo, de modo que esté en capacidad de buscar la asesoría adecuada para minimizar al máximo opciones de examinar evidencia original, con la finalidad de exponerla a la menor manipulación posible, obteniendo copias de la información almacenada en los equipos a analizarse, además, un gerente administrativo debe asegurarse que el equipo investigador manipule todas las evidencias digitales adecuadamente, sin alterarla, utilizando cadenas de custodia y documentando todo el proceso, tanto técnica como ejecutivamente.

Las organizaciones, dependiendo de su tamaño y reputación ganada, muchas veces optan por no dar parte en caso de haber sido víctimas de ataques informáticos, por no perder el espacio ganado ante sus clientes y ante la competencia, es por esto que en el país se tiene poca madurez en este tema, y no existe jurisprudencia ya que en algunos casos se opta por investigar y si se da el caso sancionar pero a nivel interno de la organización.

Un crimen informático, como cualquier otro crimen debe ser reportado a la autoridad competente, puede ser administrativa, legal local o legal internacional, dependiendo del ámbito del crimen y de la organización.

En caso de que una organización sea víctima de algún delito informático, la Gerencia General debe estar consciente de que existen varias razones para reportarlo, por

ejemplo, se puede compartir información referida al impacto en el negocio y a la sensibilidad de los datos a organizaciones semejantes para recibir asesoría y apoyo ya que solamente compartiendo información se puede identificar y procesar criminales, identificar nuevas formas de seguridad y prevenir futuros ataques, además existe mayor oportunidad de conocer y aprender de personal experimentado en el área, lo importante es saber que la capacidad que la ley tiene para procesar ataques informáticos, está directamente relacionada con la cantidad de ataques reportados.

Otro aspecto que la Gerencia General de una organización debe conocer es que si se ha detectado un ataque y se ha decidido optar por la vía judicial, es necesario inmediatamente contactar a la persona en la agencia legal competente y a la persona encargada dentro de la organización para que estos indiquen los procedimientos judiciales a seguir.

La información inicial que se debe proveer a quien investigue el caso es: [33]

- Que sistemas principales están siendo usados
- Como se cree que el ataque fue llevado a cabo
- Que se ha hecho hasta el momento para mitigar o remediar el ataque
- Indicar si existe algún sospechoso, y si es interno o externo
- Que evidencia se tiene disponible para ayudar en la investigación

Una vez reportado el crimen, mientras está siendo procesado, dependiendo de la etapa en la que se encuentre, la organización puede solicitar información acerca de su caso al respectivo responsable.

Finalmente, es necesario indicar que en caso de que en una organización se detecte un delito informático, es posible tomar una de las siguientes dos alternativas:

La primera, acudiendo a la autoridad competente (Ministerio Público), para que, este se encargue del proceso investigativo, partiendo desde la respectiva denuncia apoyada tanto en el profesional del derecho como en el profesional informático, culminando en el establecimiento de responsabilidades y sanciones a nivel judicial.

[33] Universidad de El Salvador. 2000. Trabajo Sobre Delitos Informáticos. Pág. 160

Otra forma de enfrentar un proceso investigativo, es siguiendo un procedimiento a nivel interno de la organización, contratando un equipo de profesionales calificado en informática forense con la finalidad de que sean ellos quienes obtengan toda la evidencia digital de manera adecuada, guiándose en los procedimientos indicado en este mismo capítulo, para que, posteriormente con el aval de un perito informático esta pueda ser utilizada como evidencia en una corte de justicia, o en su defecto, sea posible establecer responsabilidades y sanciones a nivel corporativo. [34]

Al hablar de un equipo de profesionales calificado, puede haber distintas opciones ya que es posible encontrar desde profesionales que trabajan por su cuenta, hasta firmas multinacionales con laboratorios forenses y equipos completos de investigadores certificados y especializados en distintas ramas de la seguridad de la información.

El hecho de escoger una u otra de las alternativas indicadas, depende mucho de la capacidad de gestión de los niveles dirigenciales, ya que debido a la idiosincrasia e inmadurez en este tema, en el Ecuador puede significar pérdida de imagen y credibilidad de la organización, así como florecimiento de desconfianza por parte de los clientes, dependiendo de qué tan público el caso llegue a ser, razón por la cual, considerando el tamaño, popularidad y naturaleza de la organización en cuestión, es sumamente importante saber tratar con personas externas, ya que, no es lo mismo que una institución educativa haya sufrido un ataque de penetración en donde se hayan alterado calificaciones de los estudiantes, a un ataque en una entidad bancaria donde se sustrajo dinero de los clientes, simplemente sus secuelas a nivel externo no serían de las mismas dimensiones.

3.4. EJEMPLOS DE DELITO SEGÚN EL MEDIO DE EJECUCIÓN

3.4.1. Ejemplo de Ataque por Medio de Redes Inalámbricas

Un ex empleado de una empresa que cuenta con tecnología que le permita el acceso a redes inalámbricas, se acerca con un equipo portátil hasta el lugar de cobertura y haciendo uso de sus datos de autentificación, sustrae datos confidenciales o causa daños a la empresa alterando o eliminando información.

[34] Apuntes Universitarios

En el ejemplo se pueden determinar fallas en la seguridad, por ejemplo, una inadecuada gestión de usuarios de los recursos (bajas de personal), además de redes desprotegidas.

Al momento de optar por la investigación del incidente, la Gerencia General de la organización debe apoyarse en un equipo técnico especializado y certificado en investigaciones sobre redes inalámbricas, así como de prestar todas las garantías para que este equipo investigador se encargue de realizar su trabajo. Técnicamente hablando, algunas actividades principales del equipo investigador son prestar especial atención a los archivos de eventos (logs) generados por el protocolo DHCP al asignar direcciones IP a las direcciones MAC, también a los logs a nivel de firewall, así como de logs generados en el access point acerca del tráfico de la red.

3.4.2. Ejemplo de Delito de Fuga de Información mediante correo electrónico y esteganografía

Simplemente, copiando datos o adjuntando archivos confidenciales a un mensaje de correo electrónico y enviándolo a personas no autorizadas. Generalmente los altos mandos o sus asistentes tienen acceso más que a los servidores de la empresa, a simples documentos donde se detallan aspectos empresariales (planes de marketing, información de clientes, etc.) que pueden ser perjudiciales en caso de ser vistos por terceros, por ejemplo, un Jefe de Recursos Humanos que envía mediante correo electrónico datos de la nómina a una empresa competidora con la finalidad de que traten de convencer a los empleados para que opten por un cambio de empleo basándose en un incremento salarial. Utilizando esteganografía, podría realizarse el envío de la información confidencial oculta bajo una fotografía.

3.4.3. Ejemplo de delito utilizando PDA

Un funcionario que trabaje con un PDA y que además tenga acceso a recursos de información confidencial, podría hacer copias de estos en el dispositivo y sacarlos de la organización con la finalidad de transmitir tantas copias como le parezca.

3.4.4. Ejemplo de delito utilizando un BlackBerry

Debido a las posibles formas de establecer un enlace entre un BlackBerry y un computador (USB o Bluetooth), es posible pasar información de un equipo a otro, lo cual, agregado a que actualmente en el Ecuador las empresas entregan a sus directivos este tipo de dispositivos, provoca mayores riesgos considerando que por lo general a nivel interno de la empresa no se regula su utilización, por lo tanto existe una gran probabilidad de que los funcionarios que poseen este tipo de equipos copien la información y la trasladen a cualquier parte, pudiendo transmitirla a cualquier persona, sin ningún tipo de restricción.

3.4.5. Ejemplo de delito utilizando Ingeniería Social

Esta técnica, puede llegar a abrir muchas posibilidades de ser víctima de fraudes, por ejemplo, relacionarse con la secretaria de uno de los gerentes, la misma que conoce cierta información relacionada a la seguridad por ejemplo, claves de acceso, horarios de turno del personal de vigilancia, etc., dicha secretaria puede incluso a veces llegar a ser ingenua y revelar información hasta de manera inconsciente, gracias a las habilidades del intruso.

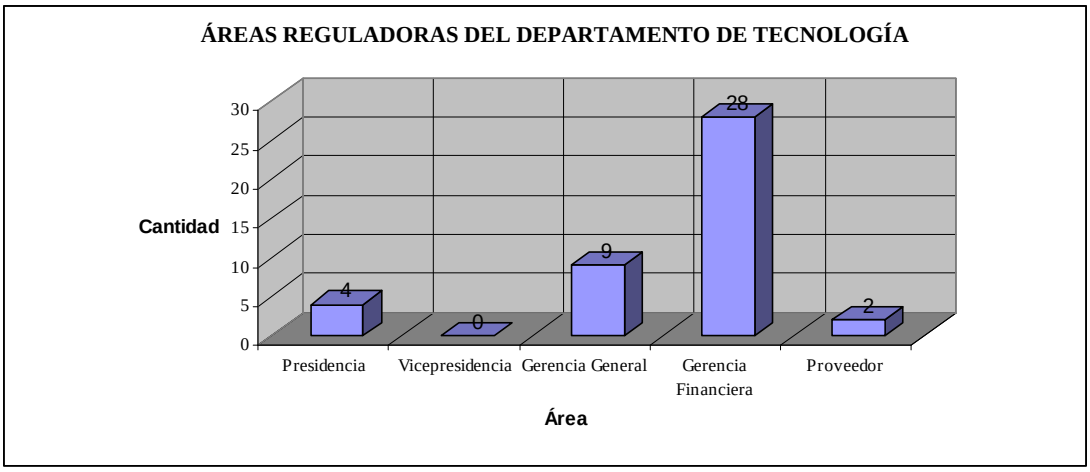
Incluso la ingeniería social puede llegar a darse entre personal de una misma organización, o con ex empleados, por ejemplo, es común que después de tiempo de haber trabajado en una organización, el personal de seguridad conozca a un funcionario, quien que después de haber terminado su relación laboral regrese a la empresa sin llamar la atención del los guardias con la finalidad de acceder de manera maliciosa a ciertos recursos.

3.5. ANÁLISIS ACTUAL DE LA UBICACIÓN JERÁRQUICA DE LOS DEPARTAMENTOS DE TECNOLOGÍA EN LAS EMPRESAS DEL ECUADOR

El presente tema de investigación se encuentra dirigido a satisfacer necesidades técnico administrativas de las Gerencias Generales en lo relacionado al aseguramiento de la

información digital de la organización, pero, como resultado de haber encuestado a auditores de sistemas, se concluyó que la tendencia en las empresas nacionales está orientada a que administrativamente los Departamentos de Tecnología sean subordinados de otros departamentos. (Referirse a Anexo 1)

A continuación los resultados de las encuestas que proporcionaron datos de una población de cuarenta y tres empresas de la ciudad de Quito, algunas de las cuales operan a nivel nacional:

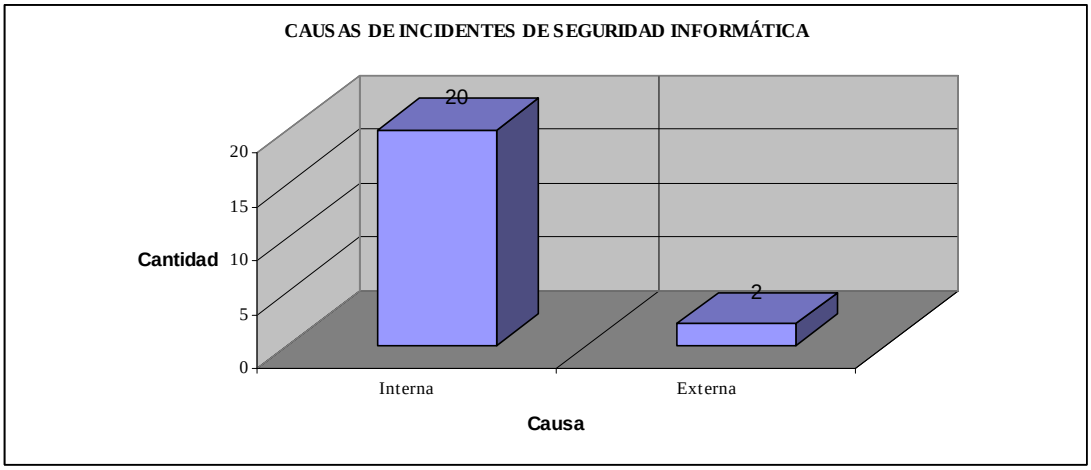


FUENTE: Datos Obtenidos de Encuestas (Anexo 1)

Con estos primeros resultados obtenidos en las encuestas, se determinó que administrativamente las organizaciones no le dan al Departamento de Tecnología el sitial adecuado dentro del organigrama, lo cual se deriva en que personal que no tiene conocimiento técnico, sea el encargado de gestionar áreas que están fuera de su competencia.

3.5.1. Análisis de Incidentes de Seguridad de Información Digital

Otro aspecto consultado a los especialistas, fue el relacionado a incidentes de seguridad de la información, a partir de lo cual se determinó que de las cuarenta y tres empresas, veinte y dos han sufrido eventos que comprometieron sus activos de información, a continuación el detalle que indica la cantidad de incidentes provocados por fuentes internas y externas:



FUENTE: Datos Obtenidos de Encuestas (Anexo 1)

En base a un análisis apoyado en la información recopilada a lo largo de la investigación, fue posible fundamentar que la cantidad de incidentes pueden deberse a que no existen controles debidamente implementados y probados, ya que la falta de conocimiento técnico y concientización por parte de los departamentos que rigen al área de tecnología pueden ser causas de la inexistencia de proyectos de implementación de sistemas de seguridad de la información.

Además es importante señalar que tanto el departamento de tecnología, como el departamento financiero (por ejemplo) cumplen con sus actividades propias, de modo que si de seguridad de información se trata, sería muy difícil establecer responsabilidades para manejar proyectos, implementar controles y realizar revisiones periódicas de los mismos. Es por eso que algunas empresas optan pos tener personal técnico especialista en seguridad de la información, quienes se enfocan netamente a aspectos técnicos, dejando de lado un enfoque administrativo.

4. GUÍA DE SEGURIDAD DE INFORMACIÓN DIRIGIDA A LA GERENCIA GENERAL

La siguiente guía nace como fruto de la recopilación, análisis e interpretación de toda la información obtenida durante la presente investigación, y está dirigida al personal administrativo regulador del Área de Tecnología de las distintas organizaciones, ya que es su obligación conocer acerca de un procedimiento de seguridad de información que pueda ser utilizado junto con la asesoría del personal técnico con la finalidad de prevenir fuga de información por parte de los empleados de la organización.

En base al análisis realizado a partir de las encuestas (Referirse a Anexo 1), esta guía recomienda fuertemente que en toda organización el Departamento de Sistemas o Tecnología reporte o sea subordinado solamente de la Gerencia General y de los niveles superiores a esta, debido a que de este modo se evitarán contratiempos y malas gestiones por parte de personal que no se encuentra debidamente capacitado.

4.1. Establecimiento de un sistema de seguridad de información

Debido a que generalmente en las organizaciones del Ecuador, las áreas de tecnología reportan a niveles superiores que no tienen conocimientos técnicos, es importante que dichos niveles estén asesorados por personal especializado en seguridad de la información, además, deben considerar la independencia entre este equipo de especialistas y el personal del área de tecnología.

4.1.1. Formación de Equipo de Especialistas en Seguridad de la Información

En base a lo anterior, el primer punto de esta guía es proponer la contratación de personal técnico-administrativo especializado en seguridad de la información, el mismo que debe estar adaptado a las necesidades y a la situación actual de la empresa.

Los integrantes del equipo deben tener las siguientes competencias:

4.1.1.1. Líder o jefe de grupo

Es la persona que se encuentra a cargo del grupo de profesionales especializados en seguridad de la información, incluso, dependiendo del tamaño del equipo, podría ser un Gerente, sus principales responsabilidades estarían orientadas a:

- Asesorar, responder y reportar a los niveles superiores.
- Coordinar, planificar y dirigir al grupo de especialistas.
- Revisar periódicamente el trabajo de los especialistas en cada uno de los proyectos.
- Planificar y dirigir los distintos proyectos de seguridad de la información, considerando que existe la posibilidad de delegar tareas, más no responsabilidades.
- Asegurar que la administración brindará todas las facilidades para que los empleados de la empresa cooperen con los especialistas durante sus proyectos.
- Establecer contactos con personal externo a la empresa cuando resulte necesaria su intervención en algún proyecto, y asesorar a la administración durante la negociación del contrato de prestación de servicios.
- Asesorar y buscar asesoría del personal interno de la organización; cuando resulte oportuno apoyarse en especialistas de ramas distintas a la informática (leyes, sicología, finanzas, etc.)
- Implementar todos los proyectos que hayan sido desarrollados por el personal bajo su mando.
- Discutir los resultados de los proyectos con la administración.

4.1.1.2. Especialistas

Es el personal especializado en cada una de las ramas donde podrían comprometer a los activos de información de la empresa, por ejemplo, administración de bases de datos, desarrollo de software, administración de redes, operaciones técnicas (obtención de respaldos, mantenimiento de equipos, etc.), incluso considerando a

personas que asesoren a los técnicos con la finalidad de crear, publicar y mantener actualizadas políticas administrativas y manuales de funciones (orientados al uso de los recursos tecnológicos) tanto para personal del área de tecnología, como para empleados en general, sus principales responsabilidades serían:

- Ejecutar los proyectos que el Jefe de Grupo y los directivos han planificado
- Responder y reportar al Jefe del Grupo durante todo el proyecto, considerando que en caso de existir incidentes con personal o con terceros, es el Jefe quien debe gestionarlos.
- Asesorar y delegar funciones a los niveles inferiores.
- Encargarse que todo lo realizado durante los distintos proyectos se encuentre documentado de manera sea posible informar y reportar de una manera sencilla y eficiente.
- Obtener conclusiones y brindar recomendaciones de los proyectos que se ejecuten.
- Relacionarse con los empleados de la empresa de manera que se establezcan relaciones de confianza donde sea factible obtener todos los recursos necesarios para ejecutar el proyecto.

4.1.1.3. Asistentes

Personal especialista con menos experiencia, básicamente realiza funciones de soporte a los encargados de cada proyecto, estas actividades de soporte podrían limitarse a tareas puntuales designadas a ellos, las mismas que pueden ir evolucionando a medida que la persona adquiere mayor experiencia en una rama específica, sus responsabilidades se orientan brindar apoyo al encargado del proyecto en lo que fuera que este necesite, por ejemplo, recopilar información, documentación, redacción de informes, etc.

Con fines de mejor manejo de los distintos proyectos, y, del tamaño de la empresa, podrían crearse distintas jerarquías dentro de los grupos antes indicados, dependiendo de la experiencia de la persona o de alguna posible especialización. Ej. Especialistas A, Especialistas B, Asistentes A, Asientes B, con programas de asenso de personal con la

finalidad de inculcar deseos de hacer carrera en la organización, lo cual resultaría beneficioso para la administración debido que siempre se contaría con personal capacitado y comprometido.

Una vez establecido el personal especializado en seguridad de la información, es responsabilidad de la Gerencia General reforzar administrativamente los aspectos de seguridad de la información de la empresa.

4.1.2. Reconocer activos de información a ser protegidos

Se basa en saber reconocer los activos de información que necesitan ser protegidos, así como su ubicación física y la tecnología sobre la cual operan y se almacenan.

Una práctica recomendable es mantener reuniones con los dueños de los distintos procesos del negocio, de modo que junto con ellos y con personal del área de tecnología se llegue a determinar la información más importante que necesita ser protegida.

Cuando a manera de consenso entre la administración, los dueños de los procesos, el personal técnico de tecnología y los profesionales en seguridad de información se han determinado los activos de información que requieren ser protegidos, es necesario determinar las amenazas que podrían comprometerlos, por ejemplo, desastres naturales (inundaciones, terremotos, erupciones, etc.), errores humanos (falta de personal, errores de mantenimiento, errores de usuario), errores de red (sobrecarga de tráfico, fallas en la red, fallas en el hardware) o amenazas deliberadas (robo, daños intencionales, ataques informáticos, etc.), además, para cada amenaza es necesario determinar una probabilidad de ocurrencia, por ejemplo, un terremoto puede tener un 5% de probabilidad de ocurrir, pero un error de un usuario con falta de capacitación podría tener un 80%. Al finalizar esta etapa, es posible obtener un reporte acerca de amenazas identificadas, un grupo de activos de información a los que podrían afectar y estimaciones de probabilidad de ocurrencia.

4.1.3. Evaluar vulnerabilidades

A continuación, el personal especializado en seguridad de información junto con el personal del área de tecnología, deben realizar evaluaciones de las distintas

vulnerabilidades que podrían provocar que las amenazas identificadas anteriormente se materialicen, por ejemplo, falta de segregación de funciones, falta de programas de capacitación de personal, falta de políticas internas, falta de manuales de funciones, líneas de cableado desprotegidas, puertas sin cerraduras, falta de antivirus, etc. Como resultado de este paso, se obtendrán informes de todas las vulnerabilidades que podrían ser explotadas por las amenazas identificadas anteriormente.

4.1.4. Determinar controles

Con la lista de las vulnerabilidades encontradas, es necesario determinar los distintos controles que la organización dispone para minimizar los riesgos que estas conllevan, de modo que el equipo de especialistas debe conocer la situación actual de los sistemas de seguridad de información de la empresa para estar en capacidad de tomar decisiones de futuros proyectos, sean de mantenimiento o implementación, básicamente deben realizarse las siguientes actividades:

- Determinar qué aspectos de la seguridad de la información van a ser evaluados, entre otros, algunos aspectos podrían ser: gestión de bases de datos, seguridades físicas, seguridades lógicas, control de cambios en las aplicaciones, operaciones (obtención de respaldos, mantenimiento de equipos).
- Una vez que se han determinado los aspectos que serán evaluados, es necesario asignar a un equipo para el proyecto de evaluación.
- El equipo se encargará de recopilar información, indagar con los responsables de las áreas evaluadas y verificar el estado actual de los controles, tanto técnicos como administrativos.
- Una vez que se ha determinado el estado actual de dichos controles, debe realizarse una comparación con un estándar reconocido, por ejemplo, comparar las seguridades físicas del cuarto de servidores de la empresa, con las seguridades físicas que según la Norma ISO 27001 deberían existir en un cuarto de servidores. Es importante señalar que la adecuación de los controles de las normas estandarizadas a la situación de la empresa, es responsabilidad de los especialistas.

- Finalmente, el punto culminante será emitir un informe que contenga una descripción de los controles que se encuentran operando, su estado de funcionamiento, y un listado de controles que deben ser implementados.

4.1.5. Informar acerca de los controles implementados

El informe acerca de los controles de seguridad de información deberá ser discutido con la Gerencia General, con la finalidad de establecer su aplicabilidad, motivo por el cual el equipo especializado en seguridad de la información debe contar con las suficientes bases para justificar su informe presentado. Lo importante es centrar la justificación en que todos estos controles reducirán la probabilidad de que una vulnerabilidad sea explotada por una amenaza, además de reducir el impacto en caso de que ocurra el riesgo.

4.1.6. Asesorar a la Gerencia General

Además de presentar el informe indicado, el equipo especializado en seguridad de información debe brindar asesoría a la administración, con la finalidad de determinar cuándo y en que activos de información se aceptarán los riesgos, se los transferirá, se los reducirá o se los evitará.

4.1.7. Implementar nuevos controles

A continuación, se deben establecer proyectos de implementación de controles junto con el área de tecnología, de modo que se establezcan tiempos estimados en los que se planee poner en producción el control, actividades que se realizarán para implementarlo, etc.

Algunos controles pueden ser:

- Políticas internas (Referirse a ANEXO 2 y ANEXO 3)
- Establecimiento de políticas de contraseñas (longitud, límite de intentos de autentificación, complejidad, etc.)
- Implementación de medidas de seguridad física (lectores biométricos, tarjetas magnéticas, cámaras de seguridad)

- Controles ambientales (Aire acondicionado, extintores de incendios, fuentes alternas de energía)
- Segregación de funciones del personal con acceso a datos críticos
- Acordar servicios con terceros (transporte y custodia de cintas de respaldo, mantenimiento de equipos, capacitación al personal)

4.1.8. Revisiones Periódicas

Una vez implementados los controles, es necesario hacer revisiones periódicas de su operatividad, esto puede hacérselo a manera de auditoría interna con intervalos de 6 u 8 meses, considerando también que las vulnerabilidades y amenazas identificadas para determinar dichos controles pudieron haber cambiado, desaparecido, o también aumentado, lo cual derivaría en un realizar un nuevo estudio similar al indicado pero a menor escala ya que la organización cuenta con controles operativamente eficaces.

4.2. Respuesta administrativa ante fugas de información detectadas

El hecho de que una organización cuente con controles para salvaguardar la seguridad de su información, no garantiza que esta se encuentra protegida, motivo por el cual el presente manual también contempla ciertos lineamientos administrativos de análisis forense de acuerdo a las herramientas o dispositivos utilizados para fugar información.

En caso de detectarse una fuga de información, es responsabilidad del equipo de especialistas asesorar al personal administrativo pertinente para efectuar las respectivas investigaciones, las mismas que pueden ser administrativas o judiciales. Debido a que las investigaciones judiciales dependen del Ministerio Público (únicamente la administración debe colaborar y dar seguimiento a la investigación), este manual se enfoca a investigaciones de tipo administrativo.

Una investigación de tipo administrativo puede ser ejecutada por el equipo de especialistas en seguridad, aunque en caso de requerirse asesoría externa, es su responsabilidad asesorar a la administración en la búsqueda de profesionales en informática forense quienes se encargarán de todo el proceso de análisis.

A continuación, lineamientos administrativos que deben seguirse en caso de optar por una investigación de tipo administrativa, realizada por personal propio de la empresa:

4.2.1. Fugas a través de correo electrónico

En caso de que un funcionario haya filtrado información mediante su cuenta de correo electrónico, tanto la administración como el equipo de seguridad de la información, deben conocer que es posible obtener evidencia digital de distintas fuentes, dependiendo si el funcionario utilizó una cuenta personal de correo (que por controles internos debería estar restringida) o utilizó su cuenta corporativa, en caso de haberse utilizado una cuenta personal, debió también haberse utilizado un explorador de internet, el mismo que podría almacenar información que permita establecer responsabilidad (Historial de navegación , información que se auto completa en los formularios de las distintas páginas, etc.)

Es responsabilidad de los especialistas saber ubicar cada una de esta información y analizarla, o también de salvaguardarla para que su integridad se mantenga hasta que intervengan los analistas forenses.

Otra forma de haber fugado información mediante el envío de correos electrónicos, es utilizando una cuenta de correo corporativa, para lo cual basta con acceder a esta y verificar junto con su dueño los mensajes enviados, o también verificando los rastros respectivos (junto con asesoría de los especialistas) en el servidor de correo.

Una forma de fugar información a través de correo electrónico, puede ser la Esteganografía, la misma que por ser una técnica muy sofisticada de ocultamiento de información, podría requerir de fuertes conocimientos por parte de los especialistas, aunque lo más recomendable sería buscar en los equipos en los cuales se sospecha se cometió el delito herramientas de software que son utilizadas para ocultar información dentro de otra, o utilizando herramientas de detección como Steganos o My Secrets, aunque esto dependería del conocimiento y experiencia de los investigadores, mientras que la responsabilidad de la administración, sería proveerles dichas herramientas.

4.2.2. Fugas a través equipos electrónicos (PDA, Blackberry, Ipod, teléfonos celulares, memorias extraíbles, etc.)

Es importante que la administración, bajo la asesoría del equipo de seguridad, se encargue de preservar la evidencia digital de la siguiente manera:

- Asegurar físicamente y apropiarse de los dispositivos que se encuentran bajo sospecha de haber sido utilizados para fugar información. Esto puede ser posible únicamente si se han establecido lo controles y las políticas adecuadas para que el personal con acceso a datos sensibles de la empresa utilice equipos electrónicos de propiedad de ésta, siempre que se encuentren en sus instalaciones (teléfonos celulares, blackberry, memorias extraíbles, etc.), además, es necesario documentar la descripción de los equipos indicando números de serie e insertando fotografías.
- Una vez que la administración se ha encargado de asegurar físicamente los dispositivos, los especialistas o los encargados de la investigación deben crear una imagen exacta del disco del dispositivo para evitar pérdida de información, y proseguir con el análisis. Este proceso debe ser supervisado por la administración, con la asesoría del Jefe del Equipo de Especialistas en Seguridad.

4.2.3. Ante fugas de información producidas por Ingeniería Social

Aunque podría resultar muy complicado llegar a dar con los responsables en caso de que la organización haya perdido información por medio de ingeniería social, es recomendable que en caso de que exista sospecha de que esto sucedió, la administración se encargue de contratar a personal capacitado para que entreviste a todos los funcionarios que tienen acceso a la información filtrada, estas entrevistas podrían ir orientadas a verificar si el funcionario ha desarrollado una conexión (amistad, miedo, chantaje, etc.) con alguna persona que le ha demostrado interés por información de la empresa y si se la ha proporcionado, lo cual podría establecer bases apoyadas en políticas para sancionar al responsable.

Una vez que se ha terminado el análisis informático forense, los informes del mismo indicarán los resultados arrojados por la evidencia digital, de modo que apoyándose en los controles y las políticas internas de la organización, será factible establecer

responsabilidades, ya que, los informes no estarán orientados a identificar a personas, sino a equipos, motivo por el cual el equipo técnico deberá asesorar a la administración para tomar medidas corporativas o al profesional legal para tomar medidas judiciales.

En caso de que no existan políticas que establezcan responsabilidades del personal, será casi imposible tomar medidas en contra de los responsables o ejecutores del delito, motivo por el cual, la primera parte de este manual resulta ser muy importante tanto para la prevención de fuga de información, como para el establecimiento de sanciones administrativas.

5. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Un nivel gerencial a cargo de un departamento que requiere conocimientos técnicos para ser administrado, necesita contar con personal capacitado y comprometido que asesore en cada una de las decisiones a ser tomadas con la finalidad de que todos los procesos del departamento sean gestionados de una forma técnico administrativa adecuada.

- Los delitos donde se vulneran seguridades de los activos de información por parte del personal de una organización se deben a desinformación, desorganización, falta de compromiso y una deficiente administración de recursos tanto materiales como humanos y tecnológicos.

- Una fuga de información puede darse por fallas en la seguridad lógica o física de las aplicaciones de software, así como en la deficiente administración y asignación de los recursos tecnológicos, ya que, al existir vulnerabilidades administrativas y de seguridad existe camino abierto para personal pueda adquirir información confidencial con la finalidad de obtener beneficio propio, provocando pérdidas significativas para la empresa; pérdidas no solamente económicas, sino de imagen y credibilidad ante sus clientes, la competencia, y demás empresas.

- Es responsabilidad de la administración de la organización precautelar por la seguridad de la información, además de oportunamente dar parte y gestionar un adecuado proceso investigativo en caso de detectarse una infracción informática, además de no preocuparse de la posibilidad de perder imagen ante sus clientes o ante la competencia, debido a que toda la información utilizada por los investigadores informáticos forenses en sus análisis nunca será revelada, ni siquiera con fines informativos, debido a que el único documento que podría catalogarse como público, es el informe final.

- Así como la tecnología ha significado un punto de avance para los infractores informáticos, las distintas metodologías y herramientas de prevención y detección, y la investigación informática forense han avanzado al punto de convertirse en una ciencia de especialización para profesionales de la informática, ya que, aunque localmente no ha alcanzado su completa madurez existen organizaciones a nivel mundial que pueden brindar asesoría sin importar si la investigación es interna o si se ha decidido acudir ante la autoridad competente.

- El rol de un auditor informático, es hallar las pruebas de un delito con la finalidad de asesorar al profesional del derecho, para que sea él quien ubique la infracción dentro del campo de las leyes y hacer la respectiva denuncia.

Recomendaciones

- Implementar controles de seguridad de la información, por ejemplo:
    - Restricción de instalación de hardware o software solo a usuarios autorizados.
    - Cuentas de usuario con privilegios adecuadamente establecidos en las aplicaciones.
    - Restricciones de acceso físico a equipos críticos de acuerdo al cargo del funcionario.
    - Adecuados valores en los parámetros de seguridad de las contraseñas (complejidad, longitud, intentos fallidos de autentificación, validez).
    - Mantener personal capacitado e informado acerca de posibles delitos y como evitarlos.
    - Adecuada segregación de funciones del personal técnico del área de tecnología.
    - Generar distintas políticas que regulen distintos procedimientos, tales como solicitud de cambios a aplicaciones, cambios de contraseña, traslado y manipulación de equipos, monitoreo de procesos automatizados, etc.
    - Establecer planes de respaldo de información sensible, así como revisiones periódicas de los mismos.

- Realizar auditorías anuales tanto de la eficacia operativa de los controles establecidos, así como del conocimiento de los mismos por parte de los empleados con la finalidad de conocer las brechas de seguridades tanto físicas como lógicas, dichas auditorías deberán evaluar aspectos tales como seguridades, control de cambios en aplicaciones, y, manejo y administración de bases de datos. Además, asegurarse de que los controles administrativos (políticas internas) son conocidos por los empleados, capacitándolos continuamente y ejecutando planes de evaluación del conocimiento de las políticas internas.

- Establecer, publicar y dar a conocer políticas, procedimientos y manuales de funciones robustos, comprensibles y reales, con la finalidad de que la empresa cuente con bases reales de apoyo para la gestionar el comportamiento personal y profesional de los empleados, así como para establecer responsabilidades y sanciones, las mismas que dependiendo de la infracción deberían ser tratadas a nivel administrativo o legal, siempre

contando con la asesoría de profesionales tanto informáticos como legales, ya que una sanción infundada o mal procesada administrativamente podría derivar en demandas legales para la organización.

- Gestionar y ejecutar programas de capacitación para el personal de la empresa, sin importar su cargo, con la finalidad de mantenerlos informados acerca de las distintas técnicas de cometer delitos (orientando las charlas al tipo de personal), para evitar que las personas se conviertan en elementos frágiles de un sistema de seguridad, además, es importante señalar que es obligación de la administración crear conciencia y compromiso en el personal, incluso apoyándose en dar a conocer elementos de sanción con la finalidad de persuadir a quienes pongan mayor resistencia a los controles, siendo este el punto clave donde deben actuar los administradores.

- Realizar selecciones de personal, estrictamente según a las necesidades y características del cargo vacante, con la finalidad de no poner en peligro los datos sensibles que podrían estar al alcance de la persona, considerando una adecuada segregación de funciones del personal técnico del Área de Sistemas, y, asignando al personal recursos y privilegios tecnológicos tanto lógicos como físicos de acuerdo a su rol.

- Prohibir o restringir al máximo el uso de equipos y dispositivos informáticos y electrónicos personales en las instalaciones de la organización, o al menos en sitios sensibles, creando áreas libres que se encuentren fuera del alcance de información y de redes de la empresa, esto con la finalidad de evitar que información corporativa sea tratada como personal.

- En caso de detectar o sospechar la existencia de un ilícito que comprometa a la seguridad de la información digital, es muy importante recibir asesoría calificada (en caso de optar por una investigación interna), seleccionando un equipo competente y reconocido para que se haga cargo de proceso investigativo informático; para esto la organización debe contar con profesionales capacitados de manera que estén en condiciones de hacer los respectivos contactos con terceros y ser parte activa en la negociación de contratos de servicios profesionales.

6. FUENTES BIBLIOGRAFICAS

6.1. Documentos Físicos

ALEXANDER, Alberto. 2008. Diseño y Gestión de un Sistema de Seguridad de Información.

Apuntes recopilados a lo largo de la Carrera Universitaria

AREITIO, Javier. 2007. Seguridad de la Información. Redes, Informática y Sistemas de Información

Documentación didáctica del Curso de Seguridad Informática bajo óptica del Estándar Internacional ISO 27001:2005

ERICKSON, John. 2008. Hacking: Técnicas Fundamentales (Hackers Y Seguridad)

GÓMEZ, Vieites. 2006. Enciclopedia de la Seguridad Informática
PLATINNI, Mario. 2008. Auditoría de Tecnologías y Sistemas de Información

PLATINNI, Mario. 2007.Gobierno de las Tecnologías y Los Sistemas de Información

ROYER, Marc. 2007. Seguridad en la Informática de Empresas - Riesgos, Amenazas, Prevención y Soluciones

SOLER, Joan. 2008. Preservación de los Documentos Electrónicos

6.2. Documentos Electrónicos

Documentación Confidencial Auspiciada

Estrategias de Seguridad. BENSON Christopher (Inobis Consulting Pty Ltd). Microsoft© Solutions. Noviembre 2000. http://www.microsoft.com/latam/technet/articulos/200011
POYATO, Chelo. COLL, Francisco. MORENO David. Recomendaciones de seguridad. Definición de una política de seguridad. España. 15 de diciembre de 2000. http://www.rediris.es/cert

Seguridad Informática - Implicancias e Implementación - Lic. Cristian Borghello. http://www.segu-info.com.ar

Trabajo sobre DELITOS INFORMÁTICOS, Universidad de El Salvador, Octubre 2000 (PDF)

7. GLOSARIO DE TÉRMINOS

Activo.- Es el conjunto de bienes y derechos de los que es titular la empresa, así como otras partidas con la característica común de que se utilizan en la generación de ingresos.

Amenaza.- Cualquier aspecto o escenario que pueda ocasionar que un riesgo se convierta en incidente, o sea, que llegue a realizarse.

Archivos de sistema.- Son aquellos archivos de uso exclusivo del sistema operativo. Estos archivos no pueden ser eliminados normalmente por el usuario o el sistema le advierte que se dispone a eliminar un fichero necesario para su correcto funcionamiento.

Ataques de Denegación de Servicio (DoS).- Este ataque se presenta cuando el servidor DNS se ve inundado con un número muy grande de requerimientos reconocidos que pueden eventualmente forzar al procesador a ser usado más allá de sus capacidades; de esta manera se imposibilita el acceso a los servicios y recursos de una organización, provocando la pérdida de la conectividad de la red impidiendo el desarrollo normal de las actividades.

Autentificación.- Verificación de la identidad de una persona, usuario o proceso, para así acceder a determinados recursos o poder realizar determinadas tareas. En un entorno de red recibe este nombre la acción de verificar la identidad de quien envía un mensaje.

BIOS.- Acrónimo de Basic Input/Output System (Sistema básico de entrada/salida), que es el programa de enlace entre la máquina y el sistema operativo, el cual se carga en la memoria ROM cuando el ordenador es encendido y desde allí controla el tránsito de información entre los diferentes elementos del sistema, tales como la memoria, los discos, el monitor, etc.

Caché.- Memoria de alta velocidad y baja capacidad de almacenamiento que va colocada entre la memoria principal y el microprocesador para almacenar los datos que el microprocesador va a utilizar con gran frecuencia en el proceso que está realizando y con ello aumentar la velocidad del proceso. Conjunto de datos duplicados de otros originales. La duplicación se basa en que los datos originales son más costosos de acceder en tiempo con respecto a la copia en memoria caché.

Capacitación.- Toda acción organizada y evaluable que se desarrolla en una empresa para modificar, mejorar y ampliar los conocimientos, habilidades y actitudes del personal produciendo una cambio positivo en el desempeño de sus tareas

Clave de acceso.- Es una combinación de letras, números y signos que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.

Código malicioso.- Término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tienen como objetivo infiltrarse o dañar un ordenador sin el consentimiento de su dueño. Esta definición incluye tanto programas malignos compilados, como macros y códigos que se ejecutan directamente, como los que suelen emplearse en las páginas Web (scripts).

Consecuencia.- Hecho o acontecimiento que resulta de otro. Correspondencia lógica entre lo que piensa y hace una persona.

Correo electrónico.- Servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos

CRM.- (Customer relationship Management) Amplio término que cubre conceptos usados por compañías para gestionar sus relaciones con clientes, incluyendo la colección, almacenamiento y análisis de la información de sus clientes.

Delito informático.- Cualquier comportamiento criminal en el cual la computadora ha estado involucrada como material o como objeto de la acción.

Delito.- Conducta o acción típica (tipificada por la ley), antijurídica (contraria a Derecho), culpable y punible.

Derecho.- Es el conjunto de normas que regulan la convivencia social y permiten resolver los conflictos interpersonales.

DHCP.- Protocolo de Configuración Dinámica de Máquinas ("Dynamic Host Configuration Protocol"), que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

Documentos electrónicos.- El documento electrónico es aquel generado, transmitido o almacenado en el ambiente digital, debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

ERP.- Enterprise Resource Planning (Sistemas de Planificación de Recursos Empresariales) son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios, es decir, que modelan y automatizan la mayoría de procesos en la empresa.

Evidencia Digital.- Cualquier información en formato digital que pueda establecer una relación entre un delito y su autor

Factura Electrónica.- Es una modalidad de factura en la que no se emplea el papel como soporte para demostrar su autenticidad. Por eso, la factura electrónica es un fichero que recoge la información relativa a una transacción comercial y sus obligaciones de pago y de liquidación de impuestos y cumple otros requisitos que dependen de la legislación del país en el que se emplea.

Fidelidad.- Noción que en su nivel más abstracto implica una conexión verdadera con una fuente o fuentes.

Firewall.- Elemento utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas;

FINALeMail.- Herramienta de software que permite recuperar correo electrónico eliminado o perdido por borrado accidental, virus o formateo de disco.

Fraude.- Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

FTK (Forensic ToolKit).- Herramienta de Software que ofrece utilidades para realizar análisis digital forense, esto puede ser realizado mediante línea de comandos o interfaz gráfica.

Gestión.- Es un conjunto de reglas y métodos para llevar a cabo con la mayor eficacia un negocio o actividad empresarial

Gusano.- Programa que se va sucesivamente duplicando por sí mismo, cuya misión es reproducirse y extenderse al mayor número de ordenadores posibles. Su efecto es similar al de un virus, ya que puede saturar los sistemas en los que se implante.

Hurto.- Apoderarse de cosa ajena contra la voluntad de su dueño, sin intimidación en las personas ni fuerza en las cosas.

Incidente.- Escenario ocasionado por la consecución de un riesgo.

Información empresarial.- Información relacionada a todos los aspectos que una empresa utiliza para llevar a cabo su actividad comercial

Informática.- Ciencia que estudia el tratamiento automático de la información en computadoras, dispositivos electrónicos, y sistemas informáticos.

Infraestructura tecnológica.- Conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, etc.) y servicios (soporte

técnico, seguros, comunicaciones, etc.); que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de una empresa.

Intrusión.-Acceso no autorizado hacia un sistema o servicio.

Investigación forense.- Análisis que se realiza a todos los componentes de la escena de un crimen con el objetivo de encontrar evidencia.

Jerarquía.- Es la disposición de personas, animales o cosas, en orden ascendente o descendente, según criterios de clase, poder, oficio, categoría, autoridad o cualquier otro asunto que conduzca a un sistema de clasificación.

Lineamiento.- Guía, tendencia, una dirección o un rasgo característico de algo.

Malware.- El término Malvare (Acrónimo en inglés de: "Malcious software") engloba a todos aquellos programas "maliciosos" (troyanos, virus, gusanos, etc.) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al sistema informático o al usuario del mismo.

Mando alto.- Persona u organismo que ejerce la potestad superior.

Manual (documento).- Documento que contiene la descripción de actividades que deben seguirse en la realización de las funciones de una unidad administrativa, o de dos ò más de ellas. El manual incluye además los puestos o unidades administrativas que intervienen precisando su responsabilidad y participación.

Mecanismo.- Conjunto de elementos, dirigidos a realizar una determinada actividad.

Memoria extraíble.- Forma desarrollada de la memoria EEPROM que permite que múltiples posiciones de memoria sean escritas o borradas en una misma operación de programación mediante impulsos eléctricos, frente a las anteriores que sólo permite escribir o borrar una única celda cada vez.

Método criptográfico.- Es el arte o ciencia de cifrar o descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que solo puedan ser leídos por las personas a quienes va dirigido el mensaje y que posean los medios para descifrarlos.

Middleware.- Es un software de computadora que conecta componentes de software o aplicaciones para que puedan intercambiar datos entre éstas. Es utilizado a menudo para soportar aplicaciones distribuidas. Esto incluye servidores Web, servidores de aplicaciones, sistemas de gestión de contenido y herramientas similares.

Plan de marketing.- Documento escrito que detalla las acciones necesarias para alcanzar un objetivo específico de mercadeo. Puede ser para un bien o servicio, una marca o una gama de producto

Política interna.- Conjunto de normas, reglas y disposiciones que regulan el comportamiento, las responsabilidades y las restricciones del personal de una empresa.

Políticas.- Conjunto de disposiciones documentadas que regulan el comportamiento de un grupo de individuos.

Pornografía.- Modernamente se entiende por pornografía un conjunto de materiales, imágenes o reproducciones de la realización de actos sexuales con la intención de excitar o promover la lujuria.

Prevención.- Adopción de medidas encaminadas a impedir que se produzcan deficiencias físicas, mentales y sensoriales (prevención primaria) o a impedir que las deficiencias, cuando se han producido, tengan consecuencias físicas, psicológicas y sociales negativas

Proceso.- Conjunto ordenado y sincronizado de actividades orientadas a lograr un objetivo

Recursos.- Todos los elementos con los que se cuenta y que pueden ser utilizados para alcanzar objetivos o ejecutar proyectos.

Robo.- Apoderarse de lo ajeno con violencia o intimidación en las personas o fuerza en las cosas.

Sanción.- Acto formal tomado hacia quién comete delito

Sistema de Detección de Intrusos.- IDS acrónimo en inglés de: "Intrusion Detection System" es un programa usado para detectar accesos desautorizados a un computador o a una red, que analiza el tipo de tráfico de la red además de su contenido y comportamiento.

Sociedad de la Información.- Es aquella en la cual la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas.

Spam.- También conocido como junk-mail o correo basura, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no deseado que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

Tarjeta de expansión.- Son dispositivos con diversos circuitos integrados y controladores que, insertadas en sus correspondientes ranuras de expansión, sirven para ampliar la capacidad de un ordenador.

Teléfono Celular.- Dispositivo inalámbrico electrónico que permite tener acceso a la red de telefonía celular o móvil. Su principal característica es su portabilidad, que permite comunicarse desde casi cualquier lugar.

Usuario.- Se define usuario como cualquier persona que utilice una computadora, sistema operativo, servicio o cualquier sistema informático, bien sea de manera individual o mediante la conexión a una red.

Ventaja competitiva.- Conjunto de ideas, actividades o proyectos que determinan una mejoría o ventaja para con los clientes, en relación a quienes cumplen con la misma actividad económica.

Virus.- Programa informático que tiene por objeto interferir con el hardware o con el sistema operativo del ordenador causando daños en el mismo, la mayoría de las veces irreparables, el cual infecta a una computadora y se propaga en ella con diversos propósitos como daño, robo de información, molestia, etc. y por lo general intenta pasar desapercibido por el usuario el mayor tiempo posible.

Vulnerabilidad.- Todo aspecto deficiente que puede ser aprovechado por una amenaza para generar la consecución de un riesgo.

8. ANEXOS

8.1. Anexo 1 – Encuestas realizadas a auditores de sistemas

ENCUESTA

Favor responder las siguientes preguntas:

1. En cuántos proyectos de auditoría de sistemas participó durante el período de tiempo comprendido entre Julio del 2008 y Abril del 2009?

   17

2. Del número señalado, indicar la cantidad de empresas cuyos Departamentos de Tecnología responden administrativamente ante las siguientes áreas:

Presidencia	2
Vicepresidencia	0
Gerencia General	6
Gerencia Financiera	9
Otro _____	0

3. De las empresas auditadas, en cuántas ocurrieron eventos que comprometieron sus activos de información digital?

   9

4. De los eventos indicados, cuántos se dieron por parte de personal de la empresa y cuántos por parte de terceros?

Personal de la empresa	8
Terceros	1

ENCUESTA

Favor responder las siguientes preguntas:

1. En cuántos proyectos de auditoría de sistemas participó durante el período de tiempo comprendido entre Julio del 2008 y Abril del 2009?

   14

2. Del número señalado, indicar la cantidad de empresas cuyos Departamentos de Tecnología responden administrativamente ante las siguientes áreas:

Presidencia	1
Vicepresidencia	
Gerencia General	1
Gerencia Financiera	11
Otro Proveedor	1

3. De las empresas auditadas, en cuántas ocurrieron eventos que comprometieron sus activos de información digital?

   6

4. De los eventos indicados, cuántos se dieron por parte de personal de la empresa y cuántos por parte de terceros?

Personal de la empresa	6
Terceros	

ENCUESTA

Favor responder las siguientes preguntas:

1. En cuántos proyectos de auditoría de sistemas participó durante el período de tiempo comprendido entre Julio del 2008 y Abril del 2009?

   12

2. Del número señalado, indicar la cantidad de empresas cuyos Departamentos de Tecnología responden administrativamente ante las siguientes áreas:

Presidencia	1
Vicepresidencia	
Gerencia General	2
Gerencia Financiera	8
Otro RRHH	1

3. De las empresas auditadas, en cuántas ocurrieron eventos que comprometieron sus activos de información digital?

   7

4. De los eventos indicados, cuántos se dieron por parte de personal de la empresa y cuántos por parte de terceros?

Personal de la empresa	6
Terceros	1

8.2. Anexo 2 – Ejemplo de Política de uso de Equipos de Computación

EMPRESA ABC

POLÍTICA DE USO DE EQUIPOS DE COMPUTACIÓN

OBJETIVO

Establecer parámetros generales para el uso adecuado de equipos de computación.

RESPONSABILIDADES

Usuario.- Seguir las políticas establecidas este documento.

Jefe de Gestión Humana.- Determinar si es necesario aplicar sanciones de acuerdo al caso.

PROCEDIMIENTO

1. El usuario se compromete a conocer y cumplir con las políticas establecidas en este documento, el Gerente de Tecnología está autorizado para que en cualquier momento pueda revisar, modificar o enmendar cualquiera de las disposiciones de este documento.
2. El usuario es responsable del equipo de computación a su cargo y velará por su buen uso.
3. Se prohíbe la distribución, instalación y uso de sistemas operativos o aplicaciones de los cuales la empresa no tiene la debida licencia. El usuario debe firmar un "formulario de propiedad intelectual de software", de no acatar esta disposición se someterá a las sanciones que imponga la Empresa
4. El equipo de computación entregado al empleado por parte de la compañía se debe registrar en un documento (Acta entrega/recepción) detallando las características del equipo, el mismo que será firmado por duplicado tanto para archivo del Departamento de Tecnología como para el usuario.
5. Al finalizar el contrato laboral, el usuario debe hacer entrega formal de los recursos informáticos al Gerente de su Área, y posteriormente a un representante o al Gerente de Tecnología para la firma de un documento de Acta Entrega/ Recepción.

6. Cualquier traslado de recursos de cómputo dentro de las instalaciones de la compañía, debe ser autorizado por el Departamento de Tecnología con 24 horas de anticipación previo al envió de un correo electrónico por el Gerente de Área.
7. Está prohibido instalar dispositivos de hardware adicionales sin el previo visto bueno del Departamento de Tecnología.
8. No se podrá instalar claves de encendido, ni modificar configuraciones del equipo. Si fuese necesario realizar una de estas operaciones debe ser informada al Departamento de Tecnología, para que el personal de soporte técnico efectúe esta labor.
9. Los dispositivos que sufran maltrato intencional o por descuido de un determinado usuario, serán reportados al gerente de área respectivo, y el costo de la reparación o reposición será cargado al usuario responsable del equipo.
10. El usuario no debe consumir alimentos o bebidas cerca de los equipos de computación.
11. Los fondos y protectores de pantallas, no podrán ser manipulados con ningún tipo de imágenes personales ni de otro tipo que no sea el logotipo de la Empresa. Además el protector de pantalla debe ser configurado con una clave se seguridad.
12. Los equipos de computación solo pueden salir de la Compañía bajo autorización del Departamento de Tecnología o del Gerente de área respectivo, deberá entregar al guardia de turno “el permiso de salida de materiales” firmado. En caso de pérdida el usuario responderá por la información extraviada y debe asumir los costos de reposición del equipo que determine la aseguradora.
13. El Departamento de Tecnología sólo presta servicio técnico a computadores de la institución.
14. Si un empleado no cumple las políticas establecidas en este documento, el Departamento de Tecnología notificará a Gestión Humana para que analice el caso y se establezcan sanciones

8.3. Anexo 3 – Ejemplo de Política de Confidencialidad y Privacidad de la Información

EMPRESA ABC

POLÍTICA DE CONFIDENCIALIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OBJETIVO

Establecer los términos y condiciones bajo las cuales el usuario mantendrá la confidencialidad de la información que dispone la empresa.

RESPONSABILIDADES

Usuario.- Seguir las políticas establecidas este documento.
Jefe de Gestión Humana.- Determinar las sanciones si es necesario de acuerdo a la falta cometida por un usuario.

PROCEDIMIENTO

1. La información generada por los empleados así como las copias de seguridad, son de propiedad de ABC y no de los usuarios que la manejan. Los empleados de ABC deben firmar el acuerdo de Confidencialidad como anexo a su contrato laboral.
2. Se prohíbe la transmisión de información o ejecución de actos que violenten o amenacen con violentar las normas, visión y misión de la compañía o que vayan en contra de la moral.
3. Los recursos informáticos de la Compañía se deben utilizar para beneficio de la misma, y en ningún caso para beneficio personal.
4. La información confidencial no debe colocarse en carpetas compartidas para evitar posibles manipulaciones o pérdidas de la misma. En caso de ser necesario compartir determinada información se deberán colocar las respectivas restricciones a través de contraseñas o permisos por usuario.
5. Los empleados no podrán disponer ni retirar información de la Empresa (en ningún medio electrónico), pues ésta es de carácter privado.

6. La información de carácter institucional, debe ser guardada en un lugar de fácil acceso para que pueda ser consultada por quienes lo requieren (otras personas de la empresa).
7. El Departamento de Tecnología podrá realizar auditoria en cualquier equipo informático de la compañía, sin previo acuerdo con el usuario del mismo.
8. El Departamento de Tecnología no se hace responsable por archivos de audio o de vídeo (mp3, wav, avi, etc.), pues no se considera información corporativa. Se hará excepciones si estos archivos tienen relación con la empresa (comerciales, capacitación).
9. Si una Gerencia de Área necesita información de un equipo de computación que pertenezca a ésta, y el usuario responsable no se encuentra o se niega a proveer la información, el Departamento de Tecnología puede tener acceso a estos archivos para realizar dicha tarea.
10. Está prohibido extraer software propio de la compañía para llevar a cabo instalaciones en equipos que no pertenezcan a esta.
11. Está prohibido almacenar material nocivo o material obsceno usando la infraestructura tecnológica de la institución.
12. No se autoriza el desarrollo de actividades que produzcan la congestión de la Red mediante el envío de información, mensajes o programas concebidos para tal fin (cadenas de mensajes, salas de Chat, descargas de archivos de Internet).
13. El departamento de Tecnología trabaja continuamente para mantener la privacidad de las comunicaciones de la compañía. Como parte de ese esfuerzo se monitorea la carga de tráfico de la red y las comunicaciones con el objetivo de tener estadísticas, cuando sea necesario, se tomará acción para proteger la integridad y operatividad de la red, siempre respetando la privacidad de sus empleados.
14. La información de la compañía es confidencial y no debe enviarse a través de Internet a menos que esté protegida por un password.
15. Si un usuario no cumple con las políticas establecidas en este documento, el Gerente de Tecnología notificará a Gestión Humana para que analice el caso y establezca las sanciones si es necesario.