# PROYECTO DE GRADO

CARLOS FERNANDO TOVAR
KEVIN AMARILES BEDOYA

PROYECTO

# MITIGACION DE RIESGO DE DELITOS INFORMATICOS EN EL CONTEXTO EMPRESARIAL

CARLOS FERNANDO TOVAR YEPES
KEVIN AMARILES BEDOYA

INGENIERIA DE SISTEMAS

PROYECTO DE GRADO

UNIVERSIDAD TECNOLOGICA DE PEREIRA
PEREIRA RISARALDA
SEPTIMBRE DEL 2014

## *1. MITIGACION DE RIESGO DE DELITOS INFORMATICOS EN EMPRESAS*

## ***2. FORMULACION DEL PROBLEMA***

En enero del año 2009 se promulgó la ley 1273 creándose un nuevo bien jurídico tutelado Denominado “de la protección de la información y de los datos “y se preservan Integralmente los sistemas que utilicen las tecnologías de información y las comunicaciones

Partiendo de esta ley se ha analizado que en Colombia es muy poco el tratamiento que se Le han dado a los delitos que todos los días se dan en los sistemas de información, hay Una gran cantidad de situaciones que no han sido reguladas y esto produce grandes niveles De inseguridad y frena un poco el avance a nivel de tecnología; son muchos los retos que Debemos enfrentar y la velocidad a la que van los avances tecnológicos ha hecho que Nuestra ley se quede corta permitiendo un gran nivel de vulneración de todos los usuarios, Y más cuando hoy en día son muchísimas las personas que poseen escasos conocimientos De los sistemas , además esto representa millones en pérdidas por parte de Las empresas y multinacionales cuando son violadas sus bases de datos, información Contable y demás.

Además las empresas se sienten desprotegidas y no hay un protocolo o unos estándares, Parámetros, metodológicas que se puedan emplear dentro de una empresa, sea grande Mediana o pequeña para mitigar los riesgos contra los delitos informáticos o saber que Hacer una vez que ocurran y como se tratan estos delitos por parte la justicia, como se Penalizan y cuál es el comportamiento de la ley como tal frente a diferentes delitos Informáticos.

### ***2,1, Identificación del problema***

En general, El problema consiste en generar unas políticas claras para que las empresas mitiguen el riesgo de situaciones en las cuales su información sea vulnerada y manipulada de forma indebida, se pretende que las Empresas puedan tener acceso a información para mejorar el conocimiento acerca del Tratamiento de delitos informáticos.

Muchas empresas no tienen desarrolladas unas políticas para evitar que ocurran delitos Informáticos, se debe tener una metodología para evitar el riesgo de que se cometa o le cometan delitos a un ente o un empresa de un delito informático, es tanto que ni se Conoce cuáles son los delitos informáticos, como se clasifican y como son tratados por la Ley.

Hay un desconocimiento, y falta de buenas prácticas en las empresas que permita evitar Cometer o ser sometido por los delitos informáticos y que las empresas muchas veces Llegan al peculado o es muy fácil que violen sus sistemas de información por no emplear Metodologías que eviten esto.

Adicionalmente, son muchísimos los delitos que se están cometiendo a nivel de los Sistemas de información, y la realidad es que con esta ley son muchos los que quedan en La completa impunidad, dándoles más garantías a los delincuentes para que los sigan Cometiendo.

Un estudio realizado por una empresa de seguridad privada llamada CIBER-ARK Denominado TRUST SECURITY Y PASSWORDS encontró que el 88 % de las personas Responsables de informática se llevarían información valiosa y sensible como lo son las Contraseñas de directivos, base de datos de clientes y demás datos financieros que son vitales en las compañías. [1]

Una cuarta parte admiten que sufren sabotajes internos, y un 35 % envía información Confidencial por correo.

Pese que en Colombia contamos con una ley en contra de los delitos informáticos esta ley Requiere de mucha más profundización en este sentido nos falta mucho camino por Recorrer, existen grandes falencias en el control de este los delitos de los sistemas de Información. A pesar de que las grandes empresas tienen sus reglas, hace mucha falta una Ley que sea suprema y logre incorporar en su contexto todas aquellas actividades ilícitas Que se cometen entorno a estos sistemas.

Está claro y un control o la implementación de protocolos de seguridad para las compañías Y diferentes tipos de usuarios del sistema, debe de ir acompañada de una ley que proteja Regule, eduque y fortalezca la confianza entre los usuarios, ya que esto ayudaría Enormemente a que se siga desarrollando aún más el sistema de economía en un entorno Virtual

.

## ***3. JUSTIFICACION***

Colombia es un país en vías de desarrollo, esto hace que se sigan unos niveles altos de Avance en el campo de la informática cambiando con ello un entorno cultural y social, Cuando las sociedades sufren cambios significativos en sus estructuras, hacen que El comportamiento humano también se vea afectado, lo que origina nuevos Comportamientos, estos pueden ser buenos y malos. Para tener un control sobre estos Comportamientos individuales es necesario sacar normas, leyes que los puedan mantener De una forma controlados. Podemos establecer que un comportamiento calificado como Ilícito es el que va en contra vía de la ley, lo que origina la conformación de un DELITO Entonces cuando el entorno de las sociedades cambia , también se originan nuevos delitos Para este caso de estudio cuando la sociedad Colombiana inicia un proceso de evolución En los sistemas de información empiezan a generarse nuevas formas de cometer actos Que van en contra del bienestar de las sociedades para cual Colombia crea la ley 1273 de 2009 con el fin de controlar evitar la generación de delitos informáticos "con esta ley se Modifica el Código Penal y se crea un nuevo bien jurídico Tutelado denominado " de la Protección de la información y de los datos " y se preservan integralmente los sistemas que Utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Este fue un gran paso para ejercer un control sobre estos delitos, y se plantea por medio De este proyecto es impregnar en las empresas de nuestro país protocolos, estándares, Unas buenas practicas que permitan evitar cometer y ser víctima de algún delito informático Y mitigar el riesgo del mismo

### ***3.1 ¿Porque es importante esta proyecto?***

1 – Este proyecto permitirá identificar una gran cantidad de delitos informáticos y como Proceder en las empresas para mitigar el riesgo de que ocurran y que hacer en el caso de Que pasen.

Se trata de relacionar como proceden las grandes multinacionales extranjeras y que Protocolos han utilizado para mitigar el riesgo de ser víctimas de delitos informáticos en los Últimos 20 años muchas empresas de las más grandes de norte américa han sido víctimas De delitos informáticos los cuales han causado pérdidas en sistemas de información Gigantescas y además por consecuencia perdidas económicas incontrolables se quiere Saber cómo procedieron estas empresas y que protocolos emplean para que estas cosas No vuelvan a suceder y como los estatutos internacionales cobijan a las empresas en caso De que estos delitos ocurran.

2- Permitirá identificar los vacíos el porqué de ellos y dar claridad a muchos conceptos que No se encuentran regulados dentro de la norma colombiana que se encargar de judicializar Los delitos informáticos en el país.

¿A qué se refiere con vacíos? Son muchos los términos técnicos que se generan en medio De los sistemas esto hace que puedan surgir un gran número de conceptos que en ultimas Solo quieren llegar a lo mismo y dar paso a la ambigüedad , pero terminan confundiendo Aún más los encargados de darle la interpretación, por esta razón debemos encontrar Concepto que se puedan generalizar y dar definiciones concretas y

rotundas y que den Mucha más claridad para quienes tienen que interpretarlos e impartir justicia en tales Comportamientos también para quienes no saben con claridad que pueden estar Cometiendo un delito y simplemente no lo saben entonces cuando se mira y se define

La palabra vacío dentro de un estatuto legal se refiere a re definir aquellas cosas que hacen Que una ley no sea concreta y justa y por último caso informativa para saber que conducta Es irregular o regular.

3- Esta investigación dará a conocer aspectos claves dentro de los sistemas de información Que están siendo aprovechados para cometer fraudes, extorciones, y dar a conocer las Tendencias actuales y viejas sobre tales delitos etc.

Con esta investigación se refiere a profundizar conocer e implementar programas de Gestión de vulnerabilidad en la red

4- Con este proyecto se dará0 a conocer información muy importante a las empresas sobre El manejo en la seguridad de sus compañías.

Este proyecto podrá servir como punto de partida para promover un cambio estructural en La ley actual demostrada cuales son los puntos frágiles de la ley actual. El porqué de la Importancia de un cambio en su estructura y su judicialización dentro del código penal.

## ***4. OBJETIVOS***

### ***4.1. OBJETIVO GENERAL:***

Elaborar un documento monográfico conteniendo políticas y normas que funcionen como estándar en las empresas para mitigar el riesgo de cometer o ser víctima de un delito informático.

1.2. Objetivos específicos

1- Conocer y relacionar sobre los elementos que conforman un delito en los sistemas Tecnológico de información y comunicación.

2- Identificar los delitos más comunes en el campo de la informática, apoyando la investigación En datos estadísticos de las entidades públicas como la Fiscalía General de la Nación y la Policía Nacional.

3- Analizar la ley 1273 de 2009, con el fin de contribuir en aspectos en los que pueda ser más Integral.

4- Documentar actividades donde se realicen procedimientos prácticos asociados con respuesta a los distintos incidentes cibernéticos.

5- Identificar las sentencias de la Corte Constitucional y las normas relacionadas con la informática forense.

6- Identificar y relacionar los procedimientos, estándares, métodos que utiliza la Fiscalía General de la Nación para reunir evidencia digital.

7- Identificar y relacionar metodologías empleadas en otros países en empresas grandes Medianas y pequeñas con las cuales intentan mitigar el riesgo de ser víctimas de un delito Informático.

8- Identificar un grupo de actividades y prácticas que sean constantes en grandes empresas y que se utilizan para evitar ser víctimas o victimarios de delitos informáticos.

9- Definir un estándar de políticas y normas que las empresas en general sin importar su índole O tamaño podrán utilizar para prevenir los delitos informáticos en sus compañías.

## ***5. MARCO REFERENCIAL***

### ***5.1ARTICULO 1 : DELITOS INFORMATICOS EN COLOMBIA***

*Link de consulta:*

[2]

A través del tiempo el uso del internet se hace por parte de toda la comunidad en el mundo Entero creando grandes oportunidades para el intercambio de información, mejorando la Comunicación y creando nuevos canales para la misma, revolucionando la manera en que Las personas interactúan y dando ventajas únicas que hace algunas décadas no existían, Pero como toda buena creación también tiene su parte maligna y es la que algunas Personas u organizaciones aprovechándose de algunas grietas que ofrece el internet o del Mal uso del mismo violentando derechos humanos prioritarios de las personas y violentando Con la información de grandes empresas.

Acá se puede ver como el ministerio del interior de la república de Colombia clasifica los Delitos informáticos

Se define como delito informático aquella situación en la cual se agravia los derechos de Una persona o varias, entidad privada o pública y en conclusión con cualquier ente el cual Sus derechos y privacidad se vean violadas por un medio tecnológico o en el mundo virtual, Pueden ejecutados por estos medios, sino también a partir de los mismos.

Algunos de los delitos informáticos más comunes en Colombia

- La expansión de virus informáticos
- Él envió intensivo de SPAM o como se conoce comúnmente, correo no deseado.
- La falsificación de los remitentes de mensajes con la técnica SPOOFING
- Él envió o entrada oculta de los archivos Espías o los KELOGGERS
- El uso de troyanos/backdoors para controlar determinados sistemas o en su efecto Para sustraer información.

***Manejo penal de los delitos informáticos en Colombia*** :"Ley de delitos informáticos en Colombia

Desde el año 2009 en Colombia se promulga la ley 1273 Por medio de la cual se modifica El Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de La información y de los datos"

Esta ley de la protección de los datos impuesta en el 2009, fue el comienzo de la Penalización de los delitos informáticos en el país, además se caracterizan y se clasifican Los delitos informáticos, pero en su ejecución no ha sido muy bien recibida esta ley y peor Aún no ha sido bien comprendida por parte de los entes encargados de impartir justicia, ¿Será que la ley no es lo suficientemente severa? O la cultura del país no está lo Suficientemente enterada de cómo se manejan delitos informáticos. Es un gran dilema pero Hasta el momento es la ley que regula los delitos informáticos en el país.

Más de 4.000.000 zonas de internet contienen material de sexo con menores. Cada día se Crean 500 sitios nuevos, además de eso estos sitios reciben más de dos mil millones

de Visitas anuales y el 60 % de estos sitios web son de pago y están situados en países donde La ley es más vulnerable (unión soviética, latino américa) [12]

## ***5.2ARTICULO 2 :98% DE LAS EMPRESAS SON VICTIMAS DE DELITOS INFORMATICOS***

*Link de consulta:*
[3]

El 98 % de las empresas en Colombia en la actualidad son víctimas de delitos informáticos Y la mayoría de estas firmas no se dan cuenta de lo que está ocurriendo "El informe recoge Datos de 1.500 clientes en más de 40 países y concluye que los sectores más atacados Son gobierno, servicios y consultoría, alta tecnología y finanzas, cuyos datos tanto internos Como los relacionados con clientes son puestos en riesgo a través de dos vectores Principales: ataques vía web o e-mail."

Las empresas en Colombia en su mayoría son víctimas de delitos informáticos diariamente Y su preparación para recibir estos ataques es mínima y lamentable lo cual pone en riesgo Los datos de millones de usuarios y además estos delitos tienden a evolucionar de acuerdo A las tendencias informáticas y en la actualidad con toda la información en la nube, los Ataques no tienen pausa.

¿Pero que deberían hacer las empresas para contrarrestar estos ataques? En este Momento en Colombia hay varias instituciones las cuales hacen énfasis en el tema de la Seguridad actuando en la prevención, corrección y detección de los delitos informáticos y Hacen énfasis en gestión de la seguridad del riesgo, métodos formales y criptografía, Informática forense y técnica y detección. "Latinoamérica está punteando en los datos que Recogemos sobre seguridad informática. Aglutina 44% de las amenazas permanentes (APT, en sus siglas en inglés) del mundo, pero al tratarse de un mercado emergente no hay Aún cifras demasiado claras", apunta Alejandro Jaramillo, gerente de territorio de FireEye."

La seguridad es el pilar en la estabilidad de las empresas actuales ya que todas poseen Información en internet y se quiere garantizar la fluidez de estos sistemas informáticos.

Los datos que maneja muestran la dimensión económica de estos ataques: cada año son Víctimas de cibercrimen 378 millones de personas, lo que tiene un costo global de US$113.000 millones. En el caso de Microsoft, la compañía destina US$9.000 millones en Investigación y desarrollo de productos que mejoren la seguridad. Pero para combatir eso Hay una lentitud y eso que Colombia ocupa el tercer lugar en Latinoamérica.

En Colombia la única maestría disponible se encuentra en la universidad de los andes, y Que comenzó hace un año, el país está tomando nota del tema de seguridad y que es una Gran fuente de empleo y que las empresas necesitan con urgencia.

***5.3ARTICULO 3 :ATAQUES EN LA SEGURIDAD DE LA INFORMACION EN LAS EMPRESAS***

Link de consulta:
[4]

“La protección contra todos los daños sufridos o causados por la herramienta informática y Originados por el acto voluntario y de mala fe de un individuo” las amenazas a las empresas Son cada día más grandes y los ataques no dan espacio a ninguna tregua es por eso que Las empresas deben estar alertas y bien preparadas a la hora de tratar con su seguridad Informática y es necesario proteger todos los medios de acceso a la empresa, muy seguido Vemos empresa sobreproteger su conexión de internet dejando otras vías de acceso Abiertas y sin protección. Es necesario implementar las principales medidas (cortafuegos, Antivirus, sistema de cifrado VPN, etc.) que sin duda alguna aportara un buen nivel de Seguridad.

***La piratería informática***Aunque es una práctica deliberada es castigada por la ley y se Basa en la violación de la propiedad intelectual para sacar provecho de la misma, existen Tres tipos de piratería informática Usuario Final por ejemplo cuando se copian cds de Licencias y se distribuyen para varias personas en Internet, Carga en el Disco Duro y Falsificación de Software.

El ataque DoS(Denial of Service) tiene como objetivo principal sacar de servicio las Maquinas del objetivo fijado, es decir sacar maquinas que presten un servicio En específico Y hacer que estas no realicen la función de la que estaban encargadas y por el contrario Colapsen. por eso el departamento de TI de la empresa es primordial para detectar Cualquier ataque de este tipo y también prevenirlo.

***INTERCEPTACION DE LOS DATOS***: La intercepción de los datos son el principal temor De las grandes compañías puesto que manejan información en la web y información Como contraseñas introducidas, las páginas web consultadas, los documentos Compartidos en la red, los e-mails enviados, información esencial sobre la empresa que el Pirata informático desea obtener, estos programas se denominan “packetsniffer”. Presupuestos, proyectos, salario y por no decir toda la información contable y no contable De las compañías pero tienen un gran problema de seguridad puesto que estos datos no Están cifrados y si llegan a caer en manos de un tercero las empresas pueden perder Millones un unos minutos.

Existen empresas las cuales sus tipos de red no son muy seguros lo cual hace que los hubsNo transmitan correctamente el paquete que envían a otro destinatario lo cual puede ser Aprovechado por un pirata informático y con programas de fácil acceso tener la información Que desea robar.

“Un hub recibe un paquete de datos, se encarga de duplicarlo entonces lo manda a todos Los puertos de salida, todas las maquinas conectadas a la red lo recibirán. De esta manera Todas las maquinas recibirán este flujo de información de todas las maquinas, así el pirata Informático podrá espiarlas a placer.

Muchas empresas no consideran la intercesión de sus datos como un problema grave , Porque consideran que las pequeñas y medianas empresas no son tan vulnerables como Las grandes empresas y por esta posición están siendo vulnerables a ataques y a pérdidas Millonarias , y existen herramientas las cuales pueden prevenir estos daños la utilización De conmutadores puede dar un mayor control a la red de la empresa y la encriptación de Los datos son pilares fundamentales en la seguridad de una compañía de cualquier tamaño.

***SOLUCION A ESTOS PROBLEMAS:*** La mayoría de empresas en la actualidad necesitan Estar comunicadas con otras empresas o comunicarse con sus empleados y sus clientes, Lo que ha generado una gran transmisión de información a nivel global y es en ese punto Donde se generan los problemas de seguridad. por eso a medida que las empresas crecer Deben consolidar un departamento dentro de su compañía el cual mantenga monitoreado Toda la parte de las redes y la información dentro de la compañía donde se fermenten unos Valores y una cultura en pro de la seguridad de la empresa, y entablar procesos de Capacitación para sus empleados sobre seguridad, en la mayoría de las empresas los Problemas en la parte de seguridad y perdida de información ocurren por la falta de Capacitación de sus empleados en temas de seguridad y el acceso a internet a sitios web Que no tienen nada que ver con la compañía y estos sitios tienen enlaces web que llevan A destinos donde se pueden acceder a códigos maliciosos como virus o spyware una Medida sería bloquear estos sitios web. Y otro problema que se genera con los empleados Es el mal uso de los correos electrónicos, se genera como solución ocultar los contactos Para evitar el mal uso de los correos.

Las empresas deben tener total legalidad en la compra de software y sus licencias Correspondientes ya que mucho código malicioso vienen incluido en software pirata y el Manejo de correo electrónico los piratas informáticos suelen enviar correos disfrazados Como información bancaria, los empleados tiene la necesidad de ser capacitados para Distinguir entre la página original y la plagiada.

La red de la empresa es el pilar para evitar ataques a la seguridad de la compañía y la Utilización de corta fuegos es vital ya que previene ataques maliciosos como lo son la Denegación del servicio (Dos) hay que estar conscientes que ninguna empresa está exenta De ser atacada

“Tener en cuenta que siempre se puede ser víctima de un ataque de este tipo y estar Preparado para ello. Siempre tener monitoreada la red de la empresa para estar al tanto de Cómo se comporta la transmisión de datos así poder identificar el problema y actuar rápido Antes de que pueda ocurrir un paro total en el sistema”

Con la implementación de los cortafuegos y los antivirus en conjunto pueden ser una pareja Primordial para liquidar el código malicioso, manteniendo actualizados se pueden evitar Virus y spyware los cuales dañan los equipos y nos pueden causar pérdidas económicas.

Cada día surgen nuevas modalidades de ataques por eso los departamentos de las Compañías deberán mantener los equipos escaneados y monitorearlos constantemente, Además de eso el spyware busca acceder a información de la empresa, muy distinto a los Airus que buscan dañar el equipo, en muchas ocasiones algunos tipos de spyware se

Activan cuando se ingresan unidades USB a la empresa, las cuales en su mayoría de Ocasiones provienen de los empleados de la empresa.

Lo que se busca es capacitar y generar una cultura de seguridad dentro de las empresas Un paro del sistema puede contraer perdidas millonarias para las compañías y los clientes, Generar cultura y costumbres sanas de seguridad dentro de las compañías es una inversión Que una empresa de cualquier índole debe realizar.

## ***5.4CUARTO ARTÍCULO: SEGURIDAD DE LA INFORMACION***

Link de consulta:

*[5]*

*L*as empresas hoy en día manejan la información de manera diferente y le dan una Importancia mayor y por lo mismo deben intentar que esta permanezca lo más segura Posible ya que se maneja de la misma manera que un activo tangible de la compañía, Aunque no se refleja en el bance cumple casi todas las características de un activo común, En la actualidad el modo de operación de las empresas obliga a utilizar herramientas Tecnológicas para el manejo de la información, además de esto las grandes empresas Manejan sus servicios de información de una manera no centralizada con la expansión Global y las nuevas tecnológicas la información puede proceder de manera Descentralizada, y la relación costo-beneficio en las compañías sobre sus mecanismos de Seguridad son complejos de implementar en las compañías, además muchas empresas Manejan procesos de terceros y por lo tanto información de terceros entonces todos estos Procesos deben ir de la mano de una buena seguridad pues está en juego la imagen y la Económica de las empresas.

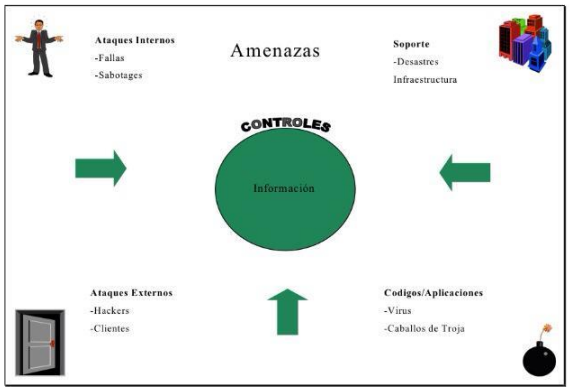
Los tres objetivos principales de la seguridad:

Confidencialidad: prevención de divulgación no autorizada de los datos

Integridad: prevención de modificación no autorizada de los datos

Disponibilidad: prevención interrupciones no autorizadas de los recursos informáticos

Procedimientos los cuales ayudan a mitigar el riesgo y las amenazas de ser víctima de un Delito informático




Es ya comprobado que la mayoría de ataques a la seguridad de una compañía es en Mayoría por las malas prácticas de sus propios empleados los cuales por falta de Capacitación realizan jugadas infantiles las cuales les puede costar millonadas a las

Compañías, y también por agentes externos, lo que lleva a las compañías a sensibilizarse Y tomar pautas y medidas para prevenir un ataque, los mecanismos más generales Independientemente de la tecnología utilizada para prevenir ataques a la seguridad son los Siguientes: Autenticación, Autorización, Administración, Auditoria y registración, Mantenimiento y la integridad de los datos

Esos mecanismos son llevados a cabo por unas técnicas las cuales permiten que estos Requisitos sean evaluados y revisados constantemente por parte de las compañías.

**Políticas de seguridad** :Las políticas de seguridad dentro de una compañía deben ser un Documento en el cual se especifiquen las pautas, los procedimientos y las conductas y muy Importante las NORMAS que deben tener los empleados respecto a la seguridad , todas Las personas de la compañía deben ser voluntarias de que no solo se quede en el papel si No que sea un ejercicio el cual se practique diariamente, las políticas deben ser revisadas Y evaluadas constantemente debido al avance de la tecnología y su fin es concientizar a Todas las personas de la compañía sobre la importancia que tiene la seguridad de la Información.

A manera de ejemplo, sin ser exhaustivo, las Políticas deben comprender:

- Definir qué es seguridad de la información, cuales son sus objetivos principales y su importancia dentro de la empresa
- Mostrar el compromiso de la alta gerencia con la misma
- Filosofía respecto al acceso a los datos
- Percepción y responsabilidades inherentes al tema
- Establecer la base para poder diseñar normas y procedimientos referidos a:
  - Organización de la seguridad
  - Clasificación y control de los datos
  - Seguridad de las personas
  - Seguridad física y ambiental
  - Plan de contingencia
  - Prevención y detección de virus
  - Administración de los computadores

***Clasificación de los datos y nivel de riesgo:***Los datos deben ser valorados y clasificarse Dependiendo de la importancia y relevancia que tengan en el modelo de negocio, después De esto se debe formalizar en un documento en cual queda constancia de cuáles son las Personas que tendrán acceso a los diferentes datos y un estudio de lo que puede pasar si Esos datos se perdieran y así realizar la clasificación.

***Seguridad física ambiental y lógica***: Se hace un énfasis en proteger la información lógica De la compañía pero no por eso se puede perder de vista la seguridad física de la Compañía, es más se deben tener controles de mantener monitoreados los equipos y más Cuando son servidores, se debe tener cámaras y puertas de acceso CDP por cerradura Electrónica, y controles sobre la seguridad del personal y de los activos de la comalia.

6. ***DISEÑO METODOLOGICO:***

***Metodología6.1. Tipo de estudio***

La investigación será básica de naturaleza descriptiva y correlacional debido que en un primer momento se ha descrito y caracterizado la dinámica de cada una de las variables de estudio.

***6.1.1 Diseño***

El diseño de la investigación fue de tipo no experimental: correlacional- transversal ya que no se manipuló ni se sometió aprueba las variables de estudio

***6.1.2 Población y muestra***

La población está constituida por 10 empresas tantos internacionales, nacionales.

La muestra estuvo conformada por 10 empleados, los cuales tienen cargos en el área administrativa de sus compañías, pero prefirieron privacidad en su identificación.

***6.1.3Método de investigación***

El método empleado en nuestro estudio fue inductivo-deductivo, con un tratamiento de los datos y un enfoque cuantitativo.

***6.1.4 Técnicas e instrumentos de recolección de datos***

Técnica de recolección de datos

La técnica utilizada fue la encuesta que permitirá recopilar la información en la muestra de estudio.

## Instrumentos de recolección de datos

Se construirá un cuestionario, para cuantificar las variables de estudio, utilizando un conjunto sistematizado de preguntas que se dirigen a un grupo predeterminado de personas que poseen la información que interesa a la presente investigación.

## Técnicas para el procesamiento de la información

Una vez recolectados los datos proporcionados por los instrumentos, se procederá al análisis técnico para el procesamiento de la información

Una vez recolectados los datos proporcionados por los instrumentos, se procederá al análisis estadístico respectivo. Los datos serán tabulados y presentados en tablas y gráficos de distribución de frecuencias.

## ***7. ESQUEMA TEMATICO***

## ***7.1 Capitulo 1 DEFINICIONES EN EL ENTORNO DE DELITOS INFORMATICOS***

### ***7.1.1 Conocer y relacionar sobre los elementos que conforman un delito en los sistemas Tecnológico de información y comunicación.***

#### ***7.1.1.1 DEFINICION DE UN DELITO INFORMATICO***

Un delito informático se entabla como una actividad marcada por la ilegalidad la cual Enmarca fases de un delito común como robo, hurto, fraude ,falsificación, perjuicio, estafa Y sabotaje, mezclados con la rama de la informática como medio para realizar estos Actos.

La (ONU) la organización de las naciones unidas

Divide los delitos informáticos en 3 secciones:

Las siguientes viñetas corresponden a la clasificación que hace la ONU sobre los delitos informáticos:

* Fraudes cometidos mediante manipulación de computadoras

* Manipulación de los datos de entrada

* Daños o modificaciones de programas o datos computarizados

Los fraudes cometidos mediante los de equipos de cómputo: Manipulación de los datos De entrada o sustracción de datos. La manipulación de programas: modificación de Programas existentes en un sistema o la inserción de nuevos programas. Manipulación de los datos de salida: Fraude efectuado por manipulación informática: también llamado Técnica del salchichón, aprovecha las iteraciones automáticas de los procesos de Cómputo. Los fraudes competidos mediante la manipulación de los datos de entrada: Como objeto: modificación de los documentos digitales. Como instrumento: uso de las

Computadoras como medio para falsificar documentos  Los daños o modificaciones de Programas o datos computarizados: Sabotaje informático: se define como una acción en La cual se modifican o eliminan datos o funciones en un equipo informático sin Autorización.

Acceso no autorizado a servicios y sistemas informáticos.

Reproducción no autorizada de programas informáticos de protección legal

### ***7.1.1.2 Actores dentro de un delito informático***

Los actores de un delito informático son los actores comunes dentro de un delito normal

Sujeto activo: aquella persona que comete el delito informático.

Sujeto pasivo: aquella persona que es víctima del delito informático

### ***7.1.1.3Cuáles son los elementos que conforman un delito en los sistemas tecnológicos de información y comunicación:***

Elementos del Tipo: Un delito informático se definido como tal y está legalmente Constituido por unos elementos materiales que lo configuran y le dan cuerpo, en tal caso De que estos elementos no estén presentes dentro de un delito informático perderá su Naturaleza esencial que revisten esas constitutiva, en tal caso no puede afirmarse ni Legalmente ni doctrinalmente que este delito sea de tal índole, la infraestructura legal de Un delito informático está constituida por: Sabotaje informático : son conductas las cuales Se basan en los daños físicos o lógicos a Través de un medio de computo , como Espionaje , copia ilegal de algún software , fraude A través de un medio informático , uso Ilegitimo de sistemas informáticos, delitos Informáticos en contra de la privacidad y datos Personales de personas o compañías. Sujetos en el Delito Informático, Sujeto pasivo es la Víctima del delito y es el ente sobre el Cual recae la conducta de la Acción o daño que Realizar el sujeto activo.

Objetos del delito: Parte Física Sistemas Informáticos Parte Lógica Sistemas Informáticos Dinero propiedad intelectual información y datos. Los delitos informáticos en su mayoría Son de tipo ocupacional ya gran parte de estos actos ocurren cuando la persona pasiva o Víctima del delito está en su jornada laboral, en la mayoría de los casos, se presentan Muchas contrariedades en la investigaciones sobre quién es el autor del delito puesto que Por la expansión de la plataforma del internet el delito puede traspasar fronteras, y al Carácter técnico de los hechos.

Hace muy poco tiempo que se están presentando las primeras denuncias por delitos de Esta índole y su perpetuación es de gran facilidad puesto que se pueden realizar en Periodos de tiempo corto y no necesitan la presencia del delincuente. Estos son delitos Que en su mayor parte causan perdidas economías relevantes para los afectados y quien Comete este delito su perfil es siempre de una persona o grupo de personas las cuales Tienen conocimientos técnicos muy amplios y una formación académica muy buena.

[6]

### ***7.1.1.4 Clasificación los delitos informáticos según frecuencia y alcance***

Exceso de acceso no autorizado: Este término se refiere a todo aquel movimiento en la Red no apropiado por parte de los empleados de una compañía, que pueda contraer en Delitos informáticos, ya sea con la abertura de links que llevan a sitios los cuales pueden Infectar los equipos y extraer información importante de la empresa, además mal manejo De las contraseñas son muy poco fiables y muy predecibles. Intercepción de datos y Comunicaciones: Las ondas de radio tienen en si la capacidad de propagarse en Cualquier dirección y dentro de un rango amplio es por esto dificil tener las transmisiones De radio en una área limitada y esto dentro de una compañía es complicado de manejar si No se tiene conocimiento por parte del departamento de TI , existen prácticas como el War- driving el cual consta en la búsqueda de redes inalámbricas lo peligroso de esta Práctica para las empresas es que se pueden interceptar las comunicaciones dentro de la Red y por si sus datos y la información en general

Intercepción de los datos: Las redes inalámbricas son inseguras por defecto una red Abierta cualquier persona puede estar dentro del área de cobertura e interceptar los datos Que se envían a la red, la amenaza es grande cuando los datos son de confidencialidad

Con un punto de acceso en una red local esta permite que cualquier estación acceda a la Red conectada y a internet si la red local está conectada a ella, es por esto que una red Inalámbrica es la puerta para que los hackers accedan al a red interna de una compañía y Además permite que tenga acceso a modificar destruir o ver datos que pueden ser Privados.

---

Destrucción de los datos: Las compañías manejan gran cantidad de información que Circula como la sangre en las venas de un ser humano como nóminas, seguro social, Banca electrónica, claves de acceso, certificados digitales...etc. pero ese flujo tiene que Ser controlado y muchas veces eliminado para evitar representaciones legales en el

Futuro es por eso que la ley les obliga a las empresas la destrucción total de los datos Para que no quede ningún rastro de ellos, y muchas veces las compañías hacen una Destrucción parcial de los datos y no se asesoran de cómo hacer una destrucción total de Los datos y esto ha causado muchos problemas.

Modificación de los datos: La modificación de los datos de una compañía puede ser un Gran problema que puede causar pérdidas millonarias en la compañía y su caso base se Consta en la alteración de cualquiera de los datos o información que maneja una Compañía como pueden ser social, banca electrónica, claves de acceso, certificados Digitales, contraseñas, balances, nominas, procesos, recetas y que estas guardadas en Bases de datos, en la nube, en archivos etc. y pueden sufrir alguna alteración. Inutilización de los datos: esta práctica consta en la destrucción de los datos informáticos Como ya se ha visto anteriormente y de la destrucción o inope ración de los artefactos Físicos que almacenan la información

Clasificación Según la Actividad Informática: Sabotaje informático Este término se refiere A aquella conducta la cual interfiere con el normal funcionamiento del hardware o el Software de un equipo informático, a medida que evolucionan estos delitos se van Volviendo más sofisticados y más difíciles de manejar el daño físico o lógico a un equipo Informático puede ser considerado un delito y grave, el daño físico puede ser causado por Incendios provocados derramamiento de líquidos sobre los equipos e introducir piezas de Aluminio dentro de los equipos causando corto circuito dentro de los mismos y dejándolos Obsoletos, pero este daño se considerara como un delito a daño de propiedad en cambio El daño lógico ha ido evolucionando de una manera sin igual y es mucho más dificil de Judicializar la destrucción, el ocultamiento u alteración de los datos contenidos dentro de Un sistema informático. Estos daños a los datos de un sistema informático pueden tener Versatilidad de formas y maneras desde la más simple hasta la más compleja, Simplemente desde desenchufar el equipo de la electricidad. Borrar documentos o Archivos hasta la utilización de programar y algoritmos complejos que se encargan de Destruir los datos

En Francia la jurisprudencia de ese país registra el caso de una empleado que programo El sistema de datos de la compañía tal que si el nombre suyo era eliminado de la lista de Empleados, se eliminarían todos los datos instantáneamente, las bombas lógicas que Son software malicioso el cual realiza su aparición en un tiempo determinado o con la Inclusión de alguna señal que pueda dar el mismo usuario del equipo, el llamado cáncer De rutinas (cáncer routine) tienen la facultan de reproducirse a sí mismos dentro de otros Programas y dañar su funcionamiento. Y él un virus una modalidad más evolucionada que hace lo mismo reproducirse en otros programas que se hallan en el mismo disco rígido y donde fue instalado y en los datos y programas posteriormente elegidos.

Fraude a través de computadoras: Son conductas que con la manipulación ilícita en la Manipulación o creación o alteración de los datos o procesos en un sistema de Información pretenden un ingreso lucrativo ilegal, en un sistema informático después de Tener el acceso indicado es muy fácil cambiar alterar datos dentro del sistema de

Información y cambiarlos por datos falsos, esta manera de realizar estos actos ilícitos en Un sistema de información se denomina manipulación del input.
Un ejemplo de esto sucedió con una empleada alamana en un banco por el año de 1983, La cual en un instante transfirió una suma importante de dinero a una amiga, la cual en un Minuto retiro la suma de dinero, esta modalidad de alterar el normal funcionamiento de un Sistema informático puede ser realizada de manera manual o utilizando programas Especiales.

“un empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor.
Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los «empleados ficticios» y los pagos realizados, no aparecieran en los listados de control.”
[6]

una similitud encontrada en este tipo de delitos es que una vez se ingresa al sistema, el ingreso se vuelve repetitivo y constante, es más hasta algunos programas especiales para este tipo de fraude tienen la capacidad de seguirse infiltrando en el sistema informático y seguir generando pérdidas, la persona que está realizando el fraude dentro de una compañía puede incluso irse de vacaciones, puede estar hasta fuera del país realizando el fraude desde una computadora personal y puede hasta morir y estos programas seguirían causando los mismos daños, cuando los sistemas de información están conectados a una red de comunicaciones entre ordenadores , a través de líneas telefónicas o de cualquier medio de comunicación , se expone a esta clase de fraudes.
Los objetos sobres los que recaen estos fraudes informáticos son datos informáticos asignados a activos y valores.

“El autor, empleado del Citibank, tenía acceso a las terminales de computaciónde la institución bancaria. Aprovechando esta circunstancia utilizó, en varias oportunidades, las terminales de los cajeros, cuando ellos se retiraban, para transferir, a través del sistema informático, fondos de distintas cuentas a su cuenta personal.
Posteriormente, retiró el dinero en otra de las sucursales del banco.
En primera instancia el Juez calificó los hechos como constitutivos del delito de hurto en forma reiterada. La fiscala de Cámara solicitó el cambio de calificación, considerando que los hechos constituían el delito de estafa.
La Cámara del crimen resolvió:
«... y contestando a la teoría fiscal, entiendo que le asiste razón al Dr. Galli en cuanto sostiene que estamos en presencia del tipo penal de hurto y no de estafa. Ello es así porque el apoderamiento lo hace el procesado y no le entrega el banco por medio de un error, requisito indispensable para poder hablar de estafa. El apoderamiento lo hace el procesado directamente, manejando el sistema de computación. De manera que no hay diferencia con la maniobra normal del cajero, que en un descuido se apodera del dinero que maneja en caja y la maniobra en estudio en donde el apoderamiento del dinero se hace mediante el manejo de la computadora...»
Como el lector advertirá, la resolución adolece de los problemas de adecuación típica a que hacíamos referencias más arriba.

En realidad, el cajero no realizó la conducta de apoderamiento que exige el tipo penal del hurto ya que recibió el dinero de manos del cajero. En el caso de que se considere que el apoderamiento se produjo en el momento en el que el autor transfirió los fondos a su cuenta, el escollo de adecuación típica insalvable deriva de la falta de la «cosa mueble» como objeto del apoderamiento exigido por el tipo penal. [6]

-

Estafas electrónicas: esta modalidad va da la mano con el uso de comprar vía internet el cual se ha triplicado en los últimos años y hay algunos países donde la legislación no cubre o no dictamina un delito por estafa vía internet.

*pesca* u *olfateo* de claves secretas: se suele engañar a aquellas personas que apenas están entrando en la red y los delincuentes tratan de acceder a su información personal haciendo pasar por policía, y como proveedores de servicio , existen programas los cuales pueden ser utilizados para identificar claves de acceso de usuarios.

Blanqueo de dinero: la red es el nuevo medio donde se hace la trasferencia electrónica de mercancías o dinero que vienen de delitos como el narcotráfico y se utiliza para ocultar transacciones.

Copia ilegal del software espionaje informático: se entablan las conductas que conllevan a obtener datos de un sistema de información de manera ilegal, comúnmente pasa con datos de investigaciones, información sensible de una compañía , listas de clientes balances y en algunos casos se suele frecuentar el apoderamiento de un producto de software el cual tiene un valor económico significativo.

Infracción de los derechos de autor: se define como la interpretación en los conceptos de copia, distribución no autorizada, están atentamente vigilados por la jurisprudencia de muchos países.

Infracción del copyright de bases de datos: no existe una protección uniforme de las bases de datos y se permite que los usuarios hagan una descarga simple de ficheros que están dentro del sistema pero se prohíbe el replicado de las bases de datos y copias masivas de la información

Acceso no autorizado: Se tipifica que el solo hecho de poseer el passwords para el acceso a información privada de una persona debe ser tipificado como un delito
Esta tipificación se refiere a quién, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

La siguiente numeración hace referencia a Conductas son consideradas como agravantes En la divulgación de archivos con el siguiente contenido

1. El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.
2. Las circunstancias de la víctima: menor de edad o incapaz.

Donde también se adiciona la interceptación de las comunicaciones donde por cualquier medio sea transmisión escucha grabación de imagen y de sonido puede ser una conducta Agravante, la pornografía infantil y su distribución está en aumento lo que ha llevado a la Unión de muchos países y se ha intensificado la lucha contra la misma por transmisión y Posesión se ha aumento de 1 a 400 casos.

La siguiente numeración corresponde a la Clasificación Según el Instrumento, Medio o Fin U Objetivo: En Esta clasificación se encuentran las conductas delictivas que se valen de Un equipo informático como medio método o símbolo en la ejecución del ilícito.

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
2. Variación de los activos y pasivos en la situación contable de las empresas.
3. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
4. Lectura, sustracción o copiado de información confidencial.
5. Modificación de datos tanto en la entrada como en la salida.
6. Aprovechamiento indebido o violación de un código para penetrar a un sistema Introduciendo instrucciones inapropiadas.
7. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta Bancaria apócrifa.
8. Uso no autorizado de programas de cómputo.
9. Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los Programas.
10. Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
11. Obtención de información residual impresa en papel luego de la ejecución de trabajos.
12. Acceso a áreas informatizadas en forma no autorizada.
13. Intervención en las líneas de comunicación de datos o teleproceso.

La siguiente numeración corresponde a la clasificación de los delitos informáticos como fin U objetivo: En esta categoría se entablan aquellas conductas delictivas que van contra el Equipo, accesorio u programas de ente físico.

1. Programación de instrucciones que producen un bloqueo total al sistema.
2. Destrucción de programas por cualquier método.
3. Daño a la memoria.
4. Atentado físico contra la máquina o sus accesorios.
5. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los Centros neurálgicos computarizados.
6. Secuestro de soportes magnéticos entre los que figure información valiosa con fines De chantaje (pago de rescate, etc.).

LA siguiente numeración corresponde a la Clasificación según Actividades Delictivas Graves: La red da cabida a que se ejecuten delitos de la siguiente índole

1. Terrorismo: envió de mensajes anónimos y envió de mensajes para la ecuación de los planes en otros países
2. Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

3. Espionaje: es el acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico entidades la cual manejan información clasificada
4. Espionaje industrial: acceso a sistemas de información de compañías donde se plagian diseños industriales, fórmulas de producción, sistemas de fabricación

Referencia bibliográfica

[6]

## *7.2 Identificación de los delitos más comunes en el campo de la informática*

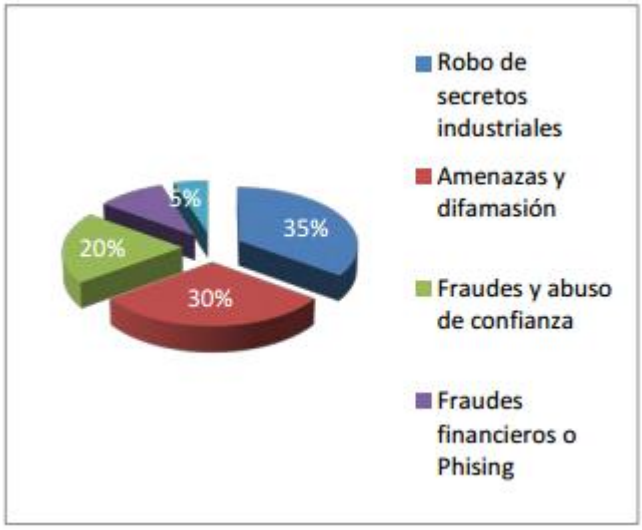
### *7.2.1 cifras de delitos informáticos internacionales y nacionales*

En Colombia los delitos informáticos han aumentado sus cifras deliberadamente en los Últimos años y es el tercer país en Sudamérica con más infracciones relacionadas con Medios informáticos e información que tiene que ver con la internet, se calcula que se Hacen 187 denuncias mensuales relacionadas con delitos informáticos, el delito más Cometido en el país es el fraude a entidades bancarias y después de Brasil Colombia es El más afectado, esta modalidad explican expertos de la Fiscalía, van en aumento y Consta en acceder a bases de datos de bancos u otras entidades sin permiso, sustraer Archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas Bancarias.

Ejemplos como los ocurridos en la ciudad de Cali en el departamento del valle fue el de Un empleado el cual era hacia parte de la directiva de la entidad bancaria donde tenía Acceso a el listado de los diferentes clientes y desde el año 2009 retiro cerca de 300 Millones de pesos colombianos a sus respectivos clientes .

En Colombia a pesar de los ataques que ha sufrido estados unidos y sus ciudadanos los Cuales fueron víctimas de seguimientos e intercepción de sus datos y comunicaciones no Hay una gran conciencia en la comunidad y tampoco en las compañías, se reporta que en Colombia las empresas pierden de cerca de 40 millones de dólares anuales por delitos Informáticos, además de que estas prácticas pararon de un 36% al 56% "Según datos de La compañía Andina Digital Security en el último año cerca de 10 millones de Colombianos han sido víctimas de algún delito informático. Pero la problemática va más Allá, el 99.9% de las víctimas de estas modalidades delictivas no las denuncian, Entendiendo así que las denuncias por esta causa no superan la cifra de 23.000, según El Colegio Colombiano de Juristas[7]

### *7.2.2 delitos informáticos más comunes en Colombia*




Según un estudio de MaTTica, laboratorio de cómputo forense de América Latina. Colombia es el noveno país generador de spam a nivel mundial y ocupa el tercer Lugar en Latinoamérica pero esto no tiene una razón proporcional indicando que nuestro País sea Inseguro, sino que es más propenso, por ejemplo Brasil es el país en Latinoamérica que Reporta más ataques cibernéticos. Pero el problema radica en la Capacidad tecnológica En el país , es muy impresionante y esto comprueba la manera Significativa que está Creciendo la tecnología en Colombia encontrarse novena a nivel Mundial cerca de china y Rusia países donde se crean los ataques informáticos más Difíciles de identificar , Colombia es el país que más le apuesta a la seguridad informática Después de Brasil Aunque estas cifras no son del todo confiables ya que las empresas Por medio a ser Desprestigiadas no reportar delitos informáticos , además de esto porque Todos sus Sistemas de información serian revisados así que prefieren omitir y no Denunciar.

[8]

### ***7.2.3 clasificación de los delitos más comunes en Colombia y los más destructivos para las empresas***

La siguiente numeración corresponde a la clasificaron de los delitos informáticos mas comunes en Colombia.

1. Robo de secretos industriales: en el entorno industrial los secretos industriales como recetas, preparados, procesos se guardan celosamente en pro de la competencia, cuando estos secretos caen en manos de personas ajenas a la compañía o la competencia los daños pueden ser irreparables.

2. Fraudes financieros o phishing: las compañías guardan información de todo tipo y entre ellas se encuentran la de los balances, transacciones, cuentas bancarias etc. por medio del phisihing se puede tener acceso a claves de cuentas de usuario, claves de cuentas bancarias y esto puede causar un daño económico considerable en las compañías.

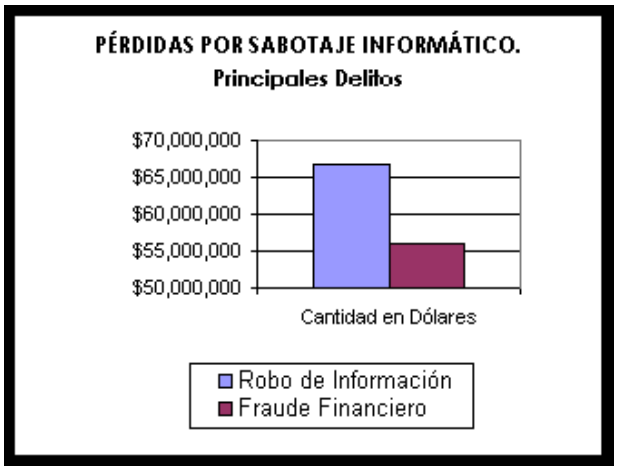
3. Fraudes y abuso de confianza: cuando los empleados de las empresas no utilizan la red para beneficios de la compañía si no para saciar sus ocios muchas veces tienden a infectar los equipos con virus y ponen en riesgo la información que manejan.

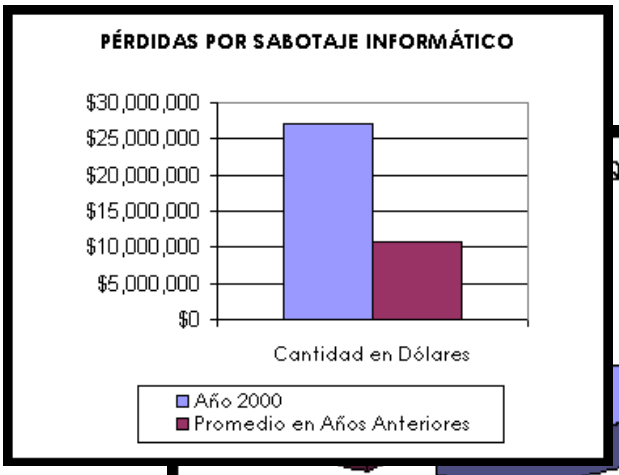
4. Amenazas y difamación: este en las empresas no suelen tener mucha relevancia pero siendo así no están exceptos de ser perjudiciales por el tema de imagen y seguridad de los empleados.

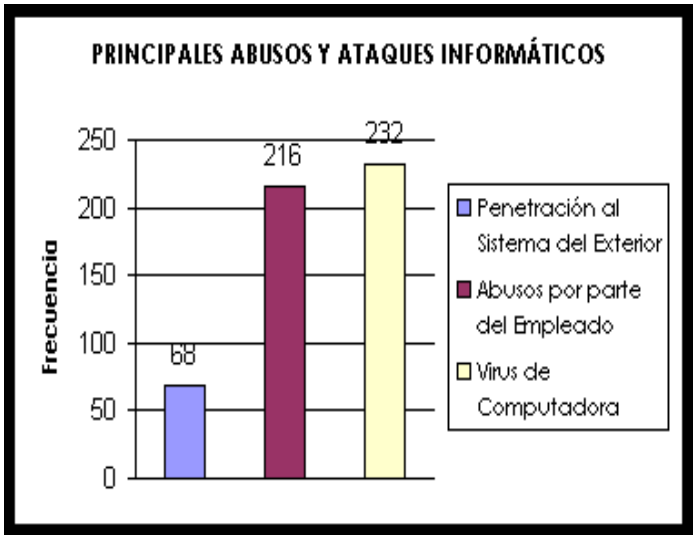
Según El Instituto de Seguridad de Computadoras (CSI) institución fundada hace más de 5 años encargada de revisar anualmente delitos sobre la seguridad informativa y Crímenes cometidos a través de equipos informáticos, anual denominado "Estudio de Seguridad y Delitos Informáticos" realizado a un total de 273 Instituciones principalmente Grandes Corporaciones y Agencias del Gobierno. En esta investigación también participo El (FBI) este estudio se basa en proveer conocimiento sobre los delitos informáticos y Determinar su alcance en los estados unidos

Este cuadro corresponde a información sobre Violaciones a la seguridad informática en Estados Unidos.

| | PORCENTAJE (%) |
|---|---|
| No reportaron Violaciones de Seguridad | 10% no reportan |
|  Reportaron Violaciones de Seguridad | 90%reportan violaciones en la seguridad de sus sistemas de información |
| 1.Las violaciones más comunes son: ***virus de computadoras***, robo de computadoras portátiles o abusos por parte de los empleados<br><br>2. Pérdidas Financieras.<br>74% reconocieron pérdidas financieras relacionadas con delitos informáticosascendieron a $265, 589,940 (el promedio total anual durante los últimos tres años era $120, 240,180). | |






Las siguientes viñetas corresponden a las conclusiones de los gráficos anteriores:

- 6I encuestados cuantificaron pérdidas relacionadas con delitos informáticos de $27, 148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10, 848,850.
- Las perdidas más importantes ocurrieron a través del robo de información
- (66 encuestados reportaron $66, 708,000) y el fraude financiero (53 encuestados informaron $55, 996,000).
- Los encuestados concuerdan en que estas pérdidas son producto del acceso no autorizado a sus sistemas de información.
- 71% de los encuestados descubrieron acceso desautorizado por personas dentro de la empres
- 25% de encuestados descubrieron penetración al sistema del exterior.
- 79% descubrieron el abuso del empleado por accesos no permitidos y uso inapropiado de la red ).
- 85% descubrieron virus de computadoras.
- 93% de encuestados tienen sitios de WWW.
- 43% maneja el comercio electrónico en sus sitios (en 1999, sólo era un 30%).
- 19% experimentaron accesos no autorizados o inapropiados en los últimos doce meses.
- 32% dijeron que ellos no sabían si hubo o no, acceso no autorizado o inapropiado.
- 35% reconocieron haber tenido ataques, reportando de dos a cinco incidentes.
- 19% reportaron diez o más incidentes.
- 64% reconocieron ataques reportados por vandalismo de la web
- 8% reportaron robo de información a través de transacciones.
- 3% reportaron fraude financiero.[9]

## ***7.3 clasificar los delitos informáticos en Colombia con referencia a la ley 1273 del 2009***

### 7.3.1 Entrevista a Andrés Ormaza sobre la ley 1273 y Habeas Data

Andrés Eduardo Ormaza Mejía es abogado bogotano egresado de **la Universidad** Santo Tomás, especialista en Derecho Penal y Criminología de la Universidad Externado de Colombia. Ponente de la ley. Experiencia de 12 años asesora al gobierno y al ministerio De justicia sobre delitos transnacionales, lavado de activos tráfico de personas cibercrime.

¿Cómo empezó la idea de formar la ley 1273 del 2009 en Colombia?

2006 estados americanos empieza a estudiar el tema de seguridad de la información y se Genera una estrategia hemisférica en conjunto con la cancillería, marco de referencia de Cibercrime esto funciono de carambola y por eso se pudo implementar en territorio Colombiano

¿Existen vacíos dentro de la ley, se cambió la ley en su elaboración?

Se presentaron inicialmente dos proyectos de ley:

1. Generar conductas de agravación y mayor pena frente a delitos que ya Existían estafa por medios informáticos hurto.
2. Un nuevo bien jurídico de la protección de la información esto causo un Revolcón al congreso en los cuales se aprobaron 10 delitos que no se Conocían y eran llamativos porque eran conductas totalmente novedosas y Lo que se hizo fue una mezcla de los dos proyectos. Donde se tipificaba el Delito como medio para cometer un delito el uso de un equipo informático o Como fin porque lo que se vulnera es la protección de la información.

¿Se ven errores en la justicia penal, nace una ley nueva en una temática nueva para el País existen dudas por todo la comunidad, nuestro sistema judicial como está preparado Para implementar la ley por ejemplo defensores y fiscales están preparados para Implementar la ley?

Es un proceso que ojala no sea muy largo, la capacitación de adaptación que se tienen Que hacer tiene que ser muy fuerte y a lo largo y ancho del territorio nacional. La ley se Generó por el estudio de un juez de un municipio del Tolima que le dedico mucho estudio, Mucho tiempo al análisis y la tipificación y exclusión de estas conductas de un delito Normal. La aplicación de la ley depende de la capacitación de quien la aplica, creo que en Ese momento hay muchas personas a nivel operativo que pueden tener conocimiento Pero a nivel de fiscales y jueves falta mucho todavía.

¿Cómo se determina que es software malicioso y que no es, si en la ley no está escrito, ni Especificado?

Había un capítulo de definiciones donde se definían estos criterios pero se sugiero extraer Este capítulo, Porque estos términos son cambiantes y se tendría que presentar un Proyecto para actualizar las definiciones, posibilidad por un decreto o un manual hacer un Listado de definiciones para el juez o el fiscal para generalizar las conductas.

¿Cómo se tipifica una conducta?

Podemos hacer una conducta que se encuadra en las descripciones intención de cometer Un delito, Se valora la intención en todo momento

¿Cómo se mide la intención?

Se tienen que precisar elementos para definir la intención delito. El que deliberadamente y Con propósito ilícito produjera traficara etc. La ley contempla el análisis de la intención en La conducta para deliberar si se trata de un delito o no.

¿Qué opina del Artículo el de interceptación de datos informáticos?

Se pretende aclarar que El que sin orden judicial intercepte datos informáticos y Emisiones electromagnéticas intercepte datos *smurf* para interceptar de lo de la red o un

Scanner a una red perimetral, la ley por ser novedosa por ser reciente para los Funcionarios de policía judicial para fiscales y cuales requiere depuración de Interpretación para tener en cuenta cuando se está incurriendo en una violación de la Privacidad.

¿Tiene que haber una acusación o me da por usar un *smurfer* o *escáner* de red y solo Por ver que yo estoy interceptando un dato sin hacer nada con el me pueden meter a la Cárcel?

Con esa situación estas atentando con la confidencialidad y la integridad de los datos, de Ser que no estés atentando con la privacidad y confidencialidad y no tengas una Intención de atentar contra un bien jurídico no transciende contra el derecho penal El solo Hecho de tenerlos no te da una responsabilidad.

¿Si yo accedo al correo de un amigo pero no hago nada con la información que veo Puedo estar infringiendo la ley?

Claro por qué está estipulado claramente en la ley que en lo inicialmente acordado o sin Autorización no puedo acceder a información privada de alguna persona.

¿Por qué un proceso para un delito informático se toma como una querella no como Daños y delito de daños y perjuicios?

Se inicia como una denuncia normal, querellable se refiere a que en cualquier momento Puedo retirar la denuncia y por lo tanto se toma como algo así.

¿Esta ley como interactúa con la comunidad?

Básicamente la idea es trabajar en tres ejes Protección de los datos e ir de la mano con la comunidad intentando llenar esos vacíos sobre la ley.

¿Tu como vez el apoyo en los últimos dos años nos ha brindado la OEA?

Internacionalmente se ha tomado conciencia colectiva después de los ataques a Estonia y esto fue el detonante de ciberterrorismo tangible lo que busca unificar las conductas Para poderlas sancionar.

¿Se contó con apoyo de gente especializada y de aspecto internacional en la elaboración De la ley?

Si obvio no cualquier nos podía aportar conceptos, era gente muy especializada en el Tema y muy profesional.

¿Porque la ley no se tipifica el spam como uno de los delitos?

Se tuvo en cuenta pero como sugerencia salió el spam por la poca capacidad logística por Esta clase de incidencia, Por medio del spam se puede llegar a conductas como el Phising, pero en estos casos el spam deja de ser una conducta inmersa y si se considera Un delito informático no por ataque vía spam si no por daño informático.

¿Cuándo se hace un Test de vulnerabilidad, contrato de confidencialidad, cuando yo Hago un proceso metodologías practicas lo que es el scanner donde yo trato si los Puertos están abiertos que servicios están disponibles hay delito?

Esta conducta no se puede judicializar en conclusión No existe delito.

¿Utilización de herramientas ofensivas y defensivas puedo incurrir en un delito??

No se considera que por que yo tenga herramientas que se consideren como un delito la Portabilidad no se judicializa, Solo propósitos son los tenidos en cuenta.

¿En suplantaciones de páginas web existe un delito?

Estas manejando lo que se quiere que la persona que desconoce que la página web esta Suplantada entregue, si hay delito por que la voluntad de la persona está viciado y no Sabe que está dando permiso y con un fin distinto que el que tiene en mente cualquier Conducta normal por medio de un medio telemático se incrementa al máximo.

¿Cuándo en mi empresa utilizan programas de administración remota de equipos y se Utilizan con fines delictivos mi empresa se vería perjudicada?

No hay delito alguno por que una analogía podría hacer un carnicero que tiene un cuchillo Para cortar la carne y otra persona lo utiliza para cometer un homicidio la culpa es de Quien realiza el acto no la herramienta.

¿Responsabilidad de usuarios de computadores zombis que atacan a servidores?

No se configurara como un delito.

¿Los Proceso por delitos informáticos tienen capacitación o es independiente?

Fiscales especializados los que se encargan de llevar estos casos.

¿Si un argentino comete un delito en Colombia y en argentina no judicializan este tipo de Conductas se puede extraditar al argentino?

Si en los dos países está tipificada la ley contra el delito se puede extraditar si no está Tipificada la conducta es muy dificil.

¿Se podría pensar que los organismos del estado tienen la potestad de chuzar a las Personas?

Esta ley cobija a todos los colombianos incluyendo cuerpos del estado.

[10]

***7.3.2 como la ley 1273 del 2009 en Colombia podría mejorar***

Después de analizar la ley 1273 del 2009 y de recopilar información sobre cómo está Funcionando y cuales han sido sus críticas y cuáles pueden ser esos vacíos jurídicos que Tiene la ley se analizó:

En Colombia desde el 2009 se creó una ley la cual tipifico 10 conductas como un delito en Contra de la información utilizando medios informáticos ya sea como medio o como fin, Pero a pesar de esto hay un gran desconocimiento por parte de la comunidad referente a Esta ley y Colombia es un país el cual con el avance del tiempo ha ido de la mano con la Tecnología y se encuentra entre los países de Latinoamérica que más ha evolucionado en El contexto tecnológico, tanto que ya se dio el primer paso a la creación de una ley.

En la ley 1273 del 2009 se plasmaron los delitos que se pueden considerar como Informático o de la información, pero la misma ley no define algunos términos que para la Comunidad por conocimiento general deberían saber a la hora de la aplicación, pero Según sus legisladores estos términos tiene la versatilidad de cambiar constantemente y Serian obsoletos en algunos años por lo tanto no fueron incluidos, pero si es dificil para el Ciudadano común denunciar un delito informático si no sabe que es y cuáles son sus Parámetros y definiciones, otro factor es el desconocimiento por parte de las personas Que tienen que impartir justicia como los fiscales que muchas veces tratan los delitos Informáticos o de la información como delitos comunes absteniéndose de utilizar la ley la Cual exalta las penas y contiene penas más fuertes y severas pero que a veces por falta De capacitación se quedan en el limbo, también la falta de socialización de la ley en la Comunidad en general pero ¿Por qué pasa esto? El gobierno debería publicitar esta ley y Mostrarle a la comunidad su alcance tanto para evitar que se cometan estos actos y para Promover la denuncia de los mismos

Se concluye que la ley flaquea en 3 aspectos claves como lo son las definiciones, la forma En que se está ejecutando y en la socialización de la misma, pueden parecer criticas Severa no obstante Colombia ha dado el primer paso para tipificar estos delitos y poderlos Juzgar cosa que algunos países todavía no han hecho, y eso nos lleva a un contexto de Actualización de adaptación y con el tiempo esta ley será mejorada y mejor aplicada.

## ***7.4 sentencias y normas de la corte constitucional con relación a la ley 1273 del 2009 y análisis de normas aplicadas a la informática forense***

### ***7.4.1 sentencias ejecutadas por el gobierno colombiano en relación a la ley 1273 del 2009***

Según la unidad de delitos informáticos de CTI reporta unnúmero de casos abiertos o en Proceso de investigación en la actualidad con relación a la ley 1273 del 2009

- En el siguiente cuadro se encontraran números de casos abiertos o en Investigación de la ley 1273 del 2009 en Colombia Según la unidad de delitos Informáticos de CTI

| DESCRIPCION DE LA ACTUACION | Vienen | Asignadas | Total Practicadas | Canceladas | Pendientes | Practicadas Efectivas |
|---|---|---|---|---|---|---|
| ACCESO ABUSIVO A UN SISTEMA INFORMATICO | 0 | 2 | 0 | 0 | 2 | 0 |
| VIOLACION DE DATOS PERSONALES | 0 | 18 | 18 | 0 | 0 | 18 |
| HURTO POR MEDIOS INFORMATICOS y SEMEJANTES. | 2 | 50 | 20 | 2 | 30 | 17 |

Conclusiones del cuadro: Se identifica en el cuadro que el hurto por medios informáticos (Artículo 269 I) Es el tipo de delito informático que más investigaciones procesa con un Numero de 50 Investigaciones por encima de las 18 que tiene la violación de de datos Personales (Artículo 269 f) y tan solo 2 casos de acceso abusivo a un sistema informático (Artículo 269 A) Con la implementación de esta ley la unidad de delitos informáticos del CTI Tuvo en Revuelo imaginado, puesto que las metodologías y procedimientos para la Recolección de La evidencia lógica y digital a conllevado a la capacitación del personal Técnico, para Adecuarse a lo que manejan otros países como por ejemplo estados unidos Entre otros.

[11]

- En el siguiente cuadro se observaran número de casos relacionados con la ley 1273 del 2009 en diferentes departamentos del estado colombiano

| UNIDAD POLICIAL | ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO | ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES | ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES | ARTÍCULO 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES | ARTÍCULO 2691. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS | TOTAL |
|---|---|---|---|---|---|---|
| CALDAS | | | | 6 | | 6 |
| CESAR | | | | 1 | | 1 |
| MAGDALENA | 4 | | | 12 | | 16 |
| MAGDALENA MEDIO | | | | 5 | | 5 |
| META | | | | 1 | | 1 |
| NARIÑO | | | | 1 | | 1 |
| RISARALDA | 1 | | | | | 1 |
| VALLE | 1 | | | 4 | | 5 |
| M. BUCARAMANGA | | | | 1 | | 1 |
| M. CALI | 1 | 1 | | 65 | 6 | 73 |
| M. BARRANQUILLA | | | | 11 | | 11 |
| M. BOGOTÁ | | | | 25 | 1 | 26 |
| M. CÚCUTA | | | | 45 | | 45 |
| M. MEDELLÍN | | | | 6 | | 6 |
| URABÁ | | | 1 | 6 | | 7 |
| BOYACÁ | | | | 31 | | 31 |
| TOTAL | 7 | 1 | 1 | 220 | 7 | 236 |

INFORMACION EXTRAIDA DEL ISTEMA SIEDCO EL DIA 05 DE ENERO DE 2010, 15:00 HORAS, SUJETA A VARIACIÓN POR DENUNCIAS QUE INGRESAN POR SIDENCO AL SISTEMA PENAL ORAL ACUSATORIO.

Referencia bibliográfica

[11]

***7.4.2 cómo se tratan los delitos informáticos en Colombia que ocurren con más frecuencia según la ley 1273 del 2009***

Artículo 269I: *Hurto por medios informáticos y semejantes*. El que, superando medidas de Seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un Sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o Suplantando a un usuario ante los sistemas de autenticación y de autorización Establecidos, incurrirá en las penas señaladas en el artículo 240 de la ley 1273 del 2009.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES: El que, sin estar facultado para Ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, Intercambie, envíe, compre, intercepte, divulgue, modifique p emplee códigos personales, Datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, Incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en Multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, Sin autorización o por fuera de lo acordado, acceda en todo o en parte a un Sistema informático protegido o no con una medida de seguridad, o se Mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo Derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a Noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales Mensuales vigentes.

[12]

***7.4.3 clasificación de las sentencias que imprime la ley 1207 del 2009 en Colombia***

- En el siguiente cuadro se clasificaran las sentencias más penas más fuertes y más leves que impone la ley 1207 del 2009 en Colombia

| ARTICULO | MESES EN PRISION | SANCION MONETARIA |
|---|---|---|
| Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, Con ánimo de lucro y valiéndose de alguna Manipulación informática o Artificio Semejante, consiga la Transferencia no Consentida de cualquier Activo en Perjuicio de un tercero, Siempre que la conducta no Constituya delito Sancionado con pena más Grave. | Se incurrirá en pena de Prisión de cuarenta y Ocho (48) a ciento veinte (120) meses | Multa de 200 a 1500 Salarios Mínimos legales mensuales Vigentes. |
| Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El Que con objeto ilícito y sin Estar facultado para ello, Diseñe, desarrolle, trafique, Venda, ejecute, programe o Envíe páginas Electrónicas, enlaces o Ventanas emergentes. Siempre que la conducta no Constituya delito Sancionado con pena más Grave. En la misma sanción | incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses | multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no Constituya delito sancionado con pena más grave. |

| | | |
|---|---|---|
| Incurrirá el que modifique el Sistema de resolución de Nombres de dominio, de tal Manera que haga entrar al Usuario a una IP Diferente en la creencia de Que acceda a su banco o a Otro sitio personal o de Confianza, siempre que la Conducta no constituya Delito sancionado con pena Más grave. la pena Señalada en los dos incisos Anteriores se agravará de Una Tercera parte a la mitad, si Para consumarlo el agente Ha reclutado víctimas en La cadena del delito.<br><br>Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El Que, sin estar facultado Para ello, impida u Obstaculice El funcionamiento o el Acceso normal a un Sistema informático, a los Datos informáticos allí Contenidos, o a una red de Telecomunicaciones | incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses | multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado Con una pena mayor. |
| Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin Orden judicial previa Intercepte datos Informáticos en su origen, Destino o en el Interior de un sistema Informático, o las emisiones Electromagnéticas Provenientes de un sistema Informático que los | Pena de Prisión de treinta y seis (36) a setenta y dos (72) meses. | Este es el delito el cual tiene una condena más leve y no tiene multas salariales |

| | | |
|---|---|---|
| Trasporte | | |

[13]

***7.5 consultar y relaciones sentencias de la corte constitucional colombia con respecto a la ley 1273 del 2009 y consultar y relacionar conceptos sobre informática forense***

***¿Qué es la Informática Forense?*** En algunas definiciones se presenta como la ciencia Que preserva, obtiene y presenta los datos procesados electrónicamente y guardados en Un medio computacional.

Teniendo en cuenta que no todas los delitos son iguales , por lo tanto sus investigaciones No son iguales no se es posible describir un procedimiento único para la recolección de Evidencias, pero si existen unos parámetros y unas metodologías para la recolección de Evidencia digital las cuales se citaran a continuación

Planeación, recolección, aseguramiento, análisis y presentación de la Evidencia Digital , Planeación: como primer paso dentro de la planeación consta de detectar el incidente y Consiste en individualizar los actores tanto usuarios como las maquinas o medios Informáticos en los cuales se realizó la acción del delito, y cuál fue la interacción de los Usuarios con el sistema para tener una percepción de la contaminación de la escena, Como segundo paso es la familiarización técnica y la valoración sobre qué tipo De sistemas informáticos se usan, qué tipo de registros generan, si se cuenta con Políticas de seguridad o no y quiénes son responsables del funcionamiento de los equipos Y los servicios de la organización, se debe describir la escena definiendo nombres de Usuarios y roles además de información gráfica como fotos y videos de la escena que se Describirán más adelante como evidencia digital.

Recolección: Esta es la etapa más importante, es la recolección y la conservación de la Información garantizando los requisitos fijados por la ley 527 de la legislación colombiana Como complemento probatorio se deberá tener una copia exacta bit a bit de los sistemas De información los cuales pertenezcan a la investigación.

Utilización*sniffers* y *honeypots*, para recolectar nuevas pruebas que permitan o bien Identificar al autor del delito o tener más evidencia.
Teniendo en cuenta la hipótesis planteada en la etapa de planeación, se debe priorizar y Ponderar la información recolectada y la información es recolectada siempre de lo más Volátil a lo menos volátil

Se deben manejar diferentes niveles de abstracción de la información debe estar Presente en su nivel mal alto como en el más bajo y estas herramientas deben ser Capaces de interpretar dicho contenido, Se debe extraer una imagen bit a bit de la Información, No se puede modificar el medio original
La aplicación no debe cambiar de ninguna manera el medio original.

Los resultados deben analizarse según criterios científicos y deben ser verificados
Y se procederá a: Examinar el estado general del sistema: la memoria RAM de un Computador, la lista de procesos en ejecución y el estado de la red.
Realizar duplicados forenses, Desarrollar scripts y aplicaciones para automatizar la Recolección, Se recomienda hacer un proceso de copia de imagen mientras el equipo Esta encendido para no perder ningún tipo de información.

Preservación y aseguramiento de la evidencia digital:

Consta de garantizar los requisitos que impone la ley 527 que valora la información Obtenida y que precede los siguiente "… habrá de tenerse en cuenta la confiabilidad en la Forma en la que se haya conservado la integridad de la información y la forma en la que Se identifique a su iniciador".

Verificación de la integridad de la información y la alteración de la misma en Colombia Existen entidades de certificación quienes garantizan que esta información sea de utilidad En algún proceso

En la ley 527 de 1999 "Cuando una firma digital haya sido fijada en un mensaje de datos Se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de Datos y de ser vinculado con el contenido del mismo. [14]

**El análisis de la evidencia digital**

Este punto consiste en analizar la evidencia recolectada por un experto en las áreas Involucradas. Se sugiere realizar dos copias de la información y distribuirlas a los expertos Para su análisis y manteniendo el respaldo de la información recolectada.

Una parte importante y que siempre puede ser un obstáculo en la recolección de Información redundante es la información que este encriptada la cual se debe filtrar y Aunque es complejo se debe realizar.

Clasificación de la evidencia digital
Es el proceso por el cual se buscan características que pueden ser utilizadas para Describirla en términos generales y distinguirla de especímenes similares
Esta clasificación es útil si con ella se puede describir el delito y tener información adicional acerca del mismo.

Ejemplo

"El investigador puede examinar cómo funciona un programa para clasificarlo y algunas Veces individualizarlo. Por ejemplo, un programa que inesperadamente transfiere Información valiosa desde un computador confiable a una locación remota podría ser Clasificado como un caballo de Troya y puede ser individualizado por la localización Remota a la que transfiere la información.

Características: los nombres de archivo, extensiones e inclusive los encabezados internos Que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la Clasificación de la evidencia digital."[15]

Los delitos informáticos tienen la característica de las escenas del crimen pueden estar Distribuidas en diferentes lugares, sistemas, horario y que pueden incluso estar Presentados en jurisdicciones diferentes el cual impide constantemente la verificación del Cuándo como donde, y por qué se presentaron los hechos

Además gran parte de estos delitos en Colombia son realizados desde cafés internet por La falta de regulación y los inconvenientes que se presentan muchas de estas conductas Quedan en el anonimato.

**Recolección**
**Presentación de la Evidencia Digital**

Este es el punto donde toda la evidencia digital recolectada debe tener un sentido Probatorio y ser interpretada en una corte, es decir la información puede ser presentada Tal cual fue recolectada, o dar un enfoque y una especia de resumen de los datos que Más relevancia se encontraron en la investigación, y presentando el porqué de la Interpretación y los aspectos técnicos en la recolección de la información
Clasificación la evidencia para su presentación ante una corte, identificando si los datos:
Verifican los datos y teorías existentes (Evidencia que inculpa).
Contradicen los datos y teorías existentes (Evidencia que exculpa).
Muestran signos de manipulaciones para esconder otros datos. Aunque en Colombia no Existen procedimientos de cómo se debe presentar la evidencia para ser presentada en Una corte lo cual causa problemas en la interpretación de los resultados por falta del Conocimiento técnico y del lenguaje utilizado y de la poca capacitación de los jueces los Cuales desconocen los términos y las conductas tipificadas sobre delitos en los sistemas De información.

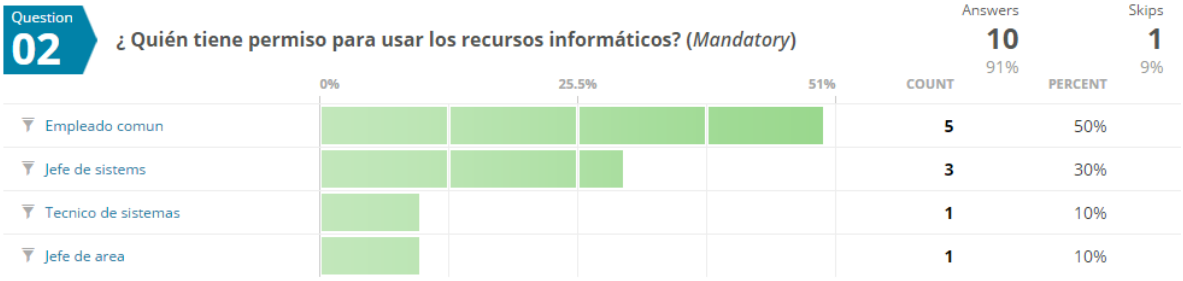
**Conclusiones**

La evidencia digital debe ser eficientemente recopilada y manejada de la mejor manera y Después clasificar lo importante y saber interpretarla para presentarla posteriormente y Que sea admisible ante una corte, Para cumplir estas expectativas se deben contar con
Los equipos y el personal calificado Para la recolección de la información
En Colombia se debería tener en cuenta formar un escuadrón el cual se encargue de Investigar delitos de esta índole.

## ***7.6 análisis y relación políticas y normas utilizadas por diferentes compañías***

### ***7.6.1 Encuesta a Grandes, medianas y pequeñas compañías para analizar y relacionar normas y políticas utilizadas***

Están son las respuestas a 23 preguntas que respondieron 10 empresas



Question **03** ¿ Quién esta autorizado a conceder acceso y a aprobar los usos? (*Mandatory*)

Answers **10** 91%

Skips **1** 9%

| | | |
|---|---|---|
| 113,433,212 | jefe de sistemas | Tuesday, Dec 30th 8:37AM |
| 113,273,018 | Administrador del sistema | Saturday, Dec 27th 11:49AM |
| 113,269,749 | Jefe de Sistemas | Saturday, Dec 27th 10:36AM |
| 113,268,680 | La responsable del área de riesgos | Saturday, Dec 27th 10:15AM |
| 113,268,302 | El gerente y los que su cargo los autorice | Saturday, Dec 27th 10:07AM |
| 113,267,860 | (Jefe de Sistemas) | Saturday, Dec 27th 9:58AM |
| 113,267,506 | Gerente Adminsitrativa Administrador Informatico | Saturday, Dec 27th 9:44AM |
| 112,997,086 | Jefe de area, Jefe de sistemas | Tuesday, Dec 23rd 1:19PM |
| 112,931,859 | JEFE DE SISTEMA OFICINA PRINCIPAL ARGENTINA | Monday, Dec 22nd 3:59PM |
| 112,920,356 | La responsable del área de riesgos | Monday, Dec 22nd 2:02PM |

Question **04**

**¿ Quién tiene privilegios de administración del sistema? (*Mandatory*)**

Answers **10** 91%

Skips **1** 9%

| | | |
|---|---|---|
| 113,433,212 | jefe de sistemas | Tuesday, Dec 30th 8:37AM |
| 113,273,018 | Administrador del sistema | Saturday, Dec 27th 11:49AM |
| 113,269,749 | Jefe de Sistemas | Saturday, Dec 27th 10:36AM |
| 113,268,680 | El gerente | Saturday, Dec 27th 10:15AM |
| 113,268,302 | El gerente y los encargados de las diferentes dependencias | Saturday, Dec 27th 10:07AM |
| 113,267,860 | (Jefe de Sistemas) | Saturday, Dec 27th 9:58AM |
| 113,267,506 | Administrador Informatico | Saturday, Dec 27th 9:44AM |
| 112,997,086 | Administrador del Sistema | Tuesday, Dec 23rd 1:19PM |
| 112,931,859 | GERENTE | Monday, Dec 22nd 3:59PM |
| 112,920,356 | EL GERENTE | Monday, Dec 22nd 2:02PM |

Question **05**

**¿ Como se maneja la información confidencial? (*Mandatory*)**

Answers **10** 91%

Skips **1** 9%

| | | |
|---|---|---|
| 113,433,212 | encriptada | Tuesday, Dec 30th 8:37AM |
| 113,273,018 | Es ckasificado | Saturday, Dec 27th 11:49AM |
| 113,269,749 | Encriptada y de acceso restringido | Saturday, Dec 27th 10:36AM |
| 113,268,680 | Restringirla a solo el personal que deba verla | Saturday, Dec 27th 10:15AM |
| 113,268,302 | Se utiliza para el fin que se deba y cuando ya no se necesita mas se elimina | Saturday, Dec 27th 10:07AM |
| 113,267,860 | Se restringe la visualización de ella a los empleados que no necesitan conocer de ella. | Saturday, Dec 27th 9:58AM |
| 113,267,506 | Esta informacion se encuentra encriptada. | Saturday, Dec 27th 9:44AM |
| 112,997,086 | Con controles de acceso | Tuesday, Dec 23rd 1:19PM |
| 112,931,859 | CON RESTRICCIONES | Monday, Dec 22nd 3:59PM |
| 112,920,356 | Restringirla a solo el personal que deba verla | Monday, Dec 22nd 2:02PM |

Question **05**

**¿ Como se maneja la información confidencial? (*Mandatory*)**

Answers **10** 91%

Skips **1** 9%

| | | |
|---|---|---|
| 113,433,212 | encriptada | Tuesday, Dec 30th 8:37AM |
| 113,273,018 | Es ckasificado | Saturday, Dec 27th 11:49AM |
| 113,269,749 | Encriptada y de acceso restringido | Saturday, Dec 27th 10:36AM |
| 113,268,680 | Restringirla a solo el personal que deba verla | Saturday, Dec 27th 10:15AM |
| 113,268,302 | Se utiliza para el fin que se deba y cuando ya no se necesita mas se elimina | Saturday, Dec 27th 10:07AM |
| 113,267,860 | Se restringe la visualización de ella a los empleados que no necesitan conocer de ella. | Saturday, Dec 27th 9:58AM |
| 113,267,506 | Esta informacion se encuentra encriptada. | Saturday, Dec 27th 9:44AM |
| 112,997,086 | Con controles de acceso | Tuesday, Dec 23rd 1:19PM |
| 112,931,859 | CON RESTRICCIONES | Monday, Dec 22nd 3:59PM |
| 112,920,356 | Restringirla a solo el personal que deba verla | Monday, Dec 22nd 2:02PM |

Question **06**

**¿Utilizan firewall y de ser así que tipo de firewall usan? (*Mandatory*)**

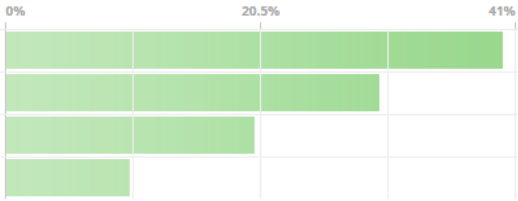
Answers **10** 91%

Skips **1** 9%

| | | |
|---|---|---|
| 113,433,212 | Si,de control de accesos | **Tuesday, Dec 30th 8:37AM** |
| 113,273,018 | Si, McCafee | **Saturday, Dec 27th 11:49AM** |
| 113,269,749 | FORTINET | **Saturday, Dec 27th 10:36AM** |
| 113,268,680 | si, de restricción según el perfil de acceso y de encriptación de la información | **Saturday, Dec 27th 10:15AM** |
| 113,268,302 | Si,de control de accesos | **Saturday, Dec 27th 10:07AM** |
| 113,267,860 | NO | **Saturday, Dec 27th 9:58AM** |
| 113,267,506 | NO | **Saturday, Dec 27th 9:44AM** |
| 112,997,086 | Sí. pfsense | **Tuesday, Dec 23rd 1:19PM** |
| 112,931,859 | - | **Monday, Dec 22nd 3:59PM** |
| 112,920,356 | si, de restricción según el perfil de acceso y de encriptación de la información | **Monday, Dec 22nd 2:02PM** |

Question **07** **¿Qué tipo de antivirus usa la compañía? (*Mandatory*)**

Answers **10** 91% Skips **1** 9%




| | COUNT | PERCENT |
|---|---|---|
| Otro | 4 | 40% |
| Mcafee | 3 | 30% |
| Avira Professional | 2 | 20% |
| Antivirus Gratiuito AVG | 1 | 10% |

Question **08** **¿ Cuáles son los derechos y responsabilidades de los usuarios? (*Mandatory*)**

Answers **10** 91% Skips **1** 9%

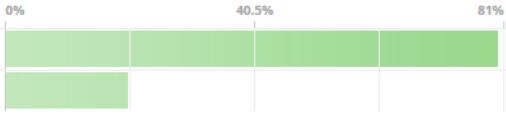
| | | |
|---|---|---|
| 113,433,212 | su derecho es tener informacion pertinente sobre su cargo y su responsabilidad saber administrarla y salvaguardarla | Tuesday, Dec 30th 8:37AM |
| 113,273,018 | xxxx | Saturday, Dec 27th 11:49AM |
| 113,269,749 | Estipulados en las políticas de Uso de los medios informáticos. | Saturday, Dec 27th 10:36AM |
| 113,268,680 | Salvaguardar la información y hacer buen uso de ella. | Saturday, Dec 27th 10:15AM |
| 113,268,302 | El buen uso de la información para la cual estan autorizados | Saturday, Dec 27th 10:07AM |
| 113,267,860 | Derechos * Tener acceso e información sobre las funciones de su puesto de trabajo. * Poder aclarar dudas de sus funciones con el Jefe Inmediato Responsabilidades * Cumplir con el contrato de confidencialidad que se firma al inicio del contrato laboral. * Hacer buen uso de l | Saturday, Dec 27th 9:58AM |
| 113,267,506 | El uso apropiado de los recursos tecnologico. | Saturday, Dec 27th 9:44AM |
| 112,997,086 | Los definidos en el perfil de cargo y asignados por el administrador | Tuesday, Dec 23rd 1:19PM |
| 112,931,859 | DEPENDE DE LAS FUNCIONES DE CADA AREA | Monday, Dec 22nd 3:59PM |
| 112,920,356 | Salvaguardar la información y hacer buen uso de ella. | Monday, Dec 22nd 2:02PM |

Question **09**

**¿ Se tiene un proceso de auditoria que revise el uso de la red y servidores de forma periódica? (*Mandatory*)**

Answers **10** 91%

Skips **1** 9%




| | COUNT | PERCENT |
|---|---|---|
| SI | **8** | 80% |
| NO | **2** | 20% |

Question **10**

**¿Bajo que normas concernientes a la seguridad de la información están certificados? (*Mandatory*)**

Answers **10** 91%

Skips **1** 9%

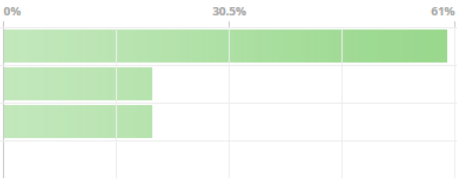
| | | |
|---|---|---|
| 113,433,212 | ninguna | **Tuesday, Dec 30th 8:37AM** |
| 113,273,018 | ISO 9001 | **Saturday, Dec 27th 11:49AM** |
| 113,269,749 | Ninguna | **Saturday, Dec 27th 10:36AM** |
| 113,268,680 | ISO 9001 y se esta buscando la certificación en la ISO27001 | **Saturday, Dec 27th 10:15AM** |
| 113,268,302 | ISO 27001 | **Saturday, Dec 27th 10:07AM** |
| 113,267,860 | IT MARK | **Saturday, Dec 27th 9:58AM** |
| 113,267,506 | ninguna | **Saturday, Dec 27th 9:44AM** |
| 112,997,086 | - | **Tuesday, Dec 23rd 1:19PM** |
| 112,931,859 | NINGUNO | **Monday, Dec 22nd 3:59PM** |
| 112,920,356 | ISO 9001 y se esta buscando la certificación en la ISO27001 | **Monday, Dec 22nd 2:02PM** |

Question 11

**¿Qué tan frecuente se auditan frente a posibles riesgos de delitos informáticos? (*Mandatory*)**

Answers 10 91%

Skips 1 9%



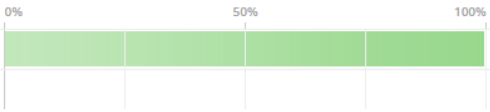

| | COUNT | PERCENT |
|---|---|---|
| cada 6 meses | 6 | 60% |
| nunca | 2 | 20% |
| cada año | 2 | 20% |
| cada 2 años | 0 | 0% |

Question 12

**¿Hay diferencia entre las responsabilidades y los derechos de las personas que manejan la información? (*Mandatory*)**

Answers 10 91%

Skips 1 9%



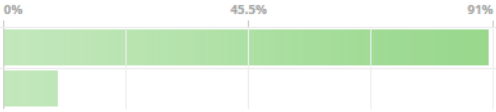

| | COUNT | PERCENT |
|---|---|---|
| SI | 10 | 100% |
| NO | 0 | 0% |

Question 13

**¿Se Realiza un cambio periódico de las contraseñas? (*Mandatory*)**

Answers 10 91%

Skips 1 9%



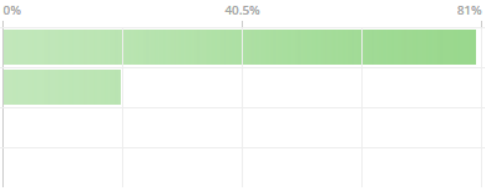

| | COUNT | PERCENT |
|---|---|---|
| Si | 9 | 90% |
| No | 1 | 10% |

Question 14

**Si la respuesta a la pregunta anterior es si ¿cada cuanto se hace ese cambio? (*Mandatory*)**

Answers 10 91%

Skips 1 9%

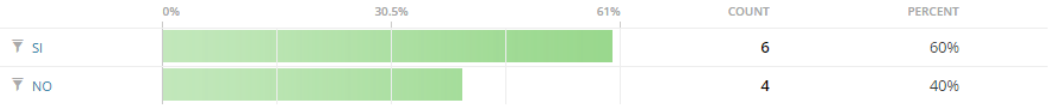



| | COUNT | PERCENT |
|---|---|---|
| cada 6 meses | 8 | 80% |
| NO | 2 | 20% |
| cada año | 0 | 0% |
| cada dos años | 0 | 0% |

Question 15

¿Siguen un estándar para las copias de seguridad de la información y quien puede acceder a ellas? (*Mandatory*)

| Answers | Skips |
|---|---|
| 10 | 1 |
| 91% | 9% |




| | COUNT | PERCENT |
|---|---|---|
| SI | 6 | 60% |
| NO | 4 | 40% |

Question 16

**¿En caso de ser afirmativa la pregunta anterior que tipo de estándar siguen?** (*Mandatory*)

| Answers | Skips |
|---|---|
| 10 | 1 |
| 91% | 9% |

| | | |
|---|---|---|
| 113,433,212 | tenemos una compañía que hace los respaldos | Tuesday, Dec 30th 8:37AM |
| 113,273,018 | Es clasificado | Saturday, Dec 27th 11:49AM |
| 113,269,749 | Ninguno | Saturday, Dec 27th 10:36AM |
| 113,268,680 | Relizar copias de seguridad cada que el estandar lo exiga | Saturday, Dec 27th 10:15AM |
| 113,268,302 | - | Saturday, Dec 27th 10:07AM |
| 113,267,860 | El estandar sugerido por IT MARK | Saturday, Dec 27th 9:58AM |
| 113,267,506 | - | Saturday, Dec 27th 9:44AM |
| 112,997,086 | Gestión de Almacenamiento | Tuesday, Dec 23rd 1:19PM |
| 112,931,859 | -- | Monday, Dec 22nd 3:59PM |
| 112,920,356 | Relizar copias de seguridad cada que el estandar lo exiga | Monday, Dec 22nd 2:02PM |

Question **17**

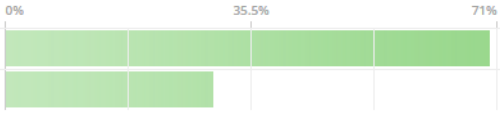
**¿Se capacitan regularmente frente a como deben administrar la información a la cual tienen acceso según la dependencia o empleado? (*Mandatory*)**

| Answers | Skips |
|---|---|
| **10** 91% | **1** 9% |

| | | |
|---|---|---|
| 113,433,212 | no | **Tuesday, Dec 30th 8:37AM** |
| 113,273,018 | No | **Saturday, Dec 27th 11:49AM** |
| 113,269,749 | Periodicamente | **Saturday, Dec 27th 10:36AM** |
| 113,268,680 | Si, mediante cursos virtuales y capacitaciones en entidades reconocidas | **Saturday, Dec 27th 10:15AM** |
| 113,268,302 | no | **Saturday, Dec 27th 10:07AM** |
| 113,267,860 | no | **Saturday, Dec 27th 9:58AM** |
| 113,267,506 | no | **Saturday, Dec 27th 9:44AM** |
| 112,997,086 | - | **Tuesday, Dec 23rd 1:19PM** |
| 112,931,859 | SI, LAS CAPACITACIONES SE REALIZAN DOS VECES AL MES | **Monday, Dec 22nd 3:59PM** |
| 112,920,356 | Si, mediante cursos virtuales y capacitaciones en entidades reconocidas | **Monday, Dec 22nd 2:02PM** |

Question 18 ¿Se evalúan los riesgos con respecto a la información? (*Mandatory*)

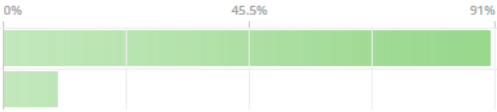
Answers 10 91% | Skips 1 9%




| | COUNT | PERCENT |
|---|---|---|
| SI | 7 | 70% |
| NO | 3 | 30% |

Question 19 ¿Se hace un seguimiento y un control con los activos de la compañía? (*Mandatory*)

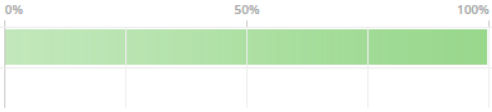
Answers 10 91% | Skips 1 9%




| | COUNT | PERCENT |
|---|---|---|
| SI | 9 | 90% |
| NO | 1 | 10% |

Question 20 ¿Se hace un seguimiento a los recursos humanos de la compañía? (*Mandatory*)

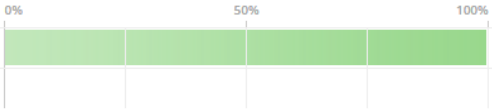
Answers 10 91% | Skips 1 9%




| | COUNT | PERCENT |
|---|---|---|
| SI | 10 | 100% |
| NO | 0 | 0% |

Question 21 ¿Se protege la seguridad fisica y ambiental de la compañía? (*Mandatory*)

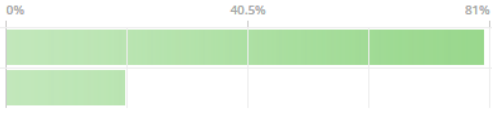
Answers 10 91% | Skips 1 9%




| | COUNT | PERCENT |
|---|---|---|
| SI | 10 | 100% |
| NO | 0 | 0% |

Question 22 ¿Existe una administracion de las comunicaciones y operaciones? (*Mandatory*)

Answers 10 91% | Skips 1 9%




| | COUNT | PERCENT |
|---|---|---|
| SI | 8 | 80% |
| NO | 2 | 20% |

Question **23**

**Si ud esta de-acuerdo proporcione los datos de la compañía a la cual representa (*Mandatory*)**

| Answers | Skips |
|---|---|
| **7** | **4** |
| 64% | 36% |

---- Movich **HOTEL** De Pereira Hotelero

Xxx Sutex Textil

816001182 AUDIFARMA MEDICAMENTOS

NIT 890.300.625-1 Coomeva Eps Salud

- Muebles BL Inmobiliario

NIT 81600 Geminus Sofware Colombia Informatico

80007 JOTA REPUESTOS SA AUTOMOVILISTICO

## ***7.7 Estándar de políticas y normas***

### ***7.7.1 ¿Por qué es importante una política de seguridad?***

La vulnerabilidad es el grado de debilidad inherente a cada red y cada dispositivo. Hay tres

Vulnerabilidades o debilidades principales:

- Debilidades tecnológicas, Protocolo TCP/IP, en los Sistemas Operativos y en los Equipos de Red.

- Debilidades en la configuración Cuentas de usuario no seguras, contraseñas fáciles de adivinar

- Servicios Internet Mal configurados, configuraciones predeterminadas no seguras y equipos de red mal Configurados

- Debilidades en la política de seguridad (Falta de políticas de seguridad, la Política, falta De continuidad, controles de acceso lógicos no aplicados, la instalación de software y hardware y los cambios no respetan la política, no existe plan de recuperación de desastres)

**AMENAZAS A LA INFRAESTRUCTURA FISICA**

- No tan conocida, pero si muy importante son las amenazas al hardware, las cuatro clases de amenazas físicas son:

• **Amenazas al hardware:** daño físico a los servidores, routers, switches, planta de Cableado y estaciones de trabajo.

• **Amenazas ambientales:** temperaturas extremas (calor o frío extremos) o

Condiciones extremas de humedad (humedad o sequedad extremas)

• **Amenazas eléctricas:** picos de voltaje, voltaje suministrado insuficiente alimentación ilimitada (ruido) y pérdida total de alimentación

• **Amenazas al mantenimiento:** manejo deficiente de los componentes eléctricos

Clave (descarga electrostática), falta de repuestos fundamentales, cableado

Insuficiente y rotulado incorrecto Algunos de los problemas deben ser abordados

Por la política de organización, para mitigarlos se presentan las siguientes formas:

**Mitigación de amenazas al hardware:**

• Bloquee el equipo y el acceso no autorizado desde las puertas, el cielorraso, el

Piso, las ventanas, los conductos y los respiraderos.

• Monitoree y controle las entradas de los armarios con registros electrónicos.

• Utilice cámaras de seguridad.

**Mitigación de amenazas ambientales:**

• Control de temperatura.

• Control de humedad.

• Flujo de aire positivo.

• Alarma ambiental remota y grabación y vigilancia.

**Mitigación de amenazas eléctricas:**

• Instale sistemas de UPS.

• Instale grupos de generadores.

• Siga un plan de mantenimiento preventivo.

• Instale fuentes de energía redundantes.

• Mantenga sistemas de alarmas y vigilancia.

**Mitigación de amenazas al mantenimiento:**

• Use tendidos de cables prolijos.

• Etiquete los cables y los componentes fundamentales.

• Utilice procedimientos de descarga electrostática.

• Tenga una provisión de repuestos fundamentales.

• Controle el acceso a los puertos de la consola.

Las amenazas a las redes se pueden agrupar en cuatro clases principales:

**Amenazas no estructuradas**

Consisten en personas sin experiencia que por medio de herramientas de piratería

Acceden a los sistemas, pueden causar graves daños.

**Amenazas estructuradas**

Con mayor experiencia, atacan a los sistemas para efectuar fraudes, robos o confusiones, sus tácticas son muy complejas y sofisticadas.

**Amenazas externas**

Vienen de personal ajeno a la empresa u organización y dependiendo de la Experiencia del Agresor, pueden tener distintos grados de gravedad.

**Amenazas internas**

Vienen de personal con acceso autorizado al sistema, y al igual que las anteriores, su grado de gravedad depende de la experiencia del agresor.

**INGENIERIA SOCIAL**

Se trata de la piratería informática que se consigue por medio de engaños al Personal de la Empresa para obtener contraseñas o accesos a archivos Confidenciales, sin necesidad de Tener gran experiencia en informática, la mayoría De las veces se logra suplantando la identidad para que las víctimas accedan a Sitios Web creados por los agresores con el Propósito de obtener información de la empresa. Para reducir estos ataques se Deben educar a los empleados sobre el manejo de los correos electrónicos, o Diseñar filtros antispam.

## DESARROLLO DE UNA POLÍTICA DE SEGURIDAD

El desarrollo de una política de seguridad, es una renta y el primer paso establecer una protección elaborada de la información de una compañía, además es una formalización de la misma con las normas que deben regir dentro de la compañía a las personas que tienen acceso a la información de una compañía.

### ***7.7.2 Objetivos de las políticas de seguridad***

**Las políticas de seguridad tienen 3 objetivos básicos**

1. Informa de los requisitos que se tienen que cumplir para salvaguardar los bienes tecnológicos y su contenido

2. Declara los mecanismos y los medios para llevar a cabo los requisitos

3. Se dictamina una línea base que lleve a cumplir los requisitos

Para definir una política se encuentra el documento estándar ISO/IEC 27002 que consta de 12 secciones:

La siguiente numeración o viñeta corresponde a los ítems a tener encuentra a la hora de elaborar una política de seguridad

La siguientes viñetas corresponde a las 12 secciones que propone la ley 27002

- Evaluación de riesgos

La evaluación de los riesgos dentro de una compañía es un factor determinante y clave ya que permite visualizar fallos y prever situaciones en las cuales se puede vulnerar la información de una compañía, se pueden hacer planes de prevención, mantenimiento y contención.

- Administración de activos

Los activos dentro de una compañía tienen que estar administrados de la manera más transparente eficiente y responsable, independientemente del área en la que se encuentren y deben estar consignados los elementos activos, por dar de baja y los dados de baja. Y que se han hecho con ellos.

- Seguridad de los recursos humanos

Las personas son un activo más de las compañías pero no pueden manejarse como tal, se debe salvaguardar su privacidad, sus derechos humanos y su integridad en todo momento.

- Seguridad física y ambiental

La integridad de las personas y tanto la responsabilidad ambiental que deben tener encuenta las compañías a la hora de implementar una política de seguridad estos son factores que se deben evaluar y tener muy presentes.

- Administración de las comunicaciones y operaciones

Todo tipo de comunicación dentro de una compañía y el medio por el cual se hace debe tener una previa administración, un control y garantizar salvaguardar esta información y que siempre este en las manos pertinentes.

• Control de acceso

Las compañías tienen recursos, información, infraestructura y elementos que no todo el personal puede acceder a ellos, por lo tanto se debe restringir documentar y verificar los accesos a tales recursos respetando y asegurando la idoneidad de cargo que pueda acceder a ellos.

• Adquisición, desarrollo y mantenimiento de los sistemas informáticos

La adquisición de equipos y software debe estar bajo un seguimiento y una documentación tanto de los equipos que ingresan con sus respectivas referencias, seriales y garantías y los software con su respectiva licencia.

• Administración de incidentes de seguridad de la información

Los accidentes, eventos, mantenimientos, a los equipos que manejan la información de una compañía y a las acciones que directamente afectan a la información como tal deben estar reportados y documentados con todo detalle.

• Administración para la continuidad de la empresa

- Política de seguridad

Definir la política con la cual se administrara la información y cuáles serán los requisitos que se van a implementar para lograr ese objetivo, mecanismos y medios para que se cumplan los requisitos y la línea que se va a seguir.

• Organización de la seguridad de la información

Presentación de manera formal de la política de seguridad ante las directivas de la organización esperando evaluación y corrección de la misma

• Cumplimiento

Las compañías en todas sus aéreas deben tener un documento llamado plan de desarrollo en el cual se consignen los diferentes objetivos y las actividades que lleven a cumplirlos y deben tener estipuladas unas fechas para el cumplimiento de tales actividades, estos planes de desarrollo se hacen de manera anual pero se pueden evaluar de manera trimestral.

### ***7.7.3 Componentes de una política de seguridad***

• **Declaración de autoridad y alcance:** especifica quien propone la política de seguridad

Y que áreas abarca.

En una compañía a la hora de implementar una política de seguridad independiente del tamaño de la cantidad de aéreas que maneje una declaración de una política de seguridad tiene que tener una declaración formal en la cual se describe las aéreas involucradas , y las especificaciones y restricciones en particular para cada área

| | |
|---|---|
| Nombre de la política | Se debe definir un nombre apropiado para la política la cual respalde los objetivos los cuales se pretende cumplir, el titulo debe representar la política por lo tanto debe ser llamativo y relevante. |
| Se debe cita la mayor autoridad de la compañía | Se debe nombrar a la máxima autoridad del ente, la cual evaluara se encargara de aprobar o no la política de seguridad. |
| Objetivo general y objetivo especifico | La política de seguridad tiene varias finalidades u objetivos, se debe citar el principal y que otros objetivos cortos ayudan a conseguir el más grande. |
| Definir aéreas involucradas | Se debe hacer un bosquejo de que áreas están involucradas dentro de la política, el por qué se involucran, en que mejorarían las áreas con respecto a la implementación de la política de seguridad. |
| Definir actividades a realizar por cada área | Se debe definir un conjunto de actividades previas las cuales ayuden a cumplir los objetivos específicos. |
| Realizar una conclusión | Se anexa una conclusión donde se tendrán encuenta las expectativas que se tienen con la implementación de las políticas donde se muestran indicadores de la situación actual y hacia donde quiere apuntar la compañía implementando la política. |
| Evaluación del documento | Este documento se debe presentar antes las mayores autoridades de la compañía y debe ser aceptado para poder ser implementado |
| | |

Para la declaración de autoridad y de alcance se deben seguir los siguientes ítems

- Elaboración del documento
  Se debe elaborar un documento simple pero concreto el cual como mínimo debe tener lo siguiente:

• **Política de uso aceptable:**

Después de validar el documento en el que se propone la política de seguridad en la compañía se debe presentar y dejar declaradas aquellas consignas y limitaciones que tiene la política de seguridad .Especifica lo que la empresa permitirá y lo que no con Respecto a su infraestructura de información.

| POLITICA DE SEGURIDAD | ALCANCE Y LIMITITACIONES |
|---|---|
| AREAS DE LA COMPAÑÍA | |
| ACTIVOS DE LA COMPAÑÍA | |
| PERFILES DE LOS USUARIOS | |
| FORMULAS RESETAS, DATOS DE ACCESO SENSURADO | |
| EQUIPOS SENSIBLES DE LA COMPAÑÍA (Servidores, plantas de energía etc.) | |

• **Políticas de identificación y autenticación:** especifica que tecnologías usa la empresa

Para garantizar que sólo el personal autorizado obtenga acceso a sus datos. 0

Las políticas de identificación y autenticación pretenden dar cobertura tanta a la información lógica que se maneja con diferentes tecnologías, tanta con la información física, por lo tanto se debe administrar de la manera más segura.

- Se debe nombrar el alcance que tiene la implementación de la política de **identificación y autenticación**

- **Se debe listar las tecnológicas** utilizadas por la compañía (aplicaciones, chats corporativos, servidores, métodos de conexión remota, topología de redes, protocolos TCP/IP , antivirus, etc.)
- **Hacer un análisis usuario – tecnología** donde se especifique con cuales de las herramientas que se nombraron con anterioridad tiene acceso usuario o empleado, también se debe tener en cuenta si hay alguna clase de restricción de acceso al tipo de tecnología Y Documentarla, a este documento solo debe tener acceso el jefe de sistemas, Gerente o aquella persona la cual sea la responsable de este tipo de información por lo tanto debe estar rigurosamente protegido, este listado se debe hacer por cada empleado y se deben citar aquellas tecnologías las cuales sean relevantes y contengan información importante.

| NOMBRE EMPLEADO | CARGO | NOMBRE DE TECNOLOGIA | DESCRIPCION TECNOLOGIA | TIPO DE LICENCIA | ACCESO CIFRADO | TIPO DE INFORMACION | CONTRASEÑA DE ACCESO |
|---|---|---|---|---|---|---|---|

- Se debe documentar el acceso a los diferentes puntos dentro del campus de la compañía y quien puede estar en las diferentes aéreas, oficinas, patios, centros de descanso.

• **Política de acceso a internet y correo electrónico:** especifica lo que la empresa considera uso ético y Correcto de sus capacidades de acceso a internet.

- Propósito
- Alcance
- Asignación de derechos de acceso (privilegios)

Asignación de derechos de acceso (privilegios)

Los privilegios de uso de Internet estarán limitados por la necesidad de Acceso que requiera el desarrollo de la función de cada usuario. Las solicitudes de nuevos códigos de

usuario y los cambios de privilegios de Acceso se presentarán por escrito con la aprobación del jefe del área a la que pertenezca el usuario. Los documentos de solicitud se retendrán Durante un período mínimo de un año. Se podrán otorgar derechos de acceso a personas ajenas al Ministerio, Siempre y cuando la solicitud haya sido aprobada por el jefe de Departamento en el que trabajarán. Estos derechos tendrán una vigencia de90 días o menos, pero podrán ser extendidos, previa solicitud del jefe de Departamento respectivo.

Los derechos especiales de acceso como la capacidad de escribir sobre Archivos de otros usuarios se asignarán a quienes ejerzan como Administradores de los sistemas. Todos los usuarios que quieran utilizar Internet del Ministerio deberán Firmar un documento de conocimiento y aceptación de las políticas de uso De la Internet antes de recibir un código de usuario.

Identificación única por usuario

Cada usuario recibirá un código de identificación y una contraseña única. Sin Importar la circunstancia, está prohibido compartir o revelar la contraseña a Otros usuarios. El uso de la contraseña se considerará equivalente a la firma del funcionario. Para prevenir el uso indebido de contraseñas, el usuario Deberá cambiar la suya con la frecuencia que indicará la Dirección Nacional De Tecnología. Se prohíbe el control de acceso a archivos, aplicaciones, bases de datos, Computadores ó redes por medio de contraseñas compartidas (no se crearán Contraseñas aplicables a grupos de usuarios)Es obligación de cada jefe reportar de inmediato al Oficial de Seguridad dela Dirección Nacional de Tecnología los cambios de personal que puedan Afectar el uso del sistema, como traslados, retiros, suspensiones, vacaciones permisos. La contraseña que recibe el usuario para que comience a utilizar el sistema Será válida únicamente durante la primera sesión en línea. El usuario será Obligado por el sistema a suministrar una nueva contraseña. El mismo Proceso aplicará cuando el usuario olvide su contraseña y solicite una nueva. Uso Adecuado de Internet Debe entenderse que Internet es una herramienta estrictamente de trabajo Y no con otros fines ajenos a las funciones del usuario. Esto será Monitoreado por la Dirección Nacional de Tecnología. Mal Uso del Internet

- El usuario no debe entrar a Páginas Web con contenido Pornográfico.
- No se permitirá el uso del denominado “CHAT” en ningún Horario (Pagina Web, ICQ, Messenger, etc.)
- El usuario no debe bajar ningún programa (software), sin La debida autorización de la Dirección Nacional de Tecnología, tales como: shareware, software de evaluación etc. Archivos de música (MP3, WAV, etc.) ya que estos no Poseen licencia para su uso en el ministerio.
- El usuario no debe instalar ningún programa para escuchar MP3, RA, WAV, o emisoras de radio vía Internet.(Winamp, REAL AUDIO, MUSIC MATCH, Oozic PLAYER)
- El usuario no debe instalar ningún programa para ver vídeos o emisoras de televisión vía Internet. (REAL AUDIO,BWV, etc.)· El usuario no debe habilitar, ni

revisar correos Electrónicos que no sean autorizados por la Dirección Nacional de Tecnología. Ya que estos correos pueden tener Virus y afectar la red del ministerio (HOTMAIL, YAHOO, etc.)

- No debe usarse el Internet para realizar llamadas Internacionales (Dialpad, NET2PHONE, FREEPHONE, etc.)
- Se prohíbe cualquier tipo de transmisión vía Internet(Escuchar músicas y ver vídeos)
- No se puede realizar ningún tipo de compras, que no sean De uso del Ministerio con su respectivo permiso.
- El horario de navegación por Internet no debe ser mayor De 3 horas, excedido lo establecido, se le enviará un reporte Al jefe inmediato, para que evalué el tiempo que el Funcionario utiliza la herramienta. Este tipo de limitaciones se da para proteger el ancho de banda Con que cuenta el Ministerio actualmente. Sanciones por Mal Uso de Internet.

• **Política de acceso al campus:** especifica como los usuarios utilizan la infraestructura de Datos de la empresa en el campus.

• **Política de acceso remoto:** especifica como acceden a la infraestructura de datos de la Empresa los usuarios remotos.

- Describir los requisitos empresariales para proporcionar servicios de trabajadores a distancia, incluidas las diferencias entre las infraestructuras de red privada y pública.
- Describir los requisitos de trabajo a distancia y la arquitectura recomendada para proporcionar servicios de trabajo a distancia.
- Explicar cómo los servicios de banda ancha extienden las redes empresariales mediante DSL, cable y la tecnología inalámbrica.
- Describir la importancia de la tecnología VPN, incluido su rol y sus beneficios para empresas y trabajadores a distancia.

- Describir cómo la tecnología VPN se puede utilizar para proporcionar a una red empresarial servicios seguros de trabajo a distancia.

## Requisitos comerciales para los servicios de trabajo a distancia

- Con los avances en las tecnologías de conexiones de banda ancha e inalámbrica, el trabajo lejos de la oficina ya no presenta los mismos desafíos que en el pasado.
- Las organizaciones pueden distribuir de manera rentable aplicaciones de datos, voz, video y en tiempo real a través de una conexión de red común que alcance a todos los empleados, sin importar su ubicación.
- Para permitir el trabajo eficaz entre empresa y trabajadores, se debe equilibrar la selección de tecnologías y diseñar cuidadosamente los servicios de trabajo a distancia.

## Servicios de banda ancha

- Los trabajadores a distancia usan distintas aplicaciones que requieren una conexión de un ancho de banda elevado.
- Debe de considerarse como primera instancia la elección de la tecnología de red de acceso y la necesidad de garantizar el ancho de banda adecuado.
- El cable residencial, DSL y el acceso inalámbrico de banda ancha son tres opciones que proporcionan un ancho de banda elevado. Una conexión dial-up por módem sólo debe considerarse cuando no hay otras opciones disponibles.

**Tecnología VPN**

- Las organizaciones usan las redes VPN para proporcionar una infraestructura WAN virtual que conecta sucursales, oficinas domésticas, oficinas de socios comerciales y trabajadores a distancia a toda la red corporativa o a parte de ella.
- En vez de usar una conexión de Capa 2 exclusiva, como una línea alquilada, la VPN usa conexiones virtuales que se enrutan a través de Internet.
- Los datos de la VPN están encriptados y ninguna persona que no esté autorizada puede descifrarlos.
- Tenga en cuenta estos beneficios al usar las VPN:

Economía

Seguridad

Escalabilidad

- Las VPN usan protocolos de tunneling criptográficos para brindar protección contra detectores de paquetes, autenticación de emisores e integración de mensajes.
- Los componentes necesarios para establecer esta VPN incluyen lo siguiente:

  Una red existente con servidores y estaciones de trabajo

  Una conexión a Internet

  Gateway VPN, como routers, firewalls, concentradores VPN y ASA, que actúan como extremos para establecer, administrar y controlar las conexiones VPN

  Software adecuado para crear y administrar túneles VPN
- Las VPN protegen los datos mediante encapsulación o encriptación

- Los hashes (messagedigest) contribuyen a la autenticación y la integridad de los datos, garantizan que personas no autorizadas no alteren los mensajes transmitidos. Son un número generado a partir de una cadena de texto.
- Las VPN utilizan un código de autenticación de mensajes para verificar la integridad y la autenticidad de un mensaje

El HMAC (código de autenticación de mensajes de hash) tiene dos parámetros: un mensaje de entrada y una clave secreta que sólo conocen el creador del mensaje y los receptores adecuados.

- El IPsec es un conjunto de protocolos para la seguridad de las comunicaciones IP que proporciona encriptación, integridad y autenticación.
- Protocolos de estructura IPsec:

Encabezado de autenticación (AH):
se utiliza cuando no se requiere o no se permite la confidencialidad.

Contenido de seguridad encapsulado (ESP):
proporciona confidencialidad y autenticación mediante la encriptación del paquete IP.

- IPse0c se basa en algoritmos existentes para implementar la encriptación, la autenticación y el intercambio de claves.

• **Procedimiento para el manejo de incidentes:** especifica quien responde ante

Incidentes de seguridad y como se deben manejar.

Todos los incidentes con la información y la integridad física de la compañía deben ser documentados y junto al departamento de recursos humanos y gerencia deben tener ese respaldo y tener un historial de novedades e incidentes.

## ***8.0 MARCO CONCEPTUAL***

- **Bluesnarfing**

  Es el acceso no autorizado a la información guardada en teléfonos celulares, computadores Y tabletas electrónicas (fotos, videos, lista de contactos, mensajes de texto) usando una Conexión de Bluetooth.

- **Hackear**

  Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar Información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

- **Hacker**

  Es un experto informático especialista en entrar en sistemas ajenos sin permiso, con Frecuencia para mostrar la baja seguridad de los mismos o simplemente para demostrar Que es capaz de hacerlo. Los Hackers son muy respetados por la comunidad técnica de Internet, y proclaman tener una ética y unos principios contestatarios e inconformistas pero No delictivos, a diferencia de los Crackers que utilizan sus conocimientos para fines Destructivos o delictivos.

- **Hammering**

  Es el acto de intentar conectarse repetidamente a un servidor FTP inexistente o no Disponible con muy breves lapsos de tiempo entre cada intento. Podemos compararlo con La acción de presionar repetidamente el botón "redial" en un teléfono sin esperar a que Haya terminado de marcar (martilleo).

- **Malware**

  Programa creado con el fin de molestar o dañar los computadores que lo tienen instalado.

- **Pharming**

  Es un tipo de fraude que consiste en suplantar los nombres de dominio de la página que Quiere navegar el usuario, para conducirlo a una página web falsa.

- **Phishing**

  Es un delito cibernético con el que por medio del envío de correos se engaña a las personas Invitándolas a que visiten páginas web falsas de entidades bancarias o comerciales.

  **Virus**

Programa que puede alterar o destruir el funcionamiento del computador. Normalmente Ocurre sin el permiso o conocimiento del usuario.

- **Vishing**

  Similar al phising, pero con teléfonos. Consiste en hacer llamadas telefónicas a las víctimas, En las que por medio de una voz computarizada, muy similar a las utilizadas por los bancos, Se solicita verificar algunos datos personales e información bancaria.

- **Adware**

  Adware es un software, generalmente no deseado, que facilita el envío de contenido Publicitario a un equipo.

- **Amenaza**

  Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de Causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos O negación de servicio (DoS).

- **Antispam**

  Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o Correo no deseado antes de que se convierta en una molestia para los usuarios. El Antispam debe ser parte de una estrategia de seguridad multinivel.

- **Antivirus**

  Antivirus es una categoría de software de seguridad que protege un equipo de virus, Normalmente a través de la detección en tiempo real y también mediante análisis del Sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una Estrategia de seguridad estándar de múltiples niveles.

- **Ataques multi-etapas**

  Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, Seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un Troyano que descarga e instala adware.

- **Ataques Web**

  Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde Un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido Creados para atacar intencionalmente a los usuarios de ésta.

- **Blacklisting o Lista Negra**

  La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, Direcciones o dominios IP conocidos maliciosos o malévolos.

- **Bot**

Un bot es una computadora individual infectada con malware , la cual forma parte de una Red de bots (bot net).

- **Caballo de Troya**

  Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy Importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no Se propagan automáticamente.

- **Canal de control y comando**

  Un canal de mando y control es el medio por el cual un atacante se comunica y controla los Equipos infectados con malware, lo que conforma un botnet.

- **Carga destructiva**

  Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga Destructiva es independiente de las acciones de instalación y propagación que realiza el Malware.

- **Ciberdelito**

  El ciberdelito es un delito que se comete usando una computadora, red o hardware. La Computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito Puede ocurrir en la computadora o en otros lugares.

- **Definiciones de virus**

  Una definición de virus es un archivo que proporciona información al software antivirus, para Identificar los riesgos de seguridad. Los archivos de definición tienen protección contra Todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las Definiciones de virus también se denominan firmas antivirus.

- **Descarga inadvertida**

  Una descarga inadvertida es una descarga de malware mediante el ataque a una Vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de Navegador sin intervención alguna del usuario.

- **Encriptación**

  La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios No autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña O clave pueden descifrar y utilizar los datos.

- **Exploits o Programas intrusos**

  Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y Que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.

- **Filtración de datos**

  Una filtración de datos sucede cuando se compromete un sistema, exponiendo la Información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado De ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse Con fines delictivos o con otros fines malintencionados

- **Firewall**

  Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en Determinados puertos del sistema, independientemente de si el tráfico es benigno o Maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de Múltiples niveles.

- **Firma antivirus**

  Una firma antivirus es un archivo que proporciona información al software antivirus para Encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos Los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas Antivirus también se denominan definiciones de virus.

- **Greylisting o Lista Gris**

  La lista gris es un método de defensa para proteger a los usuarios de correo electrónico Contra el spam. Los mensajes de correo electrónico son rechazados temporalmente de un Remitente que no es reconocido por el agente de transferencia de correos.

- **Gusanos**

  Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar Un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de Un archivo anfitrión infectado.

- **Lista blanca o Whitelisting**

  La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, Que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de Dominio autorizados o conocidos pasar por el software de seguridad.

- **KeystrokeLogger o Programa de captura de teclado (Keylogger)**

  Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del Teclado y del ratón, generalmente de forma encubierta, para intentar robar información Personal, como las cuentas y contraseñas de las tarjetas de crédito.

- **Mecanismo de propagación**

  Un mecanismo de propagación es el método que utiliza una amenaza para infectar un Sistema.

- **Negación de servicio (DoS)**

  La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los Recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido De negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de Computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.
- **Pharming**

  Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio Falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios Permanezcan ignorantes del re direccionamiento e ingresen información personal, como la Información bancaria en línea, en el sitio fraudulento.
- **Redes punto a punto (P2P)**

  Red virtual distribuida de participantes que hacen que una parte de sus recursos Informáticos estén a disposición de otros participantes de la red, todo sin necesidad de Servidores centralizados..
- **Rootkits**

  Componente de malware que utiliza la clandestinidad para mantener una presencia Persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la Instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o Consentimiento del usuario final.

- **Seguridad basada en la reputación**

  La seguridad basada en la reputación es una estrategia de identificación de amenazas que Clasifica las aplicaciones con base en ciertos criterios o atributos para determinar si son Probablemente malignas o benignas.

- **Sistema de detección de intrusos**

  Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del Sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos De acceso a los recursos del sistema de manera no autorizada.

- **Sistema de prevención de intrusos**

  Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa Las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso Y puede reaccionar en tiempo real para bloquear o evitar esas actividades.
- **Software de seguridad fraudulento (rogue)**

Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge Ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, Aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, Puede de hecho facilitar la instalación de códigos maliciosos contra los que busca Protegerse.

- **Toolkit**

  Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos Maliciosos. [16] [17]

***9..INTEGRANTES: CARLOS FERNANDO TOVAR CODIGO:92012157***

***10. CONCLUSIONES***

En Colombia, un país en vía de desarrollo pero con un avance tecnológico importante en la última década se enfrenta a cambiar y a acostumbrarse a situaciones las cuales antes no ha manejado como lo son la judicialización en términos tecnológicos y es algo que le ha causado al país algo de traumatismo pero está en el proceso , cosa que no muchos países vecinos no han hecho, pero cabe resaltar que hay un desconocimiento masivo tanto por las personas naturales , como para las compañías y esto es aún más grave porque las compañías no se preparan y no están bien informadas de cómo opera la ley como se pueden proteger , y como mitigar el riesgo que una situación la cual amanece la seguridad de la información sea controlado y mejor aún prevenida.

Existen marcos de referencia pero no se especifican bien los pasos a seguir a la hora de implementar una política de seguridad en una compañía y eso fue justamente lo que se hizo.

***11.BIBLIOGRAFIA:***


1. http://seguridad-informacion.blogspot.com/2009/06/estudio-2009-trust-security-passwords.html

2.http://myprofetecnologia.wordpress.com/2011/01/30/delitos-informaticos/

3.http://www.larepublica.co/alta-gerencia/del-total-de-empresas-las-colombianas-98-son-v%C3%ADctimas-de-ataques-inform%C3%A1ticos_1218

4.http://www.eumed.net/ce/2012/avnh.html

5.http://www.simplekey.es/files/SeguridadInformatica.pdf

6 ***{http://www.monografias.com/trabajos6/delin/delin.shtml}***

7 {http://www.elespectador.com/tecnologia/diez-millones-de-colombianos-victimas-de-delitos-inform-articulo-442538}

8. {http://www.elpais.com.co/elpais/judicial/noticias/colombia-cifras-delitos-informaticos-van-aumento } y {http://www.elespectador.com/tecnologia/diez-millones-de-colombianos-victimas-de-delitos-inform-articulo-442538}

9. {http://www.ccit.org.co/files/SEGURIDAD%20INFORMATICA/Delitos_Informaticos.pdf}

10. {http://www.dragonjar.org/wp-content/uploads/Entrevistas/Andreas%20Ormaza.mp3}

11. {http://es.slideshare.net/dxp2/aniversario-de-la-ley-de-delitos-informticos}

12.***{http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf}***

13. http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

14http://www.sic.gov.co/drupal/recursos_user/historico/d2011sic951.htm}

15. {http://www.acis.org.co/index.php?id=856}

16..http:// www.delitosinformaticos.gov.co

17 .http://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

12. ***cronograma***