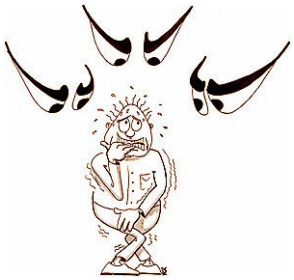
Capítulo 4

Delitos Informáticos

Los delitos informáticos surgen en primera instancia, por la aparición de las computadoras, -recurso inventado para procesar información- en segunda instancia por la propia naturaleza del ser humano que tiende a sacar provecho de sus recursos, los faltos de ética y ambiciosos promueven conductas ilícitas utilizando ese recursos.

INTRODUCCIÓN



A la par del avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos ilícitos denominados, de manera genérica, «delitos informáticos». Los delitos que se pueden cometer en la actualidad mediante el uso de la computadora son múltiples y de tipos muy variados, nadie puede estar seguro de que no va a ser víctima de alguno de ellos y por lo anterior se debe legislar este tipo de delitos. Los especialistas informáticos y legisladores deben trabajar juntos con el fin de proporcionar un instrumento confiable que permita identificar y sancionar de una manera correcta los delitos que con el uso de los equipos de cómputo se puedan presentar.

En el presente capítulo se revisarán los delitos informáticos con el fin de poder reconocer cómo se presentan, cuales son sus alcances y limitaciones, el impacto de este tipo de delitos en la sociedad y en las organizaciones, te sugiere algunas propuestas para evitarlos y te presenta el papel que juega la Auditoria Informática para prevenirlos.

1.1 GENERALIDADES

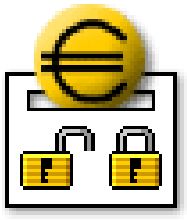
Para Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000) hablar de los delitos informáticos primero se tiene que hablar de qué es un delito, y luego de qué es la informática. Un delito es un acto u omisión sancionado por las leyes penales. Según el ilustre penalista Cuello Calon[6], los elementos integrantes del delito son:

[6] Jurista español. Fue catedrático de derecho penal en las universidades de Barcelona y de Madrid. Escribió diversas obras, entre las que destacan *Derecho penal: Penología* (1920) y *La nueva penología* (1958).

- El delito es un acto o acción humana, (ejecución u omisión) de carácter antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
- El delito debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.
- El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
- La ejecución u omisión del acto debe estar sancionada por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena, mientras que la informática según Téllez, J. (1996), es "un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones".

Ahora si juntamos las definiciones tendremos que los delitos informáticos son: El conjunto de técnicas de carácter antijurídico destinadas al tratamiento lógico y automatizado de la información sancionada por las leyes penales. Téllez, J. (1996), los define como "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".



El término delito relacionado con la computadora se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento y/o transmisión de datos.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables, la manipulación fraudulenta de las computadoras con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

No sólo la mayor cantidad de perjuicios ocasionados por el procesamiento electrónico de datos comparado con la delincuencia tradicional es lo preocupante, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos, ya que la convierten en un instrumento idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas,

apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

Debido a la gran importancia que los sistemas de procesamiento de datos representan para la operación de las organizaciones tanto públicas como privadas, los sistemas se han convertido en un objetivo importante cuyo ataque provocaría un perjuicio enorme, que va mucho más allá del valor material de los sistemas mismos, además, estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

Según Téllez, J. (1996), los delitos informáticos presentan las siguientes principales características:

- Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" muy lucrativos a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias, debido a la falta de regulación por parte del Derecho.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
- Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que:

- Tratan grandes volúmenes de datos, muchas veces muy sensibles y estratégicos para las organizaciones.

- Interviene poco personal en el procesamiento de los sistemas, lo que impide verificar la totalidad de los procesos.
- Los registros magnéticos son fáciles de alterar o dañar, por lo que es muy fácil que se pierda la evidencia auditable o la secuencia de acontecimientos.
- A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un período de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.
- Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo, del sistema y no comprenden, o no les afecta, el significado de los datos que manipulan.
- En el diseño de un sistema es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir.
- Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de "agujeros".
- Sólo parte del personal de informática conoce todas las implicaciones del sistema y las bases de datos son un gran centro de información.
- En las áreas de informática hay personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar poco recomendable implantar niveles excesivos de control y supervisión.

El error y el fraude son difíciles de equiparar, a menudo los errores no son iguales al fraude. Cuando surgen discrepancias, no se imagina que se ha producido un fraude y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla esta operación, se buscan fallos técnicos y operativos. Sólo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude.

Aunque depende en gran medida del tipo de organización, se puede mencionar que los fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones. Además de aquellos que no están claramente definidos y publicados como un delito, tales como la piratería, la mala utilización de la información, la omisión deliberada de controles, el uso no autorizado de equipos y/o servicios computacionales y que en algún momento pueden generar un impacto nocivo a la organización.

Pero si se examina la otra perspectiva, referente a los delitos de difícil detección, se deben situar a aquellos producidos por las personas que trabajan internamente en una organización y que conocen perfectamente la configuración interna de las plataformas; especialmente cuando existe una cooperación entre empleados, cooperación entre empleados y terceros, o incluso el involucramiento de la administración misma.

4.2 ALCANCES Y LIMITACIONES

Alcances

Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000), señalan que en la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio para obtener y conseguir información, lo que las ubica también como un medio de comunicación muy eficaz y condiciona su desarrollo a la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento, transmisión y administración de datos.

La informática esta hoy presente en casi todos los campos de la vida moderna, con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

La ocurrencia de delitos informáticos en las organizaciones no debe -en ningún momento- impedir que éstas se beneficien de todo lo que provee la tecnología de la información (comunicación remota, interconectividad, comercio electrónico, etc.), sino por el contrario, dicha situación debe plantear un reto a los profesionales de la informática de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etcétera.

Nuevas formas de hacer negocios como el comercio electrónico puede que encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática con el único fin de tener un marco legal que se utilice como soporte para este tipo de transacciones.

Limitaciones

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de esta área. Desde el punto de vista de la legislatura es

difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las leyes relacionadas con la informática.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

La responsabilidad del auditor informático no abarca el dar solución al impacto de los delitos o en implementar cambios, sino más bien su responsabilidad recae en la verificación de controles, evaluación de riesgos, así como en el emitir recomendaciones que ayuden a las organizaciones a minimizar las amenazas que presentan los delitos informáticos.

Existen bancos de datos, empresas o entidades dedicadas a proporcionar, -si se desea- cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un gobierno o a particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos con los consiguientes derechos jurídicos y humanos.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas.

Las leyes sobre el uso indebido de las computadoras ahora son más severas, sin embargo solo algunos países han legislado en esta materia. Esto trae como consecuencia que la investigación, enjuiciamiento y condena de los transgresores se convierte en un problema jurisdiccional y jurídico. Una vez capturados los delincuentes se tiene que extraditar y eso implica acuerdos internacionales.

4.3 TIPIFICACIÓN DEL DELITO INFORMÁTICO

Sujeto activo

El Supremo Tribunal de Justicia del Estado de Sinaloa (1998), señala que las personas que cometen los "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es,

explica Aniyar de Castro, Lolita (1980) los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas de cómputo, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Sin embargo, tendiendo en cuenta las características ya mencionadas de las personas que cometen los "*delitos informáticos*", estudiosos en la materia los han catalogado como "*delitos de cuello blanco*"[7]

Sujeto Pasivo

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo y en el caso de los "*delitos informáticos*" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "*delitos informáticos*", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casualmente por el desconocimiento del "*modus operandi*" de los sujetos activos.

Dado lo anterior, ha sido imposible conocer la verdadera magnitud de los "*delitos informáticos*", ya que la mayor parte de los delitos no son descubiertos y si lo son, generalmente no se difunden para evitar dar ideas.

Los delitos informáticos se clasifican según Téllez, J. (1996), sobre la base de dos criterios: Como instrumento o medio y como fin u objetivo.

Como instrumento o medio: En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
- Variación de los activos y pasivos en la situación contable de las empresas.

[7] Término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

- Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo: En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas y datos por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etcétera).

Tipos de delitos informáticos reconocidos por Naciones Unidas

Para Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000), los f*raudes cometidos mediante manipulación de computadoras son:*

- *Manipulación de los datos de entrada*: Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de

conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

- *La manipulación de programas:* Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
- *Manipulación de los datos de salida:* Se efectúa fijando un objetivo al funcionamiento del sistema informático. Puede ser duplicando impresiones o difundir información confidencial.
- *Fraude efectuado por manipulación informática:* Aprovecha las repeticiones automáticas de los procesos de cómputo, es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas instrucciones perceptibles, un ejemplo de esta técnica podría ser de transacciones financieras, se van sacando repetidamente de una cuenta pequeñas cantidades de dinero y se transfieren a otra.

Falsificaciones informáticas.

- *Como objeto:* Cuando se alteran datos de los documentos almacenados en forma computarizada.
- *Como instrumentos:* Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Por ejemplo, cuando empezó a disponerse de impresoras en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados.

- *Sabotaje informático:* Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- *Virus*: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

- *Gusanos:* Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus.

- *Bomba lógica o cronológica:* Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

- *Acceso no autorizado a servicios y sistemas informáticos:* Por motivos diversos: desde la simple curiosidad (hackers), como en el caso de muchos piratas informáticos hasta el sabotaje o espionaje informático (crackers).

- *Piratas informáticos:* El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema, a menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Clasificación según actividades delictivas graves

- *Terrorismo:* Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

- *Narcotráfico:* Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- *Espionaje:* Son los casos de acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.
- *Espionaje industrial:* Son los casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y estrategias mercadotécnicas que posteriormente han sido aprovechadas en empresas competidoras o ha sido objeto de una divulgación no autorizada.
- *Pornografía infantil y otras obscenidades:* La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material "ofensivo" que se transmita o archive.
- *Otros delitos:* Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o viceversa.

Infracciones que no constituyen delitos informáticos

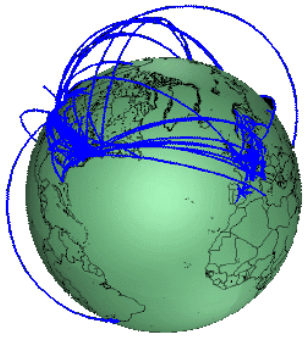
- *Reproducción no autorizada de programas informáticos de protección legal:* Se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual, esto es tiene que ver con los derechos de autor y representa otro tipo de delito.
- *Usos comerciales no éticos:* Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet.
- *Actos parasitarios:* Algunos usuarios incapaces de integrarse en grupos de discusión o foros de debate online, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc.

4.4 IMPACTO DE LOS DELITOS INFORMÁTICOS

Para Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000), el impacto de los delitos informáticos se da de la siguiente forma:

Impacto a Nivel General

En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, los usuarios que se conectan a la Internet se comunican en tiempo real con otros usuarios, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan a su médico online, el número de usuarios de la Internet supera los miles de millones hoy día.



A medida que se va ampliando la Internet, va aumentando el uso indebido de la misma, los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o "piratería informática", el fraude, el sabotaje informático, la trata de niños con fines pornográficos, el acecho y muchos otros inimaginables.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables "enlaces" o simplemente desvanecerse sin dejar ningún documento de rastro, esconder pruebas delictivas en países que carecen de leyes o experiencia para seguirles la pista.

Los delincuentes provocan pérdidas multimillonarias al robar de las cuentas “online” sus números de tarjeta de crédito, pueden sabotear las computadoras para ganarles ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los malhechores manipulan los datos y/o las operaciones, ya sea directamente o mediante los llamados "gusanos" o "virus", que pueden paralizar completamente los sistemas y/o borrar todos los datos del disco duro.

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres, también han utilizado el correo electrónico y los "chat rooms" o salas de tertulia de la Internet para buscar presas vulnerables. Además de las incursiones por las páginas particulares de la red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes y/o vender mercancías y servicios prohibidos, como armas, drogas, pornografía, medicamentos sin receta ni regulación.

Impacto a Nivel Social

La proliferación de los delitos informáticos ha hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general. Este hecho puede

obstaculizar el desarrollo de nuevas formas de hacer negocios, por ejemplo el comercio electrónico puede verse afectado por la falta de apoyo de la sociedad en general.

Las personas con conductas maliciosas están cada vez más ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global, pese al grado de especialización técnica que requieren los delincuentes para cometer éste tipo de delitos.

También se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación del personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. Estas personas pueden ser engañadas si en un momento dado requieren tener acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet, correo electrónico, etcétera.

La falta de cultura informática puede impedir la lucha contra los delitos informáticos de parte de la sociedad, por lo que el componente educacional es un factor clave en la minimización de esta problemática.

Impacto en la esfera judicial

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo, el sabotaje, etc. se consideren ilegales también en el mundo virtual.

Las leyes sobre el uso indebido de las computadoras ahora son más severas, los castigos impuestos a todo el que interfiera con los sistemas computacionales por entrada, modificación, uso o intercepción de material computarizado sin autorización son cada vez más explícitos en las leyes de algunos países, cada vez son más los grupos especializados en seguir la pista a los delincuentes cibernéticos integrado por oficiales de la ley y peritos con avanzados conocimientos de informática.

Pese a éstos y otros esfuerzos, las autoridades aún enfrentan graves problemas en materia de informática. El principal de ellos es la facilidad con que se traspasan las fronteras, por lo que la investigación, enjuiciamiento y condena de los transgresores

se convierte en un dolor de cabeza jurisdiccional y jurídico. Además, una vez capturados, los oficiales tienen que extraditarlos para que se les siga juicio en otro lugar y transferir las pruebas -y a veces los testigos- al lugar donde se cometieron los delitos.

La investigación policial se obstaculiza por la doble tipificación penal -la carencia de leyes similares en los países- y esto impide la cooperación oficial, la policía del país de los piratas pueden requisar el apartamento del pirata e incluso incautar su equipo y archivos de computadora, aduciendo posibles violaciones de las leyes nacionales, sin embargo, si los países no tienen firmado acuerdos de extradición por delitos de informática no hay nada que hacer.

Destrucción u ocultación de pruebas

Otro grave obstáculo al enjuiciamiento por delitos cibernéticos es el hecho de que los delincuentes pueden destruir fácilmente las pruebas cambiándolas, borrándolas o trasladándolas. Si los agentes del orden operan con más lentitud que los delincuentes, se pierde gran parte de las pruebas; o puede ser que los datos estén cifrados, una forma cada vez más popular de proteger tanto a los particulares como a las empresas en las redes de computadoras.

Tal vez la criptografía estorbe en las investigaciones penales, pero los derechos humanos podrían ser vulnerados si los encargados de hacer cumplir la ley adquieren demasiado poder técnico. Las empresas electrónicas sostienen que el derecho a la intimidad es esencial para fomentar la confianza del consumidor en el mercado de la Internet y los grupos defensores de los derechos humanos desean que se proteja el cúmulo de datos personales archivados actualmente en las bases de datos electrónicas.

Las empresas también recalcan que la información podría caer en malas manos, especialmente en países con problemas de corrupción, si los gobiernos tienen acceso a los mensajes en código.

Impacto en la identificación de delitos a Nivel Mundial.

En un Comunicado de prensa (2000), del Centro de Información de las Naciones Unidas para España en la lucha contra la delincuencia en Internet señalan que las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición

para poder alcanzar a los delincuentes. Ya se han iniciado algunos esfuerzos al respecto.

Un grupo europeo de especialistas sobre delitos en la tecnología de la informática ha publicado un manual sobre el delito por computadora, en el que se enumeran las leyes pertinentes en los diversos países y se exponen técnicas de investigación, al igual que las formas de buscar y guardar el material electrónico en condiciones de seguridad.

El Instituto Europeo de Investigación Antivirus (1991) colabora con las universidades, la industria, los medios de comunicación, con expertos técnicos en seguridad y asesores jurídicos de los gobiernos, agentes del orden y organizaciones encargadas de proteger la intimidad a fin de combatir los virus de las computadoras o "caballos de Troya". También se ocupa de luchar contra el fraude electrónico y la explotación de datos personales.

Los países del Grupo de los Ocho[8] aprobaron una estrategia innovadora en la guerra contra el delito de "tecnología de punta". El Grupo acordó que establecería modos para determinar rápidamente la proveniencia de los ataques por computadora e identificar a los piratas, usar enlaces por vídeo para entrevistar a los testigos a través de las fronteras y ayudarse mutuamente con capacitación y equipo. También decidió que se uniría a las fuerzas de la industria con miras a crear instituciones para resguardar las tecnologías de computadoras, desarrollar sistemas de información para identificar casos de uso indebido de las redes, perseguir a los infractores y recabar pruebas.

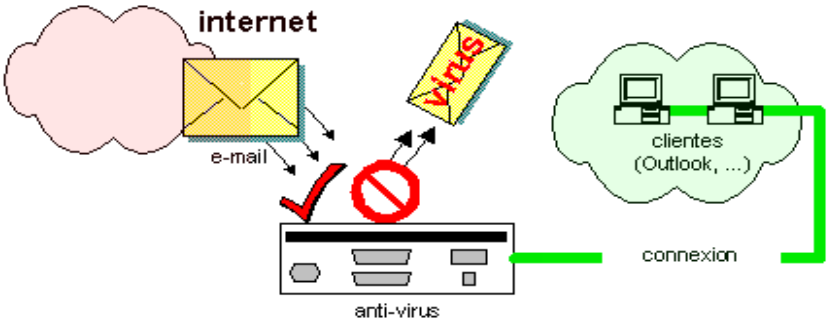
El obstáculo mayor a la adopción de una estrategia del tipo Grupo de los Ocho a nivel internacional es que algunos países no tienen la experiencia técnica ni las leyes que permitirían a los agentes actuar con rapidez en la búsqueda de pruebas en sitios electrónicos -antes de que se pierdan- o transferirlas al lugar donde se esté enjuiciando a los infractores.

4.5 SEGURIDAD CONTRA EL DELITO INFORMÁTICO

Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000), señalan que hoy en día, muchos usuarios no confían en la seguridad del Internet, por ejemplo, pues temen que alguien pueda conseguir el número de su tarjeta de crédito mediante el uso de la red. Ellos temen que otros descubran su código de acceso de la cuenta del banco y entonces transferir fondos a la cuenta del hurtador.

[8] Grupo de los Ocho (G-8) países más industrializados del mundo (Alemania, Canadá, Estados Unidos, Francia, Gran Bretaña, Italia, Japón y Rusia).

Todas las organizaciones manifiestan una gran preocupación de que información confidencial caiga en manos de personas no autorizadas, de que sus competidores tengan conocimiento sobre información patentada que pueda perjudicarlos. La seguridad significa guardar "algo seguro ", "algo" que puede ser un objeto, un secreto, un mensaje, una aplicación, un archivo, un sistema o una comunicación interactiva y "seguro" los medios son protegidos desde el acceso, el uso o alteración no autorizada.



Para guardar objetos seguros, es necesario lo siguiente:

- *La autentificación* (promesa de identidad): La prevención de suplantaciones, que se garantice que quién firma un mensaje es realmente quién dice ser.
- *La autorización*: Se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan.
- *La confidencialidad o privacidad*: Es el más obvio de los aspectos y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada.
- *La integridad de datos*: Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., ya sea durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y sabiendo que es importante, simplemente lo intercepte y lo borre.
- *La disponibilidad de la información*: Se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, ya sea por ataque doloso, mala operación accidental, situaciones fortuitas o de fuerza mayor.
- *Controles de acceso*: Esto es, quién tiene autorización y quién no, para acceder a una información determinada.

Son los requerimientos básicos para la seguridad que deben proveerse de una manera confiable. Los requerimientos cambian ligeramente, dependiendo de lo que se está asegurando. La importancia de lo que se está asegurando y el riesgo potencial

involucra en dejar uno de estos requerimientos o tener que forzar niveles más altos de seguridad.

Estos requerimientos básicos no son simplemente requerimientos para el mundo de la red, sino también para el mundo físico. La autenticación y el asegurar los objetos es una parte de nuestra vida diaria. La comprensión de los elementos de seguridad y como ellos trabajan en el mundo físico, puede ayudar para explicar cómo estos requerimientos se encuentran en el mundo de la red y dónde se sitúan las dificultades.

Seguridad contra el delito en las funciones de los sistemas

Una estrategia para alcanzar las propiedades de auditabilidad, integridad y controlabilidad es la implantación de controles funcionales para el dominio de cada interfase. Las funciones son descritas en la secuencia en las que son diseñadas dentro de un sistema.

- **Identificación**: La función de identificación nos permite establecer como su nombre lo dice, identificadores (nombres, símbolos) para cada usuario y cada recurso del sistema identifica a los usuarios, hardware, software y demás recursos disponibles para el sistema.
- **Autentificación**: Esta función se encarga de reunir evidencias para cumplir con un determinado nivel de riesgo, para que la exigencia de identidad sea valida, esto puede ser llevado a cabo mediante comparaciones de algo que el individuo sepa, tenga, sea o pueda hacer y que sea factible de ser comparado. Por ejemplo:

  Algo que él sepa: (contraseña) Un código o palabra que solamente él y el sistema conozcan.

  Algo que él posea: (foto de identificación) Alguna foto personal que pueda ser comparada con una imagen de la misma persona almacenada en memoria.

  Algo que él sea: (apariencia física) Una comparación de cuerpo entero en base a un sistema óptico.

  Algo que él pueda hacer: (su firma) Toda firma posee un estilo único que es susceptible de ser analizado por computadora.
- **Autorización**: El único propósito de la función de autorización es establecer quién y qué le esta permitido con respecto a un recurso determinado, esta función generalmente relaciona a un usuario con un recurso a través de ciertas reglas definidas para su autorización.

  Esto significa que la autorización establece reglas que restringen a los usuarios a llevar acabo solo acciones predefinidas en el recurso accesado, todos los usuarios sin excepción deberán tener una autorización explícita de la gerencia para accesar los recursos. Un ejemplo típico son los permisos que se definen en el sistema operativo UNIX.

- **Delegación**: Para poder mantener y aplicar la función de autorización, es necesario delegar, esta función determina quién y bajo que circunstancias, podrá ejercitar o cambiar las reglas de autorización.

  En los pequeños sistemas, esta tarea puede ser llevada a cabo por el administrador de seguridad, en sistemas muy grandes que poseen una compleja estructura de usuarios, recursos, ubicaciones y actividades puede requerir de un sofisticado mecanismo de delegación que les permita el manejo para actualizar las reglas de autorización en tiempos reales para necesidades reales.

  Muchos de los sistemas que se encuentran actualmente en el mercado están diseñados para que solamente el operador designado o controlado pueda cambiar identificadores de operación.

- **Seguimiento**: Provee registros escritos del uso de los recursos del sistema y de todas las actividades significativas, ofrece beneficios mayores al permitir reconstruir información, hacer respaldos y recuperaciones, puntualizar la contabilidad, seguir pistas e identificaciones, ganar visibilidad y ver que ésta sucediendo. Los sistemas nunca deberían ser diseñados sin tener la capacidad de hacer seguimiento (quién y qué capturó, donde, porqué y cómo), es la manera más efectiva para monitorear la operación, objetivos, reglas y estándares de ejecución.

- **Reconocimiento**: Es necesario que alguien revise el seguimiento, monitoreé las variaciones de actividades con respecto al uso, contenido y comportamiento esperado, en realidad lo que se busca con esta función es llegar más allá del seguimiento, informando a la gerencia o jefatura de todo tipo de irregularidades de cualquier comportamiento inesperado, es entonces cuando la jefatura deberá tomar las acciones correctivas pertinentes.

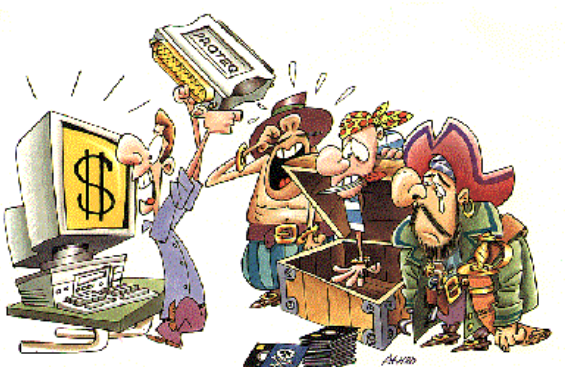
  Podría confundirse el objetivo de esta función con la de seguimiento, sin embargo, la anterior se limita a la capacidad de registrar las operaciones y ésta última se refiere a las acciones de deslindar responsabilidades y revisar oportunamente aquellos registros con el objeto de preparar las acciones correctivas a la brevedad posible

Medidas de prevención.

Para Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000), existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad y no es una tarea trivial. Ello no solamente requiere que el personal técnico comprenda todas las vulnerabilidades que están involucradas, también requiere que ellos se comuniquen efectivamente con la gerencia. La gerencia debe decidir finalmente cuánto de riesgo debe ser tomado con el activo de la compañía y cuánto se esta dispuesto a gastar con el fin de minimizar los riesgos.

Es responsabilidad del personal técnico asegurar que la gerencia comprenda las implicaciones de añadir acceso a la red y a las aplicaciones sobre la red, de tal manera que la gerencia tenga la suficiente información para la toma de decisiones. Si la política de seguridad no viene desde el inicio, será difícil imponer incluso medidas de seguridad mínimas. Es mejor trabajar con estos temas antes de tiempo y poner la política por escrito. Las políticas pueden entonces ser comunicadas a los empleados por la gerencia.

Debe crearse un procedimiento de auditoria que revise el uso de la red, servidores y sistemas aplicativos de forma periódica y el desarrollo de una política de uso de los recursos. El desarrollo de una política de seguridad comprende la identificación de los activos de la organización, identificación y evaluación de amenazas potenciales, análisis del riesgo, implementación de medidas preventivas para hacer frente a los riesgos.



- *Identificación de los activos de la organización*: Consiste en la creación de una lista de todas las cosas que precisen protección. Hardware: computadores y equipos de telecomunicación. Software: programas fuente, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones. Datos: copias de seguridad, registros de auditoria, bases de datos.
- *Identificación y evaluación de amenazas potenciales*: En este análisis se irá haciendo una lista que incluya todas las cosas indeseables que pudieran ocurrirle a los activos de la organización, ciertamente prevalece la incertidumbre de sí estaremos ya incluyendo todas las posibles amenazas y aún más, dentro de las que hemos identificado, ¿Se encuentran las más críticas?
- *Análisis del riesgo:* El objetivo de un análisis de riesgos es el cuantificar las amenazas potenciales para que sean establecidas las bases para una apropiada selección de costo eficiencia de los controles de seguridad. Conlleva la determinación de lo que se necesita proteger. No es más que el proceso de examinar todos los riesgos y valorarlos por niveles de seguridad.
- *Implementación medidas preventivas para hacer frente a los riesgos:* Cabe sugerir que para poder combatir el delito, es necesario un control y tener en consideración medidas preventivas, a través de diversas formas de carácter administrativo, de entre las principales tenemos:
  - Incluir en todos los documentos normativos, reglas, políticas, procedimientos de trabajo que consideren medidas preventivas y correctivas encaminadas a la práctica del delito informático.
  - Incluir en los procedimientos de trabajo todas las *tecnologías disponibles para hacer frente a los riesgos que entrañan los delitos informáticos.*

Otras formas de control preventivo y correctivo según Téllez, J. (1996).

- Aplicación de un examen psicométrico al personal informático previo al ingreso a la organización.
- Introducción de cláusulas especiales en los contratos de trabajo con el personal informático que por el tipo de labores a realizar así lo requiera.
- Establecimiento de un código ético de carácter interno en la organización.
- Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
- Capacitación adecuada del personal informático a efecto de evitar actitudes negligentes.
- Identificación y, en su caso, segregación del personal informático descontento.
- Rotación en el uso de claves de acceso al sistema.

Algunas formas de carácter técnico según Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000).

- Las herramientas y aplicaciones forman la base técnica de la política de seguridad, pero la política de uso aceptable debe considerar otros aspectos:

  ¿Quién tiene permiso para usar los recursos?

  ¿Quién esta autorizado a conceder acceso y a aprobar los usos?

  ¿Quién tiene privilegios de administración del sistema?

  ¿Qué hacer con la información confidencial?

  ¿Cuáles son los derechos y responsabilidades de los usuarios?

  ¿Cuáles son las restricciones del usuario?

  ¿Los usuarios pueden compartir cuentas?

  ¿Cómo mantener las contraseñas de los usuarios?

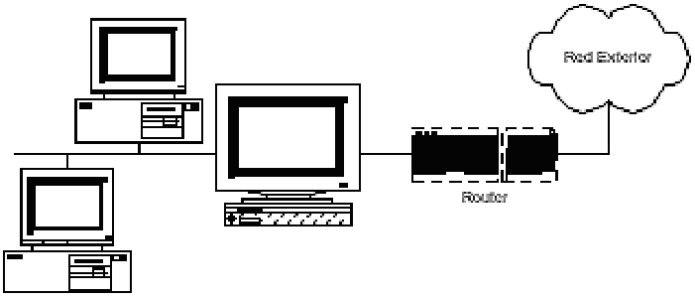
  ¿Con qué frecuencia deben cambiar sus contraseñas?

  ¿Quién debe realizar copias de seguridad de la información?

  ¿Con qué frecuencia se deben realizar copias de seguridad?

- Claves de identidad: Definir quiénes tienen acceso a las diferentes partes de la red, de los sistemas computacionales, de los directorios de las bases de datos, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente (Evitar las passwords "por defecto" o demasiado obvias).

- *Firma digital:* El cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje, en otras palabras, asegurar que proviene de quien dice. De esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma. Además, garantizan la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión. La firma se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje.
- *Firewalls:* Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner murallas. Los mecanismos más usados para la protección de la red interna de otras externas son los firewalls o cortafuegos. Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según nuestras indicaciones.



Valor probatorio de los soportes informáticas.

Para Téllez, J. (1996), las pruebas son hechos, surgen de la realidad extra-jurídica, del orden natural de las cosas. Las pruebas no son una creación del derecho. Su existencia y valor se toma de la realidad extra-jurídica preconstruidas como fuentes (documento, testigo, cosa litigiosa, etc.) y constituidas como medios (actuaciones judiciales, como por ejemplo la declaración de un testigo).

De entre los principales medios de prueba se tienen:

- Confesional: Es una declaración de parte que contiene el reconocimiento de un hecho de consecuencias jurídicas desfavorables para el confesante.
- Documental: También llamadas literal, es la que se hace por medio de documentos, en la forma previamente establecida en las leyes procesales.
- Pericial: Se deriva de la apreciación de un hecho por parte de un observador con preparación especial, obtenida por el estudio de la materia a que se refiere, o simplemente por la experiencia personal.
- Testimonial: Dada por los testigos como aquellas personas que comunican al juez el conocimiento que posee de determinado hecho (o hechos), cuyo esclarecimiento interesa para la decisión de un proceso.
- Inspección judicial: Consiste en un examen directo por el juez de la cosa mueble o inmueble sobre que recae para formar su convicción sobre el estado o situación en que se encuentra en el momento en que la realiza pueda ser fuera o en el juzgado.

- Fama pública: Estado de opinión sobre un hecho que se prueba mediante el testimonio de personas que la ley considera hábiles para este efecto.
- Presunciones: Aquellas operaciones lógicas mediante las cuales, partiendo de un hecho conocido, se llega a la aceptación como existente de otro desconocido o incierto.

4.6 AUDITORIA INFORMÁTICA RELACIONADA CON EL DELITO

Para Landaverde, M. L., Soto, J. G. & Torres, J. M. (2000) es importante establecer claramente cual es el papel que juega el auditor informático en relación con la detección y minimización de la ocurrencia de delitos informáticos dentro de la organización a que presta sus servicios. Para lograr establecer dicho rol se debe examinar la actuación del auditor frente a la ocurrencia de delitos, estrategias para evitarlos, recomendaciones adecuadas, conocimientos requeridos, en fin una serie de elementos que definen de manera inequívoca el aporte que éste brinda en el manejo de los casos de delitos informáticos.

Rol del Auditor Informático

El rol del auditor informático solamente está basado en la verificación de controles, evaluación del riesgo de fraudes, diseño y desarrollo de exámenes que sean apropiados a la naturaleza de la auditoría asignada y que deben razonablemente detectar:

- Irregularidades que puedan tener un impacto sobre el área auditada o sobre toda la organización.
- Debilidades en los controles internos que podrían resultar en la falta de prevención o detección de irregularidades.

La auditoria consiste en verificar que todas las tareas que se realicen en las áreas de cómputo se hagan conforme a la normatividad, que todas las actividades se realicen adecuadamente y que los controles sean cumplidos, etc.

Detección de delitos

El auditor informático al detectar irregularidades en el transcurso de sus revisiones que le indiquen la ocurrencia de un delito informático, deberá realizar lo siguiente:

1. Determinar si se considera la situación un delito realmente.
2. Establecer pruebas claras y precisas.

3. Determinar los vacíos de la seguridad existentes y que permitieron el delito.
4. Informar a la autoridad correspondiente dentro de la organización.
5. Informar a autoridades regulatorias cuando es un requerimiento legal.

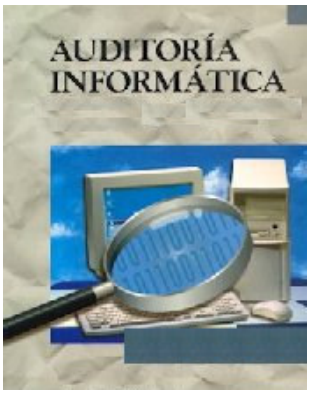
Es importante mencionar que el auditor debe manejar con discreción la situación y con el mayor profesionalismo posible, evitando su divulgación al público o a empleados que no tienen nada que ver. De no manejarse adecuadamente el delito, podría tener algunos efectos negativos en la organización, tales como:

- Se puede generar una desconfianza de los empleados hacia el sistema.
- Se pueden generar más delitos al mostrar las debilidades encontradas.
- Se puede perder la confianza de los clientes, proveedores e inversionistas hacia la empresa.
- Se pueden perder empleados clave de la administración, aún cuando no estén involucrados en la irregularidad debido a que la confianza en la administración y el futuro de la organización puede estar en riesgo.

Resultados de la auditoria

Si por medio de la auditoria informática realizada se han detectado la ocurrencia de delitos, el auditor deberá sugerir acciones específicas a seguir para resolver el vacío de seguridad, para que el grupo de la unidad informática pueda actuar, dichas acciones expresadas en forma de recomendación pueden ser como las siguientes:

- Recomendaciones referentes a la revisión total del proceso involucrado.
- Inclusión de controles adicionales.
- Establecimiento de planes de contingencia efectivos.
- Adquisición de herramientas de control, etc.



Además de brindar recomendaciones, el auditor informático deberá ayudar a la empresa en el establecimiento de estrategias contra la ocurrencia de delitos, ejemplos de estrategias podrían ser las siguientes:

- Adquisición de herramientas computacionales de alto desempeño.
- Controles sofisticados.
- Políticas, procedimientos y estándares bien establecidos y probados.
- Revisiones continuas cuya frecuencia dependerá del grado de compromiso en la solución a las recomendaciones realizadas.

Si bien es cierto que las recomendaciones dadas por el auditor y las estrategias implementadas por la organización minimizan el grado de amenaza que representa los delitos informáticos, es importante tomar en cuenta que aún cuando todos los procesos de auditoría estén debidamente diseñados y se cuente con las herramientas adecuadas, no se puede garantizar que las irregularidades puedan ser detectadas.

Perfil del Auditor Informático

El auditor informático como encargado de la verificación y certificación de la informática dentro de las organizaciones, debe contar con un perfil que le permita desempeñar su trabajo con la calidad y la efectividad esperada. Algunas competencias con las que debe contar el auditor son las siguientes:

Conocimientos generales.

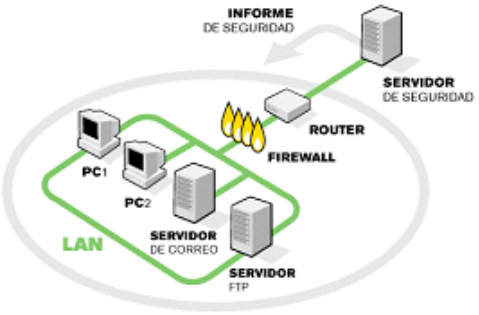
- Todo tipo de conocimientos tecnológicos, de forma actualizada y especializada respecto a las plataformas existentes en la organización.
- Normas estándares para la auditoría interna.
- Políticas organizacionales sobre la información y las tecnologías de la información.
- Características de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente, compensaciones monetarias a los empleados, extensión de la presión laboral sobre los empleados, historia de la organización, cambios recientes en la administración, operaciones o sistemas, la industria o ambiente competitivo en la cual se desempeña la organización, etc.
- Aspectos legales.

Herramientas.

- Herramientas de control y verificación de la seguridad.
- Herramientas de monitoreo de actividades, etcétera.

Técnicas.

- Identificación de amenazas potenciales.
- Definición de los puntos de control (PC) de un sistema.
- Identificación de problemas potenciales.
- Mapeo de los problemas potenciales.
- Limitación y análisis del riesgo.
- Técnica para obtener el costo / pérdida.



- Controles Básicos.
- Selección de Controles.

Si, durante el curso de auditoría, los auditores tuvieran razones para pensar que las disposiciones de seguridad de la empresa y los planes de emergencia no son los adecuados, deberán reflejar sus opiniones a la Alta Dirección, a través del informe de auditoria.

Si sospechase de algún delito informático, el auditor debe avisar a la alta dirección para que se ponga en contacto con su asesor jurídico o con la policía, sin levantar las sospechas del personal o los clientes que estuviesen involucrados. El auditor debe asegurar también todas las evidencias que pudieran utilizarse como prueba y custodiarlas para que ninguna persona que sea sospechosa del delito tenga acceso a ellas.