UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

"PROCEDIMIENTOS DE AUDITORIA APLICADOS A LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS PARA LA DETECCIÓN, PREVENCIÓN Y CORRECCIÓN DE DELITOS INFORMÁTICOS".

Trabajo de Investigación Presentado Por:

GRUPO No. 22
López Cabrera Sandra Elizabeth
Molina Ventura José Raúl
Quintanilla Quintanilla Flor de María

Para Optar al grado de:
LICENCIADO EN CONTADURÍA PÚBLICA

Mayo 2008.

San Salvador, El Salvador, Centro América

DEDICATORIA
TRABAJO DEDICADO A:

A Dios Todopoderoso por la oportunidad que me brinda de llegar a culminar una etapa más de mi vida, a mis padres Marta Gladis Cabrera y Tomás Antonio López por siempre estar a mi lado apoyándome para seguir adelante, a mis hermanos Marcos Antonio López, Carlos Humberto López, Jackelin Azucena López y Adonis Alexander López, por su apoyo, a mis amigas y amigos Ana Mirian Miranda, Reina Arevalo, Guillermo Cativo y Erick que nunca me han dejado en la buenas y en las malas y de quienes recibí siempre palabras de apoyo, a mis compañeros de grupo y a mis maestros de quienes recibí el conocimiento nos transmitieron en cada una de las clases que de ellos recibí.

Sandra López

A Dios Padre Todopoderoso, a Dios Hijo y Espíritu Santo, que han sido la fortaleza y guía espiritual y que han permitido realizar esta meta propuesta, prestándome vida, entendimiento, dedicación y sabiduría; a mis padres Manuel Quintanilla y Ester Quintanilla quienes me brindaron su amor y apoyo incondicional, a mi hermano y familia por estar siempre presente ofreciéndome su ayuda y cariño, a todos los catedráticos que me trasmitieron sus conocimientos durante la carrera, a mis amistades y compañeros que estuvieron presente en el momento oportuno para portar su granito de arena. A todos infinitas gracias por su paciencia, amor y comprensión.

Flor Quintanilla

A Dios Padre, Hijo y Espíritu Santo, por darme esta oportunidad de llegar a culminar una de las metas más importantes de mi vida; a mis padres José Miguel Molina y Vilma Esperanza Ventura, que me brindaron su cariño y apoyo para salir adelante en los momentos más difíciles; a todos mis amigos y amigas, por sus palabras de aliento en los momentos duros; a Juan Mejía que es como mi hermano; a mis maestros, por sus consejos y conocimientos que me inculcaron y especialmente, a mis amigas y compañeras de grupo Flor Quintanilla, por todo el cariño y paciencia y a Sandra López, por todo su amor y comprensión que me brindó aún cuando no lo merecía. A todos les agradezco infinitamente por formar parte de mi vida y deseo que Dios les colme de muchas bendiciones.

Raúl Molina

UNIVERSIDAD DE EL SALVADOR
AUTORIDADES UNIVERSITARIAS

Rector : Master Rufino Antonio Quezada Sánchez

Secretario : Lic. Douglas Vladimir Alfaro Sánchez

Decano de la Facultad
de Ciencias Económicas
: Lic. Roger Armando Arias

Secretario de la Facultad
de Ciencias Económicas
: Lic. José Ciriaco Gutiérrez Contreras

Asesor Director : Lic. Mario Hernán Cornejo

Jurado examinador
: Lic. Mario Hernán Cornejo
Lic. José Roberto Chacón Zelaya

Mayo del 2008

San Salvador, El Salvador, Centro América

ÍNDICE

CAPITULO III – PROCEDIMIENTOS DE AUDITORIA PARA LA DETECCIÓN, PREVENCIÓN Y CORRECCIÓN DE DELITOS INFORMÁTICOS.

ÍNDICE DE CUADROS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

Las cajas y bancos afiliados al sistema Fedecrédito son instituciones que se dedican a la prestación de fondos monetarios a sus asociados; para el proceso de sus transacciones hacen uso de sistemas de información computarizados que les ayuda a controlar el manejo de la información de cada uno de sus socios.

Por el tipo de actividades que realizan, pueden ser víctima de cualquier tipo de delito informático que conlleve a un fraude a la institución y por consiguiente a sus asociados; eso puede surgir por la falta de procedimientos de auditoría adecuados a la supervisión y seguridad del sistema informáticos.

Por lo anterior, es importante implementar procedimientos de auditoría de acuerdo a la necesidad de la institución; que sirvan como ayuda o soporte para la protección de los sistemas utilizados por estas instituciones.

De acuerdo a la utilización de procedimientos de auditoría aplicados a los sistemas de información, que detecten, prevengan y que en cierta manera corrijan delitos informáticos, la entidad obtendrá una disminución de riesgos en cuanto a la pérdida de información, sabotaje al sistema, manipulación de datos, robo de información, y cualesquier otro delito informático.

La metodología utilizada en la investigación de campo está compuesta por el conocimiento sobre los delitos informáticos y procedimientos de auditoría de sistemas por parte de las instituciones, la capacitación que se le brinda personal encargado del área informática, como a los usuarios del sistema, conocimiento de los controles generales del sistema de información, el entorno físico y el control de la información generada por sistema.

Al conocer la problemática y encontrar las deficiencias en los controles implementados por las cajas y bancos, se vuelve necesaria la utilización de procedimientos que aseguren la integridad del sistema y resulten ser eficaces, confiables y efectivos.

Los procedimientos que se presentan en este documento están orientados a la auditoría de sistemas para que puedan ser aplicados a los sistemas de información con el objeto de detectar, prevenir y corregir delitos informáticos; y pueden ser utilizados como herramienta de estudio y evaluación en la práctica de la profesión de la contaduría pública, tanto por estudiantes como también por profesionales.

INTRODUCCIÓN

Toda institución busca ser un lugar seguro donde las personas que hacen uso de sus servicios tengan la certeza de que no serán víctimas de algún tipo de delito.

Las cajas y los bancos afiliados al sistema Fedecrédito en la actualidad no cuentan con procedimientos de auditoría que les ayuden a detectar, prevenir y corregir delitos informáticos que se pueden dar en sus instituciones; por lo que la investigación realizada se lleva a cabo con el objeto de brindar una propuesta de procedimientos de auditoría que puede minimizar el riesgo de ocurrencia de estos delitos, esta investigación está compuesta por cuatro capítulos que son el marco teórico, el diseño metodológico y diagnóstico, la propuesta de procedimientos auditoría y las conclusiones y recomendaciones al respecto del tema.

En el primer capítulo se presentan las generalidades de las instituciones afiliadas al sistema Fedecrédito de los delitos informáticos de los cuales pueden llegar a ser víctimas.

En el segundo capítulo, se desarrolla un diagnóstico sobre la situación en la que se encuentran estas instituciones en cuanto a los procedimientos de auditoría que estas realizan a sus sistemas de información computarizados.

Dentro de la estructura del tercer capítulo, se presenta la propuesta de procedimientos de auditoría que pueden ser utilizados para la detección, prevención y posible corrección de los delitos informáticos a los cuales están propensas estas instituciones.

En el cuarto y último capítulo, están contenidas las conclusiones y recomendaciones a las que se llegó como grupo con respecto de la investigación realizada.

CAPITULO I: MARCO TEÓRICO

1.1 GENERALIDADES DE LA AUDITORIA DE SISTEMAS

1.1.1 Conceptualización de Auditoria de Sistemas

La palabra auditoría proviene del latín auditorius y de esta se deriva la palabra auditor, quien tiene la virtud de oír y revisar cuentas; pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando, para que por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

Algunos autores proporcionan otros conceptos, pero todos coinciden en hacer énfasis en la revisión, evaluación y elaboración de un informe para la administración, encaminado a un objetivo específico en el ambiente computacional y los sistemas.

A continuación se detallan algunos conceptos recogidos de algunos expertos en la materia:

Auditoría de Sistemas es:

a. La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación de éstos con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.
b. La actividad dirigida a verificar y juzgar información.
c. El examen y evaluación de los procesos del Área de Procesamiento Automático de Datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.
d. Es el examen o revisión de carácter objetivo (independiente), crítico(evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a:

    1. Eficiencia en el uso de los recursos informáticos
    2. Validez de la información
    3. Efectividad de los controles establecidos

1.1.2 Tipos de Auditoria de Sistemas

a. Auditoría de ciclo de vida del desarrollo de los sistemas.

Se evalúa según el ciclo de vida del desarrollo de un sistema, los controles y el uso de una metodología hasta la liberación del sistema.

b. Auditoría de sistemas de información en operación.

Comprende la evaluación de los sistemas que se encuentran ofreciendo algún tipo de servicio de computación. Asimismo evalúa los controles de acuerdo con su mantenimiento y en cada una de sus funciones: entrada, procesamiento y salida.

1.2 LOS DELITOS INFORMÁTICOS

1.2.1 Antecedentes de los Delitos Informáticos

1.2.1.1 A Nivel Mundial

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación.

Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que facilita la comisión de los delitos.

En 1986 la OCDE publicó un informe titulado “Delitos de informática: análisis de la normativa jurídica”, donde se

reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992, elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

En 1990, la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello, se había difundido la comisión de actos delictivos.

En 1992, La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad"

En Noviembre de 1997 se realizó la Segunda Jornada Internacional sobre el Delito Cibernético en Mérida, España; donde se desarrollaron temas tales como:

a. Aplicaciones en la Administración de las Tecnologías Informáticas/cibernéticas.
b. Blanqueo de capitales, contrabando y narcotráfico Hacia una policía Europea en la persecución del delito Cibernético.
c. Internet: a la búsqueda de un entorno seguro.
d. Marco legal y Deontológico de la Informática.

1.2.1.2 A Nivel de El Salvador

En El Salvador también se han dado casos de delitos informáticos, dichos delitos dieron como resultado fraudes financieros, de los cuales la población teme que esté sucediendo en la mayoría de las instituciones públicas y privadas; dentro de este tipo de instituciones se pueden mencionar los siguientes casos ocurridos:

a. El caso de los empleados de la Corte Suprema de Justicia[1], que de acuerdo a las investigaciones, comenzaron a apropiarse ilegalmente de un aproximado de 199 mil dólares, desde abril del dos mil cinco, hasta abril del dos mil siete, a través de la incorporación de planillas adicionales de 50 personas, quienes laboraban haciendo interinatos.

[1] Fiscalia General de la Republica, Oficina de Prensa y Protocolo; Boletín de Prensa, “Orden de captura para involucrado en fraude a CSJ”, San Vicente._ 29/10/2007.

De acuerdo a los Fiscales del caso, los acusados en forma ilícita extendieron cheques a nombre de los 50 trabajadores contratados interinamente en diferentes Tribunales del Departamento de La Paz, y los fondos fueron depositados en cuentas de varias instituciones.

Además se hicieron pagos indebidos en varias Asociaciones de Fondos de Pensiones, y del Instituto Salvadoreño del Seguro Social.

b. Fraude en el Banco de Fomento Agropecuario (BFA)[2]

Entre los años 1995 y 1999, hubo un fraude en el BFA por un monto de 138.6 millones de colones (alrededor de 16 millones de dólares). Por el hecho fueron acusados el presidente del BFA, Raúl García Prieto y otros altos funcionarios del banco, a quienes se acusó de comprar el ingenio El Carmen por 59 millones de colones y sin poner dinero de garantía. También se les acusó de haber realizado la venta a través de maniobras financieras. Al ex presidente del BFA se le acusó de favorecer la negociación desde su cargo.

La Cámara 2a. de lo Penal luego exoneró de cargos, en forma definitiva, a Enrique Rais, Ruth Salazar Campos, Héctor Cristiani, Luís Omar Cruz Guevara, Ricardo Rivera Villalta y Raúl Castellón Lemus, acusados por delitos de defraudación a la

[2] http://www.elsalvador.com/noticias/2003/09/04/nacional/nacio19.html

economía pública, negociaciones ilícitas y asociaciones ilícitas. García Prieto, quien fue condenado, está prófugo. Fraude a la economía pública y lavado de dinero por parte de empresa financiera.

c. El 19 de julio de 2004 se conoció el fraude cometido por los Inversionistas de Operaciones Bursátiles de Centroamérica (OBC)[3], con un monto de 6.3 millones de dólares. La empresa realizó una captación ilegal de fondos y cometió irregularidades en el manejo y administración de las inversiones. Un total de 400 personas fueron estafadas.

   Uno de los socios fundadores de la empresa es Mauricio Sandoval, ex Director de la Policía Nacional Civil durante el gobierno de Francisco Flores. Hasta la fecha el caso se mantiene estancado en el juzgado Séptimo de Instrucción, debido a la fuga de los dos principales implicados.

1.2.2 Marco Conceptual de los Delitos Informáticos

Es un tanto difícil tratar de dar una definición apropiada y de aceptación general en la mayoría de países del mundo respecto de los delitos informáticos pues son diversas las formas de cometer tales hechos, y en muchas legislaciones se trata de adaptar o asimilar a conductas ya tipificadas en las leyes para efectos del

[3] Fiscalía General de la República. http://64.233.169.104/search?q=cache:OrveP14SSTkJ:www.fgr.gob.sv/sitio/dinamicos/boletinver.asp%3Fid%3D3072+el+salvador,+caso+obc&hl=es&ct=clnk&cd=3&gl=sv

tratamiento legal que estos países deciden dar a los delitos informáticos.

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que no varíe de acuerdo al lugar y al tiempo, lo cual, no ha sido posible pues es difícil enmarcar en una sola definición todo lo que comprende el delito.

Penalistas como Cuello Calón, han tratado de identificar los elementos del delito, según el (Cuello Calón), los elementos integrantes del delito[4] son:

a. El delito es un acto humano, es una acción (u omisión)
b. Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido
c. Debe corresponder a un tipo legal[5] (figura legal de delito), definido por la ley, ha de ser un acto típico.
d. El acto ha de ser culpable, imputable[6] a dolo (intención) o a culpa (negligencia)
e. La ejecución u omisión del acto debe estar sancionada por una pena.

Incluyendo los elementos citados anteriormente, se puede formular una definición de delito, que es, una acción antijurídica

[4] Delitos Informáticos, Melvin Leonardo Landaverde, Octubre 2000
[5] Figura legal bajo la cual la ley da al delito el tratamiento respectivo
[6] Una acción se considera imputable cuando puede ponerse a cargo de una determinada persona

realizada por un ser humano, tipificado en la ley, culpable y sancionado por una pena legal.

Ahora bien, se podría definir el delito informático como toda acción (u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena establecida por las leyes locales. Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo. Es decir, que cualquier hecho ilegal cometido en el cual se use, directa o indirectamente, una computadora es considerado como un delito informático.

Julio Téllez Valdés conceptualiza al "delito Informático" en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Entonces, delitos informáticos, son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio Informático. El delito

Informático implica actividades criminales que en un primer momento los países han tratado de enmarcar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del Derecho.

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora, tales como "delitos informáticos", "delitos electrónicos", “delitos relacionados con la computadora”, "crímenes por computadora", “delincuencia relacionada con el ordenador”.

1.2.3 Caracterización de los Delitos Informáticos

Características de los Delitos Informáticos:

Según el mexicano Julio Téllez Valdés, los delitos informáticos presentan las siguientes características principales:

a. Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya trabajando.

c. 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.
d. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
e. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
i. 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.

1.2.4 Tipificación de los Delitos Informáticos[7]

Téllez Valdés clasifica a estos delitos de acuerdo a dos criterios:

a. Como instrumento o medio.

[7] www.monografias.com

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:

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 ficticia.
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 informáticas en forma no autorizada.
13. Intervención en las líneas de comunicación de datos o teleproceso.

b. 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:

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.).

Los tipos de delitos informáticos reconocidos por las Naciones Unidas, se clasifican en:

a. Fraudes cometidos mediante manipulación de computadoras
b. Falsificaciones informáticas
c. Daños o modificaciones de programas o datos computarizados.

Cuadro 1: Fraudes cometidos mediante manipulación de computadoras.

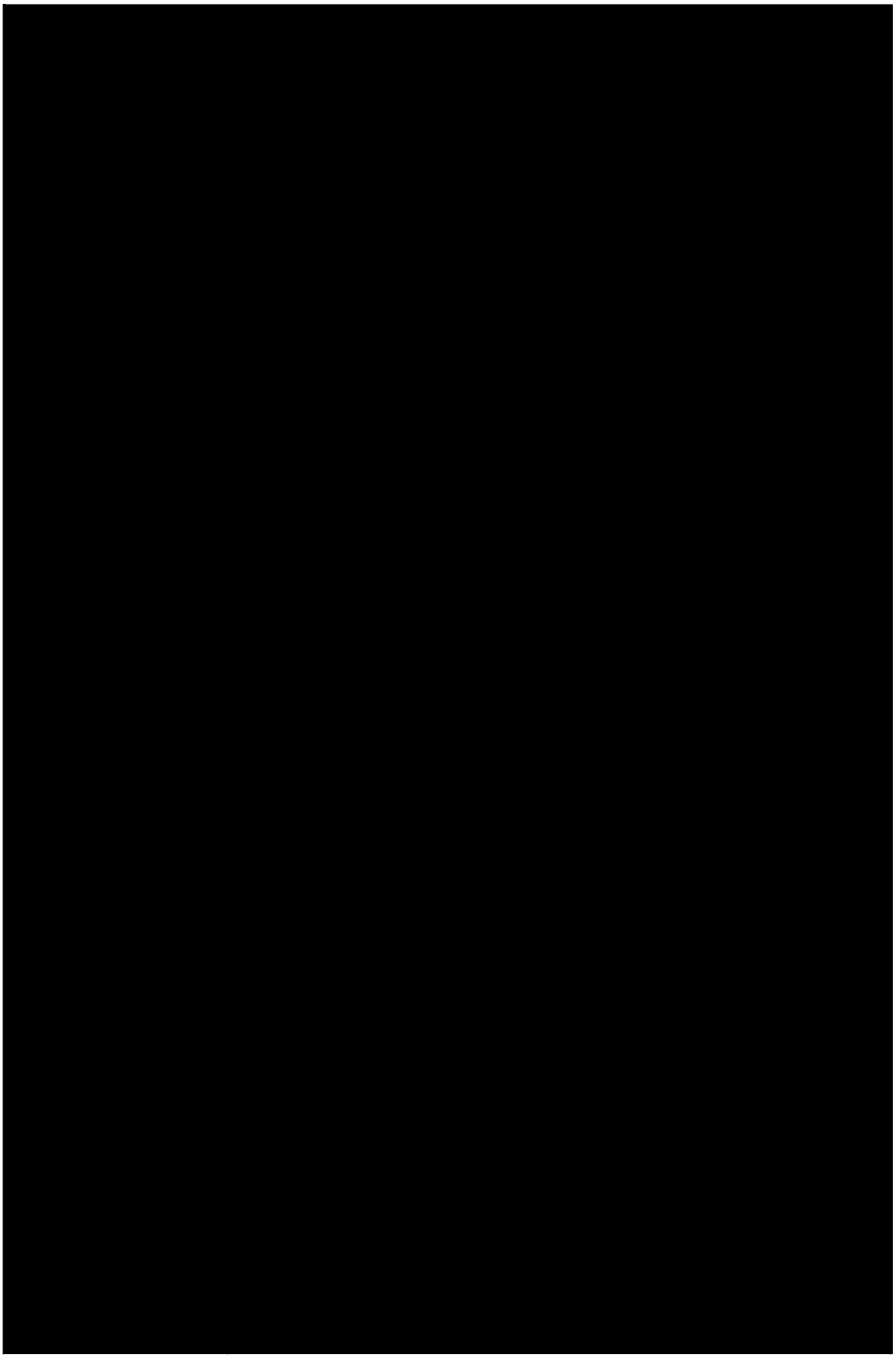
DELITO	DESCRIPCIÓN
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
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 perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Cuadro 2: Falsificaciones informáticas.

DELITO	DESCRIPCIÓN
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. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Cuadro 3: Daños o modificaciones de programas o datos computarizados.

DELITO	DESCRIPCIÓN
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. Las técnicas que permiten cometer sabotajes informáticos son:
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: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.



1.2.5 Incidencia de los Delitos Informáticos en las Empresas

La realización de delitos informáticos que perjudican de cualesquier forma a las empresas, es una cuestión altamente sensible para las entidades afectadas, lo cual se pone de manifiesto en las reacciones que éstas tienen ante los casos de fraude; dos de cada tres entidades mantienen en secreto o dan a conocer información incompleta al respecto.

Los empleados, las autoridades o los medios de comunicación rara vez son informados por temor a la imagen negativa que se pueda proyectar, es decir, a la mala imagen que se genera de la empresa que ha sido objeto de este tipo de hechos, y que, para no perder prestigio ante terceros y sus clientes, decide mejor tomar cartas por ella misma y tratar de enmendar esa vulnerabilidad del sistema informático que poseen.

Como resultado de ello, no suelen iniciarse investigaciones penales al respecto. En la mayoría de los casos, se efectúan investigaciones independientes llevadas a cabo por profesionales expertos en la materia sin que se informe de ello a la policía o las autoridades públicas

El daño económico ocasionado por los autores de los delitos puede ser no muy grave, aunque en algunos casos, si puede llegar a perjudicar a la empresa en gran forma. Muchos navegantes del

ciberespacio, que tienen conocimientos amplios respecto de la informática, solo buscan un poco de diversión y su “pasatiempo”, es violar la seguridad de los sistemas informáticos, para hacerse notar mediante ello y decirle a los programadores de la empresa afectada, que ellos son mejores que las personas que desarrollaron el software, pero también hay muchas personas que, valiéndose de sus habilidades, buscan hacer este tipo de cosas para poder obtener algún tipo de beneficio económico de ello. En la mayoría de los casos, las empresas afectadas tienen que asumir las pérdidas por sí solas. "Las empresas no suelen resarcirse de los daños económicos sufridos" afirma Ignacio Cortés[8].

Se cita el ejemplo de una empresa de telefonía celular la cual fue estafada. La escena hasta parece que fue extraída de una película de ciencia ficción: imagine a una docena de personas, con teléfonos celulares, alrededor de una mesa, marcando simultáneamente el número que aparece en el dorso de una tarjeta de prepago de la más alta denominación. “¡Ocho!”, grita el líder. “¡Ocho!”, repite y marca todo el grupo, y así sucede con el resto de dígitos hasta que ya los han ingresado todos[9].

De esa forma, los doce teléfonos ingresan el código al mismo tiempo y la “recarga” es válida en todos. Prácticamente recargan 12 celulares por el precio de uno. Este hecho ocurrió hace algunos

[8] Senior Manager del área de Forensic de KPMG en España
[9] www.elsalvador.com El Diario de Hoy, Vértice, 27 de febrero de 2005

meses en suelo salvadoreño. Los expertos en informática de la empresa “asaltada” descubrieron la debilidad del sistema e hicieron los cambios necesarios para que el robo no se repitiera.

El delito ni se hizo del conocimiento público ni se llevó ante un juez, pues la empresa de teléfonos no quiso quedar en ridículo ante su competencia ni generar desconfianza entre sus clientes. Sin embargo, ellos no han sido las únicas víctimas de los delincuentes de la era digital en El Salvador.

Este tipo de delitos perjudicarían en gran manera la imagen de cualesquier empresa y en todo caso, el costo de su divulgación al público, pudiese ser más alto que el costo de asumir el delito cometido.

1.2.6 Sujetos que Intervienen en los Delitos Informáticos

1.2.6.1 Sujeto Activo

Al respecto los Doctores Julio Valdés y María Luz Lima, entre otros, sostienen que las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, es decir, 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 informáticos, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente Informático es tema de controversia ya que para algunos dicho nivel no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo 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", término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año 1943.

Efectivamente, este conocido criminólogo señala un sin número de conductas que considera como "delitos de cuello blanco", aún

cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar, las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se consideran a sí mismos "respetables". Otra coincidencia que tienen

estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

Por otra parte, se considera que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo.

1.2.6.2 Sujeto Pasivo

En primer término tenemos que distinguir que el 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", mediante el sujeto pasivo se puede conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

Ha sido imposible conocer la verdadera magnitud de los "delitos informáticos" ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables; que sumado al temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y la consecuente pérdida económica que esto pudiera ocasionar, hace que éste tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

1.2.7 Normativa Técnica Y Legislación Relacionada Con Los Delitos Informáticos

1.2.7.1 Base Técnica

En la actualidad no existe una Base Técnica local que sirva de forma especifica para auditar los sistemas de información computarizados de las empresas; para tal efecto, se considerarán en lo que sean aplicables los objetivos de control recomendados por COBIT, con el fin de desarrollar procedimientos de auditoria que se apliquen a los sistemas de información y que sirvan de guía para la detección, prevención y posible corrección de delitos informáticos. COBIT se divide en cuatro dominios, los cuales son:

1. Planear y Organizar
2. Adquirir e Implementar
3. Entregar y Dar Soporte
4. Monitorear y Evaluar

Estos dominios están compuestos en total por 34 objetivos de control de tecnología de la información de alto nivel para proporcionar asistencia a los auditores de sistemas.

Para efectos de desarrollar los procedimientos de control, se tomará como base el Dominio de Monitoreo y Evaluación, dentro del cual se encuentran los siguientes objetivos de control de alto nivel:

a. Monitorear y evaluar el desempeño de la Tecnología de Información (TI).

b. Monitorear y evaluar el control interno.

c. Garantizar el cumplimiento regulatorio.

d. Proporcionar Gobierno de Tecnología de Información.

1.2.7.2 Legislación Aplicable a los Delitos Informáticos

1.2.7.2.1 A Nivel Mundial

A medida que se han ido innovando las tecnologías de la información, se ha hecho tanto buen uso como malo de estos recursos, pues no solo son una herramienta que busca facilitar las actividades diarias de las personas; sino también, son una forma malintencionada de cometer delitos informáticos.

En muchos países no se cuenta con una normativa reguladora adecuada en la cual se tipifiquen exactamente este tipo de conductas delictivas, es por eso que, se asocian estas conductas con hechos ya tipificados en la Ley en relación a la informática, o también, lo que hacen es enmendar (reformar) las Leyes locales, para tratar de enmarcar o tipificar las figuras de los delitos informáticos, en lugar de tratar de crear una ley especial para ello; se cita el ejemplo de Costa Rica, que lo que ha hecho es agregar algunos artículos a su Código Penal; los artículos 196 bis, 217 bis y 229 bis[10], para tratar de enmarcar las actuaciones delictivas relacionadas con los delitos informáticos y que en su texto mencionan lo siguiente:

[10] Ley No. 8148 de fecha 24 de octubre de 2001, San José, Costa Rica

"Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"Artículo 217 bis.-Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"Artículo 229 bis.-Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años

de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

La verdad, es que son pocos los países que se preocupan por tener un cuerpo legal en el cual se enmarquen los delitos informáticos de manera específica y que puedan de alguna manera contrarrestar y proteger a las personas, tanto naturales como jurídicas, contra dichos delitos informáticos. Existen algunos países que sí se preocupan al respecto del tema y han tomado cartas en el asunto, citándose países como España, Perú, Chile, Venezuela y Argentina[11] que sí tienen una Ley local contra tales delitos.

Cuando un país no cuenta con la normativa técnica legal apropiada, busca la forma de poder reglamentar los delitos informáticos, en virtud de ello, se ve en la necesidad de recurrir a la normativa internacional tratando de retomar las partes que puedan resultar aplicables a ese país.

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

El Acuerdo General de Aranceles Aduaneros y Comercio (GATT por sus siglas en ingles), se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los

[11] Obtenido del sitio Web www.delitosinformaticos.com/legislacion/

acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes.

En tal sentido Argentina es parte del acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio, que en su artículo 10 relativo a los programas de ordenador y compilaciones de datos, se establece que este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas, y que las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual.

En el Artículo 61 (GATT) establece que para los casos de falsificación dolosa de marcas de fábrica, comercio o de piratería, nociva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales, además de que, los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias[12]. A continuación se presenta un listado de países que poseen Leyes o Proyectos de Ley específicas para la regulación de los delitos informáticos[13].

[12] Introducción a los Delitos Informáticos, Tipos y Legislación. Publicado en el VI Congreso Latinoamericano en 1998, en Colonia, Uruguay.
[13] Fuente: www.monografias.com; http://lac.derechos.apc.org/ y www.tribunalmmm.gob.mx/biblioteca/biblioteca.htm

Cuadro 4. Regularización Legal de los Delitos Informáticos en diferentes países

PAÍSES	REGULACIÓN LEGAL PARA LOS DELITOS INFORMÁTICOS
Gran Bretaña	Ley de Abusos Informáticos (la Computer Misuse Act), la cual regula los delitos informáticos.
Holanda	Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking, la distribución de virus, entre otros
México	Proyecto de Ley sobre Delitos Informáticos, presentado por Francisco Suárez Tánori, Adalberto Balderrama Fernández. (Año 2000)
Perú	Reforma su Código Penal para incorporar la regulación de los delitos informáticos.
Uruguay	Reforma su Código Penal, para regulara los delitos informáticos
Venezuela	Ley Especial Contra los Delitos Informáticos
Alemania	Este país cuenta con la Ley contra la Criminalidad Económica, dentro de la cual se contemplan los delitos de Espionaje de datos, Estafa informática, Alteración de datos y Sabotaje informático.
Argentina	Anteproyecto de Ley de Delitos Informáticos. Sometido a Consulta Pública por la Secretaria de Comunicaciones por Resolución.
Austria	Este país reformo su Código Penal, para regulara y sancionar los delitos informáticos
Brasil	Este País realizo una modificación a su Código Penal en la que define y tipifica los delitos informáticos.

PAÍSES	REGULACIÓN LEGAL PARA LOS DELITOS INFORMÁTICOS
Chile	Este país cuenta con Ley contra delitos informáticos, y fue el primer país en Latinoamérica en poseer una regulación para este tipo de delitos.
Costa Rica	Este país realizo una reforma a Código Penal en el cual le adiciono unos artículos, para reprimir y sancionar los Delitos Informáticos
España	Ha realizado reformas Código Penal de España, en el cual se incluyó la regulación de los delitos informáticos.
Estados Unidos	Este adoptó en 1994 del Acta Federal de Abuso Computacional
Francia	Este cuenta con la Ley relativa al fraude informático.

1.2.7.2.2 A Nivel de El Salvador

Aunque en El Salvador no existe un cuerpo legal en el cual se contemplen las regulaciones sobre los delitos informáticos, hay algunos artículos del Código Penal, que pueden ser aplicados a algunos delitos informáticos.

Tipo de Delito:

a. Amenazas que atentaren contra la seguridad de la persona y su familia a través de medios electrónicos y/o que pudiesen ser

anónimos. Por ejemplo: amenazas de muerte a profesores universitarios a través de correo electrónico.

Artículo que puede ser aplicado:

Amenazas

Art. 154.- El que amenazare a otro con producirle a él o a su familia, un daño que constituyere delito, en sus personas, libertad, libertad sexual, honor o en su patrimonio, será sancionado con prisión de uno a tres años.

Tipos de Delitos:

a. Intercepción de mensajes electrónicos y otra información. Por ejemplo: a través de la red se pueden interceptar correos electrónicos.
b. Obtención de claves de acceso y/o información electrónica. Por ejemplo: el uso de programas para monitorear computadoras, a través de los cuales se pueden obtener las claves y/o información.

Artículos que pueden ser empleados:

Violación de comunicaciones privadas

Art. 184.- El que con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apoderare de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le este dirigido, o se apodere de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o de cualquier otro tipo de archivos o

registro publico o privado, será sancionado con multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos revelados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de cien a doscientos días multa.

El tercero a quien se revelare el secreto y lo divulgare ha sabiendo de su ilícito origen, será sancionado con multa de treinta a cincuenta días multa.

Violación agravada de comunicaciones

Art. 185.- Si los hechos descritos en el artículo anterior se realizaren por las personas encargadas o responsables de los ficheros, soportes informáticos, archivos o registros, se impondrá, además de la pena de multa, inhabilitación del respectivo cargo o empleo publico de seis meses a dos años.

Captación de comunicaciones.

Art. 186.- El que con el fin de vulnerar la intimidad de otro, interceptare, impidiere o interrumpiere una comunicación telegráfica o telefónica o utilizare instrumentos o artículos técnicos de escucha, transmisión o grabación del sonido, la imagen o de cualquier otra señal de comunicación, será sancionado con prisión de seis meses a un año y multa de cincuenta a cien días multa.

Si difundiere o revelare a terceros los datos reservados que hubieren sido descubiertos, a que se refiere el inciso anterior, la sanción será de prisión de seis meses a un año y multa de cien a ciento cincuenta días multa.

Tipos de Delitos:

a. Robo de hardware;
b. Robo de títulos valores a través de transacciones electrónicas; por ejemplo: el robo de un domino (dirección del www).
c. Robo de capital por medio de infiltración electrónica a cuentas varias, personales, comerciales y estatal. Por ejemplo: alterar una cuenta del banco Cuscatlán a través de su sitio en internet.
d. Estafa electrónica para beneficio propio y terceros. Por ejemplo: los empleados pueden modificar los balances de las cuentas bancarias para su beneficio.

Artículos que pueden ser empleados:

Hurto

Art. 207.- El que con ánimo de lucro para sí o para un tercero, se apoderare de una cosa mueble, total o parcialmente ajena, sustrayéndola de quien la tuviere en su poder, será sancionado con prisión de dos a cinco años, si el valor de la cosa hurtada fuere mayor de quinientos colones.

Hurto Agravado

Art. 208.- La sanción será de cinco a ocho años de prisión, si el hurto fuere cometido con cualquiera de las circunstancias siguientes (solo se listan los numerales aplicables):

2) Usando la llave verdadera que hubiere sido sustraída, hallada o retenida; llave falsa o cualquier otro instrumento que no fuere la llave utilizada por el ofendido. Para los efectos del presente numeral se considerarán llaves las tarjetas magnéticas o perforadas y los mandos o instrumentos de apertura de contacto o a distancia;

6) Por dos o más personas;

10) Sobre objetos que formaren parte de la instalación de un servicio público o cuando se tratare de objetos de valor científico o cultural.

Estafa Agravada (De Los 5 Literales, Solo es aplicable el 5o.)

Art. 216.- El delito de estafa será sancionado con prisión de cinco a ocho años, en los casos siguientes:

5. Cuando se realizare manipulación que interfiera el resultado de un procesamiento o transmisión informática de datos.

Daños Agravados

Inciso Número 2 de Art. 222: Se impondrá prisión de dos a cuatro años:

2) Si el daño se realizare mediante manipulación informática;

Tipos de Delitos:

a. La reproducción de software, con fines de lucro.
b. La reproducción de música y video, con fines de lucro. Por ejemplo: la grabación de música (de archivos mp3 a cinta o CD de audio), para luego ser vendida.
c. Comercialización de sistemas sin autorización previa del programador. Por ejemplo: si una farmacia le vende a otra su programa sin previo aviso al programador.
d. Adjudicarse una obra electrónica. Por ejemplo: adquirir un libro de la red, y luego cambiarle el nombre del autor.
e. Violación de distintivos. Por ejemplo: realizar una venta, utilizando el distintivo de una empresa sin autorización de esta.

Artículos que pueden ser aplicados:

Violación De Derechos De Autor Y Derechos Conexos

Art. 226.- El que reprodujere, plagiare, distribuyere o comunicare públicamente, en todo o en parte, una obra literaria, artística, científica o técnica o su transformación o una interpretación o ejecución artística fijada en cualquier tipo de soporte o fuere comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios, será sancionado con prisión de uno a tres años.

En la misma sanción incurrirá quien no depositare en el Registro de Comercio, importare, exportare o almacenare ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Violación agravada de derechos de autor y de derechos conexos

Art. 227.- Será sancionado con pena de prisión de tres a cinco años quien realizare cualquiera de las conductas descritas en el artículo anterior, concurriendo alguna de las circunstancias siguientes:

1) Usurpando la condición de autor sobre una obra o parte de ella o el nombre de un artista en una interpretación o ejecución;

2) Modificando sustancialmente la integridad de la obra sin autorización del autor; y,

3) Si la cantidad o el valor de la copia ilícita fuere de especial trascendencia económica.

Violación de privilegios de invención

Art. 228.- El que con fines industriales o comerciales y sin consentimiento del titular de una patente o modelo de utilidad, fabricare, importare, poseyere, ofreciere o introdujere en el comercio objetos amparados por tales derechos, será sancionado con prisión de uno a tres años.

La misma sanción se aplicará a quien con los mismos fines utilizare un procedimiento o diseño industrial protegido por un

registro, sin la autorización del titular o sin la licencia respectiva u ofreciere o introdujere en el comercio o utilizare el producto directamente obtenido por el procedimiento registrado.

Violación de distintivos comerciales

Art. 229.- El que con fines industriales o comerciales, y sin el consentimiento del titular, reprodujere, imitare, modificare o de cualquier modo utilizare marca, nombre comercial, expresión, señal de propaganda o cualquier otro distintivo comercial, infringiendo los derechos amparados por la propiedad industrial registrada conforme a la ley, será sancionado con prisión de uno a tres años.

En la misma sanción incurrirá quien, a sabiendas, poseyere para su comercialización o pusiere en el comercio, productos o servicios con distintivos comerciales que, conforme al inciso anterior, constituyere una infracción de los derechos exclusivos del titular de los mismos.

Tipos de Delitos:

a. Poseer documentación de una empresa sin su previo consentimiento y divulgarlo. Por ejemplo: poseer los estados financieros y divulgarlos a la competencia.

Artículos que pueden ser empleados:

Infidelidad comercial

Art. 230.- El que se apoderare de documentos, soporte informático u otros objetos, para descubrir o revelar un secreto evaluable económicamente, perteneciente a una empresa y que implique ventajas económicas, será castigado con prisión de seis meses a dos años.

Revelación O Divulgación De Secreto Industrial

Art. 231.- El que revelare o divulgare la invención objeto de una solicitud de patente o un secreto industrial o comercial, estando legal o contractualmente obligado a guardar reserva, será sancionado con prisión de seis meses a dos años.

Si el secreto se utilizare en provecho propio, la sanción se aumentará hasta en una tercera parte de su máximo.

Cuando el autor fuere funcionario o empleado público y el hecho se ejecutare en razón de sus funciones, se impondrá además la inhabilitación del respectivo cargo o empleo de seis meses a dos años.

Otra Ley que puede ser aplicada es la:

Ley de Fomento y Protección de la Propiedad Intelectual:

Art. 32.- Programa de ordenador, ya sea programa fuente o programa objeto, es la obra literaria constituida por un conjunto de instrucciones expresadas mediante palabras, códigos, planes o en

cualquier otra forma que, al ser incorporadas en un dispositivo de lectura automatizada, es capaz de hacer que un ordenador, o sea, un aparato electrónico o similar capaz de elaborar informaciones, ejecute determinada tarea u obtenga determinado resultado.

Se presume que es productor del programa de ordenador, la persona que aparezca indicada como tal en la obra de la manera acostumbrada, salvo prueba en contrario.

Caso de ejemplo: El Lic. Juan Gómez, ha diseñado su propio sistema de Cuentas por Cobrar en su empresa de alimentos para gatos, "El Gato Feliz", para ello le encargó el desarrollo de su sistema al Técnico en Computación Kevin Martínez, para esto, se firmó un contrato. El Técnico Martínez, le entrega el sistema al Lic. Gómez, según lo establecido en el contrato, y este lo implementa en su empresa. En este caso, se presume que el propietario del sistema es el Lic. Gómez, ya que él es quien lo mandó a elaborar.

Art. 33.- El contrato entre los autores del programa de ordenador y el productor, implica la cesión ilimitada y exclusiva a favor de éste de los derechos patrimoniales reconocidos en la presente ley, así como la autorización para decidir sobre su divulgación y la de ejercer los derechos morales sobre la obra, en la medida que ello sea necesario para la explotación de la misma, salvo pacto en contrario.

Caso de ejemplo: Volviendo al caso del Lic. Gómez, aún cuando esté lo haya diseñado, es el Técnico Martínez quien tiene los derechos para vender, pero con diferentes modificaciones, salvo pacto en contrario.

1.2.8 El Auditor De Sistemas Informáticos Y Los Delitos Informáticos

1.2.8.1 La Ética del Profesional de la Contaduría Publica

Al hablar de la ética del profesional de la contaduría pública, puede analizarse desde dos puntos de vista, el primero, es desde el punto de vista de la ética de un contador; el segundo, es desde el punto de vista de la ética de un auditor.

1.2.8.1.1 Ética del Contador Público

De acuerdo a los requisitos que exige el Código de Comercio tanto para los comerciantes individuales como comerciantes sociales, en su mayoría, están obligados a llevar contabilidad formal; por ende, existe la necesidad de contratar los servicios de un contador público para que se desenvuelva dentro del área de contabilidad de la empresa. Ahora bien, al hablar de la ética del contador, se ve reflejada la transparencia con la cual éste plasma las operaciones en los registros contables, que pueden ser de forma mecanizada o manual.

Algunas empresas de acuerdo a su capacidad económica deciden implantar sistemas informáticos que les ayudan en el procesamiento

de sus operaciones; pero desgraciadamente muchos colegas se prestan a actuaciones ilícitas ya sea por sí o con la complicidad de otras personas, con el fin de obtener algún lucro personal.

Debido a su posición jerárquica dentro de la empresa y a que él mismo es responsable de los controles internos de esta; se vale de dicha situación para poder alterar de alguna forma la información que se presenta mediante los sistemas de información computarizados que utiliza la empresa, debido a que no existen niveles de autorización dentro de los sistemas porque para él no hay restricciones en el uso de los sistemas informáticos.

Es así, como de un delito informático se puede pasar a un fraude financiero, en el cual se está desfalcando el capital de la empresa, reflejando así, cifras irreales dentro de los estados financieros (aquí también puede entrar la contabilidad creativa[14]).

1.2.8.1.2 Ética del Auditor

También puede analizarse desde el punto de vista del auditor, pues también éste se puede prestar al juego de otras personas para poder tener algún beneficio económico, poniéndose de acuerdo con alguna o algunas personas de determinada empresa auditada para ocultar dentro de sus informes, cualquier tipo de irregularidad

[14] Contabilidad creativa: consiste básicamente en el maquillaje de los estados financieros para hacer reflejar una realidad ficticia dentro de la empresa.

que se encuentren falsificando la información o simplemente destruyéndola.

Se cita anteriormente en este mismo documento, el ejemplo de la firma de consultoría Artur Anderson, que era una de las cuatro más importantes del mundo, la cual estaba relacionada con el caso de la corporación Enron; se le descubrió en una investigación que había destruido documentos que mostraban las irregularidades de esta corporación, lo cual ocasionó obviamente una pérdida de credibilidad de esta firma.

CAPITULO II: DISEÑO METODOLÓGICO Y DIAGNOSTICO

2.1 TIPO DE INVESTIGACIÓN

El problema de los delitos informáticos cometidos en los sistemas de información computarizados en las compañías, ha ocurrido principalmente por controles débiles ó inexistentes para la protección de la información. Dicho fenómeno se investigó utilizando el enfoque Hipotético Deductivo, se estudió el surgimiento del problema con el objeto de proponer procedimientos de auditoría que permitiesen detectar, prevenir y corregir, posibles delitos informáticos en los sistemas computarizados de las compañías, partiendo de aspectos generales hasta llegar a conclusiones específicas.

2.2 TIPO DE ESTUDIO

El tipo de estudio que se utilizó en la investigación del problema de los delitos informáticos cometidos en los sistemas de información computarizados, que afectan a las compañías al momento de generar información procesada en dichos sistemas, fue el Explicativo-Analítico y correlacional[15].

Se utilizó este tipo de estudio en la investigación para explicar las causas y efectos que el problema de estudio provoca en las empresas, analizar aquellos elementos y características que se

[15] Guía para realizar investigaciones Sociales, Raúl Rojas Soriano, 40º. Edición, Pág.40.

encuentran involucradas en el fenómeno y principalmente la relación de las variables con el propósito de disminuir el problema objeto de estudio, con la ayuda de procesos aplicados en una auditoría preventiva para los sistemas de información computarizados.

2.3 UNIDADES DE ANÁLISIS

Las unidades de análisis que se consideraron en la investigación están constituidas por las Cajas de Crédito y Bancos de los Trabajadores afiliados al Sistema Fedecrédito de El Salvador, por haberse considerado un área propensa a sufrir delitos informáticos por la manipulación fraudulenta en los sistemas informáticos que utilizan, generando así revelación de estados financieros erróneos y no confiables.

Asimismo se tomaron en cuenta como unidades de análisis aquellos profesionales de la Contaduría Pública que se desempeñan en el área de auditoría en sistemas dentro de dichas instituciones, con el fin de analizar y determinar las dificultades y obstáculos que se presentan al momento de llevar a cabo una auditoría que prevea, controle y detecte delitos informáticos.

2.4 UNIVERSO Y MUESTRA

2.4.1 Universo

El universo de la investigación se constituyó por las 48 Cajas de Crédito y los 7 Bancos de los Trabajadores afiliados al Sistema Fedecrédito los cuales se detallan a continuación:

1. Caja de Crédito de Soyapango
2. Caja de Crédito de Joyeros y Relojeros
3. Caja de Crédito Metropolitana
4. Caja de Crédito de Acajutla
5. Caja de Crédito de Ahuachapán
6. Caja de Crédito de Aguilares
7. Caja de Crédito de Armenia
8. Caja de Crédito de Atiquizaya
9. Caja de Crédito de Berlín
10. Caja de Crédito de Candelaria de la Frontera
11. Caja de Crédito de Ciudad Barrios
12. Caja de Crédito de Quezaltepeque
13. Caja de Crédito de Colón
14. Caja de Crédito de Concepción Bátres
15. Caja de Crédito de Chalatenango
16. Caja de Crédito de Chalchuapa
17. Caja de Crédito del Chilamatal
18. Caja de Crédito de Ilobasco
19. Caja de Crédito de Izalco
20. Caja de Crédito de Jocoro
21. Caja de Crédito de Juayúa

22. Caja de Crédito de Jucuapa
23. Caja de Crédito de La Libertad
24. Caja de Crédito de La Unión
25. Caja de Crédito de Nueva Concepción
26. Caja de Crédito de Olocuilta
27. Caja de Crédito de San Agustín
28. Caja de Crédito de San Alejo
29. Caja de Crédito de San Francisco Gotera
30. Caja de Crédito de San Ignacio
31. Caja de Crédito de San Juan Opico
32. Caja de Crédito de San Martín
33. Caja de Crédito de San Miguel
34. Caja de Crédito de San Pedro Nonualco
35. Caja de Crédito de San Sebastián
36. Caja de crédito de San Vicente
37. Caja de Crédito de Santa Ana
38. Caja de Crédito de Santa Rosa de Lima
39. Caja de Crédito de Santiago de María
40. Caja de Crédito de Santiago Nonualco
41. Caja de Crédito de Sensuntepeque
42. Caja de Crédito de Sonsonate
43. Caja de Crédito de Suchitoto
44. Caja de Crédito de Tenancingo
45. Caja de Crédito de Tonacatepeque
46. Caja de Crédito de Usulután
47. Caja de Crédito de Zacatecoluca

48. Caja de Crédito de Cojutepeque
49. Banco Izalqueño de los Trabajadores
50. Banco de los Trabajadores de San Miguel (BANCOMI)
51. Banco de los Trabajadores de Santa Ana(PRIBANTSA)
52. Banco de los Trabajadores y de la Pequeña y Microempresa (BANTPYM)
53. Banco de Cooperación Financiera de los Trabajadores (BANCOFIT)
54. Banco de Los Trabajadores de Soyapango (BANTSOY)
55. Primer Banco de los Trabajadores

2.4.2 Muestra

Para la selección de la muestra se consideró el método de muestreo aleatorio simple, que consiste en numerar todos los elementos de la población (la cual debe ser finita), para luego seleccionar, por medio de una tabla de números aleatorios, los elementos que formarán parte de la muestra según sea el tamaño de ésta.

Este método se caracteriza porque cada elemento de la población tiene su respectiva probabilidad de pertenecer a la muestra; por esa razón se determina que es el método más adecuado para obtener representatividad en la muestra y para ello se utilizó la siguiente fórmula[16]:

$$n = \frac{Z^2PqN}{(N-1)e^2 + Z^2Pq}$$

[16] Estadística para Administración y Economía, David R. Anderson, Muestreo Aleatorio Simple, Capítulo 21, 8ª Edición.

Donde:

n = Tamaño de la muestra

N = Población

P = Proporción de la población que posee la característica que se desea investigar

q = Complemento de P

Z = Nivel de confianza y exactitud

e = Error máximo admisible

Operando la formula se tiene lo siguiente:

Datos:

n = ?

N = 55

P = 0.95

q = 0.05

Z = 1.96 (área bajo la curva para nivel de confianza de 95%)

e = 0.05

Sustituyendo los datos en la formula tenemos:

$$n = \frac{Z^2PqN}{(N-1)e^2 + Z^2Pq}$$

$$n = \frac{(1.96)^2(0.95)(0.05)(55)}{[(55-1)(0.05)^2]+[(1.96)^2(0.95)(0.05)]}$$

$$n = \frac{10.03618}{0.135+0.182476}$$

$$n = \frac{10.03618}{0.317476}$$

n = 31.6124 **n = 32** (valor del tamaño de la muestra)

De acuerdo con los datos obtenidos de la formula, la muestra se determinó en 32 instituciones.

Para la presente investigación se tomaron para la muestra, las entidades que se encuentran ubicadas en San Salvador y sus alrededores, así como a los profesionales en Contaduría Pública que realizan auditorías a los sistemas y los profesionales encargados de informática de estas entidades.

2.5 INSTRUMENTOS Y TÉCNICAS A UTILIZAR EN LA INVESTIGACIÓN

El instrumento que se utilizó en la recolección de datos para la investigación fue el cuestionario, el cual está compuesto por preguntas cerradas donde se relacionaron las variables con el objeto de obtener la mayor información posible sobre el objeto de estudio.

Las técnicas utilizadas en conjunto con el instrumento en la investigación fueron:

a. El Muestreo: En este se utilizó una fórmula estadística para poblaciones finitas por conocer el número exacto de instituciones afiliadas al Sistema Fedecrédito.

b. Observación: se empleó esta técnica con el fin de adquirir información útil y suficiente sobre el comportamiento de los individuos que conforman la muestra.

c. Referencia Bibliográfica: Se recolectó información bibliográfica disponible sobre la problemática, de diversas fuentes como libros, páginas Web, revistas, boletines, normativa técnica y legal aplicable en El Salvador.

2.6 PROCESAMIENTO DE LA INFORMACIÓN

El procesamiento de la información se hizo mediante el uso de hojas electrónicas de Microsoft Excel, con respecto a la tabulación y análisis de datos y la elaboración de gráficos por medio de dicho Software.

2.7 ANÁLISIS E INTERPRETACIÓN DE DATOS

El análisis e interpretación de los datos se hizo mediante el uso de gráficos de tipo pastel y de barras, que contienen las respuestas obtenidas de las preguntas del cuestionario elaborado

para la recolección de datos, con el fin de obtener valores expresados en forma porcentual a través de un cruce de variables y al final se concluyó sobre los datos analizados, donde se determinó el respectivo diagnóstico de la investigación.

2.8 DIAGNOSTICO DE LA INVESTIGACIÓN

El propósito de este diagnostico es mostrar los resultados obtenidos en la investigación de campo que se realizó, a través de un diagnostico analítico acerca del problema de los delitos informáticos en los sistemas de información computarizados de las empresas y como pueden llegarse a detectar, prevenir y si fuese posible corregirlos.

Para tal efecto, los resultados obtenidos a través de las encuestas servirán como un parámetro de medición, ya que estas se han agrupado en aéreas especificas, las cuales son:

A. Aspectos Generales de la Empresa
B. Aspectos Relacionados al Sistema de Información Computarizado
C. Respaldo de la Información Generada por el Sistema
D. Controles Generales del Sistema de Información
E. Conocimiento sobre Delitos Informáticos y Procedimientos de Auditoria de Sistemas

2.8.1 Aspectos generales de la empresa

Aquí se evalúan criterios como la existencia de un Departamento de Informática y un Departamento de Auditoria en la empresa; el nivel académico que tiene el personal de dichos departamentos y la capacitación que estos reciben dentro de esta.

Según el cuadro siguiente, se observó que las cajas y los bancos del sistema fedecrédito no cuentan con un departamento de auditoría especializado en el área de sistemas, sino que solo en el área legal y contable (auditoría interna).

Cuadro No. 1: Aspectos Generales de la Empresa

Relación A Encuesta	Criterios De Evaluación	Frecuencia Relativa
Pregunta 1	Existencia de Departamento de: • Informática • Auditoria	 100% 37.14%
Pregunta 2	Nivel Académico Promedio: • Universidad • Técnico • Otros Niveles • No Contestó	 48.57% 2.86% 5.71% 42.86%
Pregunta 3	Capacitación del Personal: • Solo depto. de Informática • Solo depto. De Auditoria • Ambos • Ninguno • No contestó	 22.86& 5.71% 42.86% 22.86% 5.71%

En este apartado se pudo observar que en el 100% de las instituciones encuestadas existe un Departamento de Informática y que solamente el 37.14% posee un Departamento de Auditoria, el restante 62.86% no lo tiene (Pregunta 1).

Además, al evaluar el nivel académico promedio de las personas que conforman ambos departamentos, se verificó que la mayoría cursa o ha cursado estudios universitarios (48.57% de la muestra) aunque el 42.86% prefirió reservarse su respuesta a esta pregunta (Pregunta 2).

También, se pudo observar que en la mayoría de instituciones (42.86%) se capacita al personal de ambos departamentos, pero que el 22.86% no capacita a ninguno (Pregunta 3 - Anexo No. 2).

2.8.2 Aspectos relacionados al sistema de información computarizado

Cuadro No. 2: Aspectos Relacionados al Sistema de Información

Relación A Encuesta	Criterios De Evaluación	Frecuencia Relativa
Pregunta 4	Adquisición del Sistema de Información: • Compra de Sistema estándar • Elaboración de sistema a la medida • Donación • Arrendamiento • otros	 45.72% 37.14% 0.00% 17.14% 0.00%

Pregunta 5	Posee Licencia del Sistema: • Si • No	 97.14% 2.86%
Pregunta 6	Estructura funcional del Sistema: • Módulos • Aplicaciones Independientes • Menús y Submenús • Otros	 94.29% 0.00% 5.71% 0.00%
Pregunta 7	Posee Programas Fuente del Sistema: • Si • No	 48.57% 51.43%
Pregunta 8	Uso de Internet para traslado de información: • Si • No	 48.57% 51.43%
Pregunta 9	Ha presentado fallas el sistema: • Si • No • No contestó Áreas de fallas del Sistema: • Entrada de datos • Procesamiento de datos • Salida de datos Tipos de Fallas: • Los datos se duplican • La información no concuerda con los datos • Los datos o la información se pierde • La información se cruza con otra • Procesa mal los datos	 74.29% 17.14% 8.57% 46.15% 53.85% 42.31% 11.54% 26.92% 11.54% 11.54% 23.08%

	• La información que sale del sistema está alterada • No ingresa bien los datos • Otros • No contestó	3.85% 11.54% 3.85% 11.54%

Las cajas y los bancos de los trabajadores cuentan con un sistema que fue diseñado de acuerdo a la activadad que realizan, este sistema fue adquirido por las instituciones de la siguiente manera:

El 46% de ellas adquirió un sistema estándar, mientras que 37% de la muestra desarrollaron un sistema a la medida y un 17% de ellos lo obtuvieron por medio de arrendamiento (Pregunta 4 – Anexo No. 2), lo que indica que no todas tienen el mismo sistema, ni realizan las mismas operaciones.

Esto le dificulta a la institución en el momento en que se presentan problemas en el sistema, ya que se ve en la tarea de llamar al proveedor, y esperar que este le programe una visita para atender el requerimiento.

En la mayoría de las instituciones los sistemas que utilizan se encuentran compuestos por módulos integrados (94.29%) y además, el 97.14% posee la licencia respectiva del sistema (Pregunta 5 y 6 – Anexo No. 2).

Además ninguna de ellas posee los programas fuente (como se puede observar en el gráfico de la Pregunta 7 contenida en el Anexo No. 2) para realizar modificaciones al sistema en caso de errores o en el caso de que se realizara una nueva actividad.

Del total de la muestra, el 51% contestó que el sistema que utilizan no necesita el uso de Internet para el traslado de la información entre los usuarios, mientras que el 49% contestó que su sistema si traslada la información por medio de Internet.

Por lo que se determina que el 49% que utiliza Internet tiene mayor riesgo en cuanto a la ocurrencia de delitos informáticos, o manipulación de la información (Pregunta 8 – Anexo No. 2).

Se verificó según las respuestas obtenidas en las encuestas que el 74.29% de las instituciones presenta fallas en su sistema de información; de esta cantidad, el 46.15% presenta fallas en la entrada de datos, 53.85% en el procesamiento y 42.31% en la salida de datos.

Dentro de las fallas más comunes están: la duplicidad de datos, la pérdida de la información, cruce de datos, alteración de la información que sale del sistema; sobresaliendo entre estas, el mal procesamiento de los datos (23.08%) y la falta de concordancia entre la información y los datos (26.92%) (Pregunta 9 – Anexo No. 2).

Con esto se puede observar que los sistemas son de fácil manipulación y que se corre el riesgo de pérdida de la información, acreditándose de esta forma a ser victima de delitos informáticos.

2.8.3 Respaldo de la Información Generada por el Sistema

Cuadro No. 3: Respaldo de la Información del Sistema

Relación A Encuesta	Criterios De Evaluación	Frecuencia Relativa
Pregunta 10	Hacer respaldo de la Información: • Si • No	 100.00% 0.00%
Pregunta 11	Tiempo en que se hacen los Respaldos: • Diariamente • Semanalmente • Mensualmente • Anualmente • Otros	 42.86% 14.29% 40.00% 8.57% 5.71%
Pregunta 12	Medios de Almacenamiento de Respaldos: • Disquete • CD • DVD • Memorias USB • Microfilm • Otros	 0.00% 34.29% 31.43% 0.00% 8.57% 25.71%

En la encuesta realizada se pudo observar que el 100% de las instituciones realizan respaldo de la información que se procesa en el sistema, en diferentes lapsos de tiempo, notándose que la mayoría lo hace diaria y mensualmente (42.86% y 40% respectivamente) y en diferentes medios de almacenamiento especialmente en CD y DVD (como se muestra en la pregunta 10, 11 y 12- Anexo No. 2), se observar que la información es respaldada con los errores que genera el sistema, por lo que este tipo de información se vuelve no confiable.

2.8.4 Controles Generales del Sistema de Información.

Cuadro No. 4 Controles Generales del Sistema

Relación A Encuesta	Criterios De Evaluación	Frecuencia Relativa
Pregunta 13	Controles para el resguardo de información • Hacer Backups • Crear cuentas de usuario • Hacer varias copias de los respaldos • Restringir el acceso al sistema • No contestó	 100.00% 91.43% 28.57% 45.71% 2.86%
Pregunta 14	Creación de Cuentas de Usuario: • Si • No	 91.43% 8.57%

Pregunta 15	Permiso del sistema para el ingreso de dos ó más personas a una misma cuenta de usuario: • Si • No	 22.86% 77.14%
Pregunta 16	Cambio de contraseña periódicamente: • Si • No Tiempo en que se cambia la contraseña: • Semestral • Mensual • Quincenal • Semanal • Cada 45 días • Bimensual • No Contestó	 48.57% 51.43% 5.88% 23.53% 5.88% 5.88% 11.76% 5.88% 41.19%
Pregunta 17	Existencia de distribución de funciones del sistema de acuerdo al perfil de cada usuario: • Si • No • No contestó	 68.57% 25.71% 5.72%
Pregunta 18	Se hacen revisiones al sistema: • Si • No Frecuencia de tiempo en el que se realizan: • Semanalmente • Mensualmente • Trimestralmente	 62.86% 37.14% 18.18% 36.16% 18.18% 9.09%

	• Semestralmente • Anualmente • Otros • No contestó	4.55% 4.55% 9.09%
Pregunta 19	Hacen pruebas al sistema para verificar funcionamiento: • Si • No	 60.00% 40.00%
Pregunta 20	Realizan pruebas de validación de datos e información generada por el sistema: • Datos de entrada • Procesamiento de datos • Salida de información • Ninguno	 28.57% 20.00% 22.86% 28.57%

Se puede observar que dentro de las medidas de seguridad que poseen estas instituciones, está la realización de varios respaldos que son resguardados en diferentes lugares, así como la creación de cuentas de usuario (91.43% de las instituciones crea cuentas de usuario), de las cuales las contraseñas son cambiadas cada cierto tiempo, mayormente de forma mensual (23.53%) (Pregunta 16 – Anexo No. 2).

Este tipo de controles conlleva ciertos riesgos debido a que en algunos casos el sistema permite que estén trabajando dos o más usuarios con la misma clave, al sistema no se le realizan revisiones periódicas, además un 60% realizan pruebas al sistema para ver si los comandos generan la información para lo que fueron programados.

2.8.5 Conocimiento sobre Delitos Informáticos y Procedimientos de Auditoria de Sistemas

Cuadro No. 5: Conocimiento sobre Delitos Informáticos

Relación A Encuesta	Criterios De Evaluación	Frecuencia Relativa
Pregunta 21	Conocimiento sobre Delitos Informáticos: • Si • No	 100.00% 0.00%
Pregunta 22	Ha sido victima la empresa de algún delito informático: • Si • No • No contestó Tipos de delitos informáticos: • Manipulación del sistema • Uso no autorizado o indebido del sistema • Destrucción de la información del sistema • Implantación de virus en el sistema • Otros	 65.71% 31.43% 2.86% 27.27% 27.27% 9.09% 27.27% 9.10%
Pregunta 23	Ha tomado la empresa alguna acción para evitar ser nuevamente victima de algún delito informático: • Si • No • No contestó Acciones tomadas en contra de los delitos informáticos: • Mejorar la seguridad del sistema	 40.00% 34.29% 25.71% 42.86%

	• Implantar nuevos controles de seguridad • Restringir el acceso al sistema • Otro	28.57% 50.00% 7.14%
Pregunta 24	Ejecución de plan de auditoria relacionado al sistema de información: • Si • No • No contestó Frecuencia de tiempo de ejecución del plan de auditoria: • Mensual • Trimestral • Semestral • Semanal • Otro • No contestó	 37.14% 57.14% 5.72% 7.70% 15.38% 15.38% 15.38% 15.38% 30.78%
Pregunta 25	Posee el sistema registro de las personas que ingresan y lo que realizan en este: • Si • No • No contestó	 51.43% 45.71% 2.86%
Pregunta 26	Medidas de auditoria para evitar los delitos informáticos: • Realizar pruebas de validación de datos • Realizar pruebas de integridad de la información del sistema • Otras • Ninguna	 45.71% 20.00% 8.57% 25.72%

Dentro de la muestra tomada, el 100% manifestó saber qué eran los delitos informáticos (Pregunta 21- Anexo No. 2). Pero el 31.43% de muestra afirmó no ser victimas de delitos informáticos, mientras que el 65.71% sí confirmó haber sido victima de diferentes delitos (Pregunta 22- Anexo No. 2), las personas que han sido victimas de ellos han procurado mejorar sus controles (40% de las instituciones que sufrieron algún delito), pero las personas que no han sufrido delitos informáticos se mantienen sin tomar la importancia pertinente a este tipo de hechos, que pueden ser muy dañinos para la institución.

Además, el 57.14% de las instituciones no ejecuta ningún plan de auditoria en relación al sistema de información, el 37.14% si lo hace; y con respecto de las medidas tomadas para la protección del sistema, el 45.71% dijo que si realiza pruebas de validación de datos y el 20% de integridad de los datos (Preguntas 21 a la 26 – Anexo No. 2). Debido a esto se debe considerar que las instituciones no tienen auditores preparados en el área de sistemas que puedan velar para que este tipo de hechos no ocurran.

CAPITULO III: PROCEDIMIENTOS DE AUDITORIA PARA LA DETECCIÓN, PREVENCIÓN Y CORRECCIÓN DE DELITOS INFORMÁTICOS.

3.1 OBJETIVOS E IMPORTANCIA DE LA PROPUESTA

3.1.1 Objetivos.

3.1.1.1 Objetivo General

Proponer procedimientos de auditoria que ayuden a la detección, prevención y si fuera posible la corrección de los delitos informáticos dentro de los sistemas informáticos utilizados por las instituciones afiliadas al Sistema Fedecrédito.

3.1.1.2 Objetivos Específicos

- ✓ Analizar las diferentes características que ayuden a identificar cuando se puede presentar un delito informático.

- ✓ Sugerir procedimientos detectivos, preventivos y correctivos que sean aplicables a los sistemas de información.

- ✓ Identificar los diferentes puntos de debilidad que presentan los sistemas informáticos de la empresa.

3.1.2 Importancia

Considerando los avances de la tecnología dentro las diferentes áreas laborales, y de los diferentes grupos de empresas que se ven obligadas a manejar todas sus operaciones en sistemas de información computarizados que les permitan manejar el volumen de transacciones que cada una de estas realizan, exponiendo así su información a posibles manipulaciones, pérdida, sabotaje, robo, hurto, y una diversa gama de delitos informáticos.

Es por ello que las empresas deben estar preparadas para contrarrestar o minimizar lo mayormente posible este tipo de hechos con planes de auditoria de sistemas que contengan procedimientos que se apliquen de forma recurrente, revisándolos cada cierto tiempo para evitar el desfase de estos. Por tanto, es necesario contar con una estructura de procedimientos de auditoria de sistemas que sirvan como una base para poder auditar los sistemas informáticos y con ello lograr la detección, prevención y corrección de delitos informáticos.

Por ende, y en vista de que la mayoría de empresas en el país no cuenta con un departamento de auditoria de sistemas que supervise el buen funcionamiento y fidelidad de la información de los sistemas informáticos, se considera la propuesta de procedimientos de auditoria que se apliquen a los sistemas de información computarizados de las empresas.

3.2 ÁREAS DE APLICACIÓN DE PROCEDIMIENTOS DE AUDITORIA

Área No. 1 PROCESAMIENTO ELECTRÓNICO DE DATOS

En el procesamiento electrónico de datos es importante considerar tres facetas para lo que es una auditoria a los sistemas de información dentro de este como lo son la entrada de los datos, procesamiento y la salida.

A. Entrada de Datos

El proceso de entrada de datos en el sistema de información es muy importante, debido a que en esta fase se puede realizar el delito de manipulación de los datos, este es un tipo de fraude informático conocido también como sustracción de datos, es uno de los delitos más comunes ya que es fácil cometerlo y muy difícil de descubrirlo, por lo que las instituciones deben estar evaluando constantemente el tipo de información a la que tienen acceso sus empleados:

1. Procedimientos Detectivos:

1. Pasar un cuestionario de control interno y ver las diferentes áreas de seguridad con las que cuenta la institución en cuanto al procesamiento de datos para su entrada al sistema.

2. Solicitar permiso para ingresar al sistema y realizar actividades de las autorizadas, verificando que los registros realizados sean acordes a la documentación física que se tiene.

3. Verificar que la persona que ingrese la información al sistema sea la persona que está autorizada para realizar dicha operación.

4. Verificar los tipos de usuarios que el sistema tiene y los niveles de acceso que le permite a cada uno de los usuarios.

5. Realizar comparativos de información de un mes ya procesado con el que se encuentra en proceso, para determinar si se han realizado alteraciones en esta información.

6. Verificar si el sistema tiene una opción para ingresar datos sin necesidad de abrir una ficha de información ya existente que permita sobrescribir sobre la información ingresada previamente para ver si ésta no ha sido alterada.

2. Procedimientos Preventivos:

1. Verificar la existencia de controles que permitan tener la certeza de que la información introducida al sistema sea la correcta.

2. Indagar sobre la existencia de manuales de funciones y puestos en el cual se definan las funciones de cada uno de los puestos con lo que cuenta la institución y los permisos de acceso que estos tengan para el ingreso de la información en el sistema.

3. Evidenciar si el sistema muestra algún mensaje de error cuando se introducen datos erróneos al sistema de información para evitar la manipulación de estos y que se procesen mostrando información inexacta.

4. Verificar si las personas encargadas de ingresar los datos al sistema de información lo hacen de la forma establecida en los manuales de procedimientos de la institución y según el manual del sistema para lograr que la información sea introducida de forma integra.

5. La información introducida debe ser revisada y autorizada previamente para evitar la introducción de datos erróneos al sistema o datos que pueden ser ocupados para realizar malversación de la información.

3. Procedimientos Correctivos

1. Si se verifica que cuando se realiza la introducción de los datos hay que realizar la apertura de una cuenta ya creada para crear una nueva, debe de hablarse con el proveedor para que le realice cambios al sistema, para la introducción de datos.

2. Verificar los flujos de los procesos que deben seguirse antes de introducir los datos al sistema, para evitar la manipulación, hurto o extravío de la información.

3. Sugerir a la gerencia la implantación de filtros dentro del sistema de información concerniente a la entrada de los datos.

4. Verificar a través de la bitácora de registro de eventos donde y quien introdujo datos erróneos al sistema para ver especialmente el efecto que esto ocasiona en la información que genera el sistema.

B. Procesamiento de Datos:

Esta fase es muy susceptible para la realización de delitos informáticos, es necesario que se establezcan los controles adecuados para evitar que los datos se procesen de forma inadecuada produciendo así datos equívocos o inexactos que puedan a su vez generar información incorrecta.

1. Procedimientos Detectivos

1. Solicitar diagrama Entidad/Relación del sistema (en caso de que haya sido elaborado por la empresa), en el cual se muestre la relación de las tablas en las que el sistema procesa la información que es introducida en este para verificar que dicha relación no haya sido alterada sin autorización de la gerencia.

2. Solicitar la asignación de una cuenta de usuario para ingresar al sistema y acceder a la información contenida en este y

cambiar datos que ya hayan sido procesados para ver si el sistema permite manipularlos después de procesados.

3. Verificar si las instrucciones de programación del sistema pueden ser modificadas por cualquier usuario para lograr un propósito determinado (beneficio o perjuicio).

4. Realizar pruebas del funcionamiento del sistema de información, en cuanto a cálculos que realiza el sistema desarrollándolos de forma manual para ver si se obtiene el mismo resultado para ver si hay así alteración o no alteración de las funciones del sistema.

5. Solicitar a la administración de la institución los controles que ésta posee para el procesamiento de la información que es introducida al sistema de información para verificar que son adecuados.

2. Procedimientos Preventivos

1. Realizar periódicamente pruebas de validación de la información para verificar que el sistema realiza los cálculos correctamente y no se están dando problemas en el procesamiento de estos para evitar la manipulación del sistema.

2. Realizar muestreos de clientes y solicitarles la documentación original que se les dio, para realizar un cruce de la

información procesada en el sistema con la documentación entregada al cliente para verificar que sea la misma que está contenida en el sistema de la institución.

3. Entrar al sistema y realizar un usuario y procesar una cantidad específica de datos, revisando que el sistema lo realice conforme a los parámetros establecidos previamente según la programación, dichos parámetros deben estar de acuerdo a las políticas de institución para el procesamiento de la información.

3. Procedimientos Correctivos

1. Si se determina que el sistema no realiza adecuadamente el procesamiento de la información debe de llamarse al proveedor del sistema para verifique si a sido modificada alguna forma de operar del sistema, y pedirle que se limiten los accesos a este en los que se refiere a programación, solo al personal determinado por la empresa.

2. En caso de que la información proporcionada por el cliente no concuerde con la contenida en el sistema, debe realizarse una investigación de la persona que procesó la información, e indagar si es primera vez que lo realiza o ya tiene experiencia en este proceso; de no ser así, investigar si es alguien ajeno a la empresa quien entró al sistema usando una cuenta de usuario hurtada y tratar de indagar sobre las razones por las

cuales realizó ese tipo de operaciones y los daños que esto ocasionó al sistema.

C. Salida de Información

Son varias las formas en las que se puede sacar información de un sistema, a través de discos, memorias usb, impresa o simplemente mostrándola en pantalla; por ende, es necesario tener controles sobre la salida de información para evitar sobre todo que sea sustraída o destruida.

1. Procedimientos Detectivos

1. Verificar si el sistema cuenta con un registro donde se evidencie la salida de datos así como el usuario que tuvo acceso a dicha información, hora, fecha y tipo de información que sale del sistema para ver que solo las personas autorizadas puedan sacar información.

2. Verificar si la empresa cuenta con una política, que regule a los empleados a mantener la privacidad de los datos contenidos en el sistema de información de la institución.

3. Solicitar una lista de las personas y de los lugares a los que se puede enviar la información y cada cuanto tiempo se realiza esta actividad y verificar que solo ha los lugares detallados se halla enviado dicha información.

4. Determinar cuales son los medios permitidos por la gerencia para la salida de información y comprobar que los usuarios involucrados con esta función los usen de forma correcta y no ocupen otros medios extraíbles no autorizados.

2. Procedimientos preventivos

1. Verificar que existan controles en cuanto a la información que es extraída del sistema para efecto de llevar un control de las personas que lo hacen y para que va a ser ocupada esta información para evitar que se sustraiga información de la empresa.

2. Sugerir que se limite el uso de medios de almacenamiento extraíbles a aquellos usuarios que no están involucrados en la salida de información del sistema para evitar que personas ajenas a la empresa tengan acceso a esta información y la hurten.

3. Verificar la existencia de contraseñas especiales asignadas a usuarios específicos para que con esta efectúen la salida de información del sistema evitando que cualquier persona tenga acceso y saque información del sistema.

4. Indagar si existen políticas de la administración para la salida de información y el uso que se le dará a esta fuera del sistema de información.

Área No. 2 SOFTWARE

Los sistemas de información de las empresas, comúnmente conocidos como software, son vulnerables a los delitos informáticos; por ende, es necesario contar con procedimientos que ayuden a detectar, prevenir y de ser posible corregir dichos delitos; aunque corregirlos es poco probable, debido a que cuando se da un delito informático, los daños ocasionados a los sistemas de información son casi irreversibles. Por eso, es necesario tomar en cuenta ciertos aspectos dentro de todo sistema de información, aplicando procedimientos detectivos, preventivos y correctivos para cada uno de ellos; dichos aspectos son los siguientes:

A. Uso del software,
B. Licenciamiento del software,
C. Protección del software, y
D. Respaldo y Restauración del software

A. Uso del software

Es muy importante tomar en cuenta la capacitación que reciben los usuarios del sistema de información con respecto del buen uso de este. En muchas ocasiones se han causado daños a los sistemas y pérdidas de información a causa del mal manejo que se da a los sistemas, no necesariamente constituyendo así un delito informático.

Además de la capacitación de los usuarios, también se hace necesario y casi imprescindible contar con un departamento de informática y un departamento de auditoria en sistemas para hacer las revisiones pertinentes dentro del sistema de información, verificando que todas las operaciones ejecutadas dentro del sistema de información, estén acordes a las establecidas para cada usuario, previendo que no existan operaciones ajenas a la institución.

1. Procedimientos Detectivos

1. Determinar si las funciones que los usuarios realizan dentro del sistema de información son acordes a las asignadas para el cargo que desempeñan con el fin de evitar que dos o más usuarios realicen las mismas actividades duplicando y/o alterando la información.

2. Indagar sobre la existencia de cuentas de usuarios (nombre y contraseña) para ver la forma en la cual los usuarios ingresan y salen del sistema de información con el objeto de evitar que personal ajeno a la empresa tenga acceso al sistema de información.

3. Revisar si el sistema genera algún tipo de registro de las operaciones que cada usuario realiza con el fin de evidenciar posibles irregularidades en cuanto al uso del sistema (que no

haya fuga de información confidencial, manipulación o uso mal intencionado del sistema).

4. Revisar la estructura con la que fue diseñado el sistema de información (módulos, aplicaciones independientes, otros) y la forma en que procesa la información (en línea o integrado, por lotes, etc.) evidenciando la forma correcta en que trabaja el sistema con el fin de detectar si ha habido manipulación en cuanto a sus funciones.

5. Verificar que exista una separación especifica de funciones para cada usuario dentro del sistema de información (identificación de perfiles de usuarios) para individualizar responsabilidades en caso de encontrarse hallazgos sobre la realización de un delito informático dentro del sistema.

2. Procedimientos Preventivos

1. Verificar la existencia de manuales de procedimientos para el uso del sistema de información computarizado, para evitar el uso indebido o mal intencionado del mismo.

2. Indagar sobre la existencia de manuales de puestos donde se detallen las actividades a realizar para cada usuario dentro del sistema de información con lo cual se puedan identificar claramente los perfiles de cada usuario.

3. Indagar sobre la existencia de un plan de capacitación en el cual se involucren a todos los usuarios del sistema de información para evitar fallas por el mal uso del sistema.

4. Verificar la existencia de políticas que regulen el uso, no solo del sistema de información, sino también de todo el sistema operativo, con el fin de evitar que se instalen programas ajenos a las actividades de la empresa que pudiesen contener o ser en si un virus o un spyware.

5. Verificar la existencia de niveles de autorización en el uso del sistema de información para evitar que los usuarios tengan acceso y/o realicen operaciones para las cuales no están autorizados.

6. Determinar si la empresa tiene la política de cambiar periódicamente la contraseña para cada usuario para evitar el ingreso no autorizado al sistema de personas ajenas a esta.

7. Verificar si los usuarios cuentan con su propia estación de trabajo (computadora en la cual solo trabaje un usuario a la vez con su respectiva cuenta de usuario) para evitar accesos no autorizados, manipulación de las funciones del sistema u otros.

8. Verificar si existen políticas de control por parte de la administración de las visitas que los usuarios reciben dentro de

sus estaciones de trabajo para evitar que personas ajenas a la empresa hagan uso del sistema de información.

9. Identificar si la administración monitorea a los usuarios del sistema de información para verificar que las actividades que realizan estén acordes a las asignadas al cargo que desempeña.

10. Revisar periódicamente la bitácora de registro de eventos para determinar si hay posibles irregularidades en cuanto a las actividades realizadas por los usuarios.

3. Procedimientos Correctivos

1. Realizar, previa autorización de la gerencia, pruebas de fallas en el uso del sistema, con el fin de verificar si existen puntos vulnerables del sistema de información para corregirlos haciendo las modificaciones necesarias al sistema siempre y cuando lo haya autorizado la administración.

2. Sugerir una limitación rigorista en cuanto al acceso al sistema de información estableciendo una jerarquía de niveles de autorización dentro de la empresa.

3. Determinar si existen planes de contingencia que contengan las medidas adecuadas para corregir errores ocasionados por el mal uso o uso mal intencionado del sistema de información.

4. Verificar si se han instalado programas auxiliares o complementarios que ayuden a controlar la seguridad del sistema de información computarizado y del sistema operativo en general (antivirus, antispyware, otros).

B. Licenciamiento del software

En el medio actual, la piratería es un delito muy frecuente, puesto que se reproducen sin la licencia respectiva películas, música y, por supuesto, no son la excepción los programas computarizados. Es por ello, que se vuelve necesario garantizar el uso y tenencia legítima del software que la empresa está usando para el registro de sus operaciones.

1. Procedimientos Detectivos

1. Determinar la forma de adquisición del sistema de información computarizado (adquisición, donación, diseñado a la medida, etc.) para ver la procedencia del mismo.

2. Verificar la legitimidad de la licencia del software que la empresa está utilizando a través del soporte documental (acuerdo de licencia del proveedor y documentos donde se muestre la adquisición legal del sistema informático o donde se reflejen el diseño y desarrollo si fue elaborado la medida) para determinar si la copia del sistema es legal o ilegal.

3. Cotejar el costo de elaboración o de adquisición del sistema de información computarizado de la empresa con otros similares en

el mercado para determinar si es razonable dicho costo, un costo por debajo del estándar en el mercado puede dar lugar a pensar en la posibilidad de que el sistema puede ser una copia pirata.

4. Indagar respecto de las condiciones del proveedor del software establecidas en el contrato: número de máquinas para las que está autorizada la licencia, restricciones de uso y soporte.

2. Procedimientos Preventivos

1. Verificar que el distribuidor del software esté autorizado por el diseñador o productor de este para su distribución con el fin de evitar la adquisición de un software pirateado o sin licencia.

2. Verificar al momento de la adquisición del software que el proveedor cumpla con las condiciones de venta, es decir, que entregue todo lo que ofertó en el momento de ofrecer el sistema, incluyendo la licencia y manuales en especial.

3. Indagar sobre el tipo de licencia que ofrece el proveedor al momento de adquirir el software para ver las restricciones y beneficios que se incluyen y las obligaciones que las partes contraen en la adquisición, para determinar especialmente si se autoriza al comprador la realización de cambios en el sistema.

4. Cuando el software haya sido diseñado a la medida, hay que verificar que esté debidamente registrado en el Centro Nacional de Registros (CNR) para evitar que se copie y/o distribuya sin la autorización de la empresa, además hay que determinar si la empresa cuenta con los programas fuente del software para modificarlo si es necesario.

3. Procedimientos Correctivos

1. Determinar si la administración cuenta con políticas para la adquisición de software, observando especialmente que el software a adquirir esté protegido por derechos de autor y cuente con su respectiva licencia.

C. Protección del software

Deben considerarse las medidas de seguridad que la empresa ha establecido para la protección de su sistema de información, evitando que pueda ser reproducido o modificado sin permiso; además, el sistema debe estar diseñado con medidas que permitan asegurar tanto el mismo sistema como la información contenida en el, debiendo proteger especialmente los programas fuente y las bases de datos.

También debe tenerse en cuenta el uso de otros programas de protección como los antivirus y los antispyware, que complementen la seguridad del sistema de información.

1. Procedimientos Detectivos

1. Identificar los niveles de acceso al sistema, observando especialmente el personal que tienen acceso a las bases de datos y los programas fuente para evitar daños en el sistema o pérdida de la información contenida en este.

2. Determinar si el sistema mismo brinda funciones de protección para evitar cualquier ingreso no autorizado a este.
3. Indagar si existen políticas de la administración en cuanto a la protección del sistema de información computarizado.

4. Realizar una inspección del sistema en cada una de las aéreas de trabajo o si son varias estaciones, selectivamente para verificar el tipo de acceso al sistema, si es total o parcial a las partes o módulos del sistema.

5. Verificar si el sistema permite el ingreso de dos o más personas con una misma cuenta de usuario para evidenciar que una persona no tenga acceso a la parte del sistema en la que trabaja otra.

6. Determinar si es posible ingresar al sistema sin el uso de una cuenta de usuario especifica para ver la seguridad o vulnerabilidad del sistema.

2. Procedimientos Preventivos

1. Verificar las limitaciones que los usuarios tienen dentro del sistema de información en cuanto al acceso para evidenciar una jerarquización de niveles de seguridad.

2. Identificar la existencia de programas (Antivirus, Antispyware, etc.) que ayuden a mantener la seguridad de los computadores donde se encuentra instalado el sistema de información de la empresa.

3. Verificar si la administración ha implementado políticas de seguridad en cuanto a la protección del sistema de información, para controlar las acciones de los usuarios y evitar que alguien haga daño al sistema o modifique algo para beneficiarse a si mismo o a otra persona.

4. Controlar el acceso a internet dentro de la empresa para evitar que alguien ajeno pueda dañar el sistema a través de este medio (hackers o crackers).

3. Procedimientos Correctivos

1. Verificar si la gerencia ha realizado alguna modificación respecto del acceso al sistema para crear tanto cuentas de usuario como una jerarquía de acceso total o parcial a las partes o módulos del sistema.

2. Determinar si la empresa cuenta con una red interna para el traslado de información en lugar o sustitución del uso de internet.

3. Indagar si existe una restricción del acceso a internet para limitarlo solo a la alta gerencia y complementarlo con el uso de programas complementarios como los antivirus, antispyware, firewall u otros.

Área No. 3 HARDWARE

En el área de los sistemas es necesario que las entidades se aseguren no solo del sistema en si, sino también del hardware y el entorno físico, ya que puede resultar objeto de algún *Sabotaje informático* (el término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema).

Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

Es por ello que resulta de suma importancia que las entidades se preparen previniendo, detectando y corrigiendo este tipo de hechos.

A. Implementación de la seguridad Física y Lógica

La seguridad física y lógica del equipo y el sistema debe de implementarse en cualquier entidad con el objeto de salvaguardar el hardware y el sistema de información que posee.

Por lo tanto al momento de realizar una auditoria a los sistemas de información es importante que se tome en consideración la seguridad del hardware que posee el sistema en si y darnos cuenta si se poseen controles sobre ellos.

1. Procedimientos Detectivos

1. Indagar sobre la existencia de controles orientados a la seguridad del hardware, si es necesario intentar accesar a áreas restringidas: del servidor computadoras usuarias del sistema; y determinar si se cumple la restricción con personal no autorizado.

2. Observar si se les da el uso adecuado a los equipos en las horas laborales y fueras de estas por el personal que trabaja de forma extraordinaria y si estos realizan el trabajo asignado según su cargo después de las horas ordinarias, verificando las entradas y las funciones realizadas dentro del sistemas en dichas horas.

3. Verificar si el personal tiene acceso a disponer de los equipos (portátiles, y de escritorio) para extraerlos de la institución y si se hace con autorización de que o quien; y si es así determinar el riesgo inherente, de control, y de detección que puede existir._ para determinar algún posible delito.

4. Al realizar un estudio completo implementando la observación, indagación e investigación sobre la seguridad que poseen los equipos en la entidad, determinar si existe la posibilidad de que los equipos se estén utilizando como instrumento para realizar algún delito informático.

5. Si se encuentra la posibilidad que se esté realizando algún tipo de delito, es necesario verificar que existan controles que aseguren de forma satisfactoria al hardware de la empresa (y de no existir controles, recomendarlos a la gerencia de acuerdo a las necesidades de ésta).

2. Procedimientos Preventivos

1. Investigar si existen personas responsables de la seguridad física y lógica de los activos dentro de la entidad.

2. Conocer formalmente a las personas responsables de los datos y del sistema de información en cuanto al acceso a este y al equipo; y conocer el perfil que poseen; para determinar el cargo y responsabilidades que tienen.

3. Determinar si las personas responsables del hardware y software, realmente realizan las funciones que se le han asignado; y verificar que no se les permita que dichas funciones las realice también personas ajenas al área.

4. Conocer si existen algún plan de seguridad; si no se posee recomendar el diseño un plan a la medida de la institución.

5. Verificar que haya políticas y/o procedimientos para el uso del equipo y del software; con el fin de determinar si el personal hace buen uso del equipo.

3. Procedimientos Correctivos

1. Si se ha detectado alguna probabilidad de que se esté cometiendo algún delito como puede ser: sabotaje informático, falsificaciones informáticas (utilizando el equipo como instrumento) entre otros; para ello es recomendable evaluar primordialmente si existen puntos críticos de los cuales puedan prevenir dichas debilidades en los controles establecidos por la entidad en cuanto a la seguridad del hardware y del sistema.

2. Al identificar las debilidades en la seguridad física del equipo, en la entidad, es necesario comprobar que tan vulnerable puede ser, Realizando procedimientos que traten de sobrepasar a lo estipulado por la entidad para indagar si

realmente se cumple la seguridad que se le implementa al hardware.

3. Al reconocer las debilidades encontradas se debe determinar el nivel de riesgo que puede existir y las posibles consecuencias que estas pueden traer.

4. Recomendar las medidas necesarias a la Gerencia sobre los hallazgos encontrados y como depurarlos hasta cierta forma con el fin de que las consecuencias de los hechos no perjudiquen a la entidad.

B. Hardware de Respaldo

Las entidades deben poseer hardware de respaldo, el cual puede ser utilizado en situaciones de contingencia (como desastres naturales, pérdida, incendios, saqueos entre otros.), estos deben estar en sitios seguros para que en cualquier emergencia se encuentren en la disposición de continuar con las operaciones de la entidad.

1. Procedimientos Detectivos

1. Verificar si la entidad posee hardware de respaldo y si es, ha sido, o será utilizado con el objeto predestinado.

2. Determinar si el equipo de respaldo se encuentra en un sitio seguro.

3. Verificar quienes son los responsable de dicho equipo, y si hacen buen uso de ellos.

4. identificar si existe la posibilidad que personas no autorizadas pueden disponer de los equipos sin la autorización correspondiente.

5. Verificar si existe algún riesgo inherente en los controles que posee la entidad para los equipos.

6. Si existe riesgo de que el equipo pueda ser utilizado para otros fines o que pueda cometerse algún fraude con éste, determinar si la entidad posee un alto grado de riesgo de algún delito y recomendar procesos de control a utilizar por la institución.

2. Procedimientos Preventivos

1. Identificar si la entidad posee control, mantenimiento y custodia de los equipos de respaldo.

2. Si se posee control sobre los equipos de respaldo, conocer la unidad responsable, persona responsable, documentación que respalde el uso y destino del equipo de respaldo.

3. En caso de que las entidades no posean controles de seguridad sobre aquellos equipos de respaldo, es necesario que sean diseñados e implementados con el fin de contrarrestar posibles intentos de fraudes y delitos informáticos.

3. Procedimientos Correctivos

1. Si se ha descubierto, al realizar auditoria en los equipos de respaldo que posee la entidad, la falta de control sobre estos, es necesario hacer un estudio y evaluar el riesgo que esto puede contraer; y a la vez sugerir la implementación de métodos para que se evite cualquier sospecha de uso mal intencionado del equipo.

2. Si se descubre que la persona encargada de los equipos permite que personas ajenas al departamento tengan acceso a estos, es necesario sugerir la restricción y limitación de responsabilidad del uso del equipo, evaluando previamente si esto puede ser causa de algún delito informático.

3. Al verificarse que los equipos de respaldo los empleados de la entidad pueden disponer de ellos fuera de la institución, es importante que el auditor indague el motivo, quien lo solicita, quien lo autoriza, y si no existe riesgo de perdida o mala utilización de estos.

C. Backup

Las entidades deben poseer backup de la información, por cualquier contingencia que se presente.

1. Procedimientos Detectivos

1. Verificar si la información es salvaguardada de la divulgación no autorizada, daños, sustracción, robo o perdida.

2. Verificar si se llevan controles de acceso que aseguren la información almacenada y en caso de que no existan, recomendar su desarrollo e implantación.

3. Identificar a la persona responsable de la información almacenada, y verificar si el trabajo que realiza es lo suficiente para poder prevenir cualquier alcance de la información por parte de personal no autorizado; de lo contrario evaluar y estudiar el riesgo que existe para llevar a cabo nuevas funciones para la protección de dicha información.

4. Evaluar el sitio donde se encuentran los backup con la información del sistema con el objeto de identificar si es apropiado, de no ser así determinar las causas y las posibles consecuencias que pueden traer.

2. Procedimientos Preventivos

1. Conocer si la entidad posee políticas y control sobre los respaldos que realiza de la información del sistema, y si están de acuerdo a las necesidades, de lo contrario recomendar controles que permitan establecer una barrera de protección de la información para que no pueda ser sustraída fácilmente.

2. Identificar a la persona encargada de realizar y de resguardar los backup; para conocer los procesos que esta realiza para la seguridad de la información, e identificar si se posee algún tipo de riesgo sobre el alcance de dicha información.

3. Verificar si se realizan restricciones al resto del personal que no pertenece al departamento de informática con el objeto de conocer si la información se encuentra protegida de personas ajenas al departamento.

3. Procedimientos Correctivos.

1. Al conocer que la entidad posee deficiencias en el manejo de los respaldo de la información, debido a que cualquier persona puede tener acceso a ella; se deberá sugerir la implementación de nuevas medidas que permitan obtener la seguridad suficiente y el control para que no se dé el caso de sustracción de la información.

2. Si al determinar que existe un posible riesgo de la exposición de los respaldos de información del sistema, es necesario que se tomen medidas adecuadas como: construir instalaciones adecuadas, brindar seguridad en el lugar donde se encuentra almacenada la información, designar personal responsable de ésta área, realizar restricciones al personal etc.

3. Si se descubre que la mayoría del personal tiene acceso a los backup en el momento que desea; se deberá dar a conocer a la gerencia que esto puede conllevar a tener un riesgo muy alto de que haya una sustracción de información o daños a la misma.

Área No. 4 MEDIOS FÍSICOS Y VIRTUALES

Para la detección de los delitos informáticos deben de considerarse los medios físicos y virtuales con los que la institución cuenta para el traslado de la información de las transacciones que esta realiza.

Por lo que se debe realizar una evaluación para investigar los puntos vulnerables que la institución posee en este tipo de medios, donde puedan darse la introducción de hackers, o personas mal intencionadas que desean dañar la integridad del sistema.

Para la detección se pueden considerar los siguientes procedimientos:

1. Procedimientos Detectivos

1. Solicitar un cuadro de inventario de los medios físicos con los que la institución cuenta, y verificar aleatoriamente el estado o condiciones en que se encuentran estos.

2. Solicitar las políticas de seguridad con la que la institución cuenta para la protección de estos medios y determinar los posibles riesgos que no se encuentran cubiertos.

3. Verificar quien es la persona responsable de los medios físicos y virtuales de la institución y conocer las funciones que dicha persona posee.
4. Ingresar al área de sistemas sin ninguna identificación y evaluar las incidencias.

5. Trate de ingresar al sistema de red sin contraseña o sin tener autorización para hacerlo.

6. Entrar al sistema e intentar enviar información hacia otra Terminal exterior y evaluar si este es recibido en la Terminal sin ningún problema y la información recibida de este es legible.

2. Procedimientos Preventivos

1. Determinar si la empresa cuenta con controles de seguridad que ayuden a encontrar los vacíos que pueden existir dentro de las políticas que la institución posee en cuanto a los medios físicos y virtuales.

2. Definir los niveles de acceso de las personas que no pertenezcan al área de sistemas con el fin de evitar que cualquier persona ingrese al sistema de la empresa.

3. Para el envío de la información a través de la intranet e Internet, utilizar firmas digitales para certificar la procedencia de los datos y asegurar así que aun cuando sean interceptados, no sean vistos por personas ajenas a la empresa.

4. Configurar la red por medio de IP’s lo que se puede realizar a través de router; donde a cada maquina se le asigna una dirección IP para identificarla estos actuaran como filtro entre el servidor y las terminales.

5. Realizar evaluaciones periódicas de acuerdo a la necesidad de la entidad a los controles que esta posee para los medios físicos y virtuales.

Procedimientos Correctivos

1. Si se han detectado problemas por desactualización de equipos que se utilizan para los medios virtuales, realizar una revisión exhaustiva para determinar las diversas actualizaciones que deben realizarse al equipo para su buen funcionamiento y protección.

2. En el caso que existiera vacíos en el medio virtual, de lo cual puedan ser victimas de delitos informáticos, solicitar al

proveedor la creación de parches para cubrir los vacíos encontrados.

3. Al detectarse que existen empleados que tengan acceso para realizar modificaciones del medio virtual de la institución, y que éste no pertenezca al área de informática, se debe de restringir dichos accesos para proteger los medios virtuales de cualquier eventualidad que vaya en contra del bienestar de institución.

4. Al encontrar que no se realiza el mantenimiento adecuado a los medios físicos y virtuales, y estos representen algún riesgo, es recomendable que se realice una propuesta de mantenimiento de acuerdo a las necesidades de la institución para prevenir cualquier manipulación por defectos del equipo o del sistema de la institución.

5. Si se determina que el lugar donde se encuentra el servidor, no cumple con las condiciones de seguridad adecuadas para el resguardo de la información, realizar un estudio de las condiciones más adecuadas para determinar la mejor ubicación de este.

CAPITULO IV. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

De la investigación de campo realizada a las cajas y Bancos de los trabajadores del sistema fedecrédito, se logro recabar información que ha permitido obtener las siguientes conclusiones:

1) Se determinó que las cajas y los bancos de los trabajadores del sistema fedecrédito no cuentan con una auditoria especializada en el área de sistemas informáticos por lo que no realizan procedimientos para la detección de delitos informáticos.

2) Se observó que las instituciones no poseen controles que les garanticen la seguridad de los sistemas de información por lo que se encuentran en el riesgo de ser victimas de delitos informáticos.

3) La principal causa por la que los auditores internos de las instituciones, no realizan procedimientos para la detección de delitos informáticos, es la falta de conocimientos para la realización de estos.

4) El contenido de la propuesta se encuentra enfocada a sugerir procedimientos de auditoria que ayuden a la detección, prevención, y corrección de delitos informáticos.

4.2 RECOMENDACIONES

1) Se recomienda que las cajas y los bancos de los trabajadores del sistema fedecrédito, contraten o capaciten al personal de auditoria en el área de sistemas de información computarizados.

2) Es recomendable que las instituciones del sistema fedecrédito elaboren controles que ayuden a minimizar y garantizar la seguridad de los sistemas de información, para que no sufran ningún tipo de delito informático.

3) Se recomienda a las instituciones que cuentan con sistemas de información computarizados, la implementación de los procedimientos propuestos en el capitulo III de este documento, para la detección, prevención y corrección de delitos informáticos.

BIBLIOGRAFÍA

Metodología de la Investigación

Autor: Roberto Hernández Sampieri

Carlos Fernández Collado

Pilar Baptista Lucio

Tercera Edición, Año 2003

Guía para Realizar Investigaciones Sociales

Autor: Raúl Rojas Soriano

40ª Edición. Año 2004

Legislación de la República de El Salvador

Código Penal

Ley de Marcas y Otros Signos Distintivos

Ley de Fomento y Protección de la Propiedad Intelectual

Estadística para La Administración y Economía

Autor: David R. Anderson

Octava Edición

Auditoria de Sistemas Electrónicos

Autor: W. Thomas Porter, Jr.

1ª Edición. Año 1971.

Auditoria de Sistemas Computacionales

Autor: Carlos Muñoz Rozo

1ª Edición Año 2002.

Pearson Educación

Sitios Web visitados

www.delitosinformaticos.com

www.pricewaterhousecooper.com

www.perantivirus.com

www.monografias.com

www.elsalvador.com El diario de Hoy, vértice, 27 de febrero de 2005.

www.uca.edu.sv/publica/idhuca/articulos.html

www.auditoriasistemas.com/auditoria-de-sistemas-informaticos/

Boletín de Prensa - Fiscalía General de la República.htm

ANEXOS

ANEXO No. 1

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECONÓMICAS
ESCUELA DE CONTADURÍA PÚBLICA

"CUESTIONARIO SOBRE DELITOS INFORMÁTICOS Y PROCEDIMIENTOS DE AUDITORIA APLICADOS A LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS"

Área de Trabajo: _____ Cargo: _____

Este instrumento esta diseñado para recopilar información relacionada con los delitos informáticos y los procedimientos de auditoria aplicados por las empresas en el área de los Sistemas de Información Computarizados. Los datos recopilados se estudiaran para poder brindar una propuesta de procedimientos de auditoria aplicables al área informática.

Objetivo: Recopilar la información necesaria para proponer procedimientos de auditoria que ayuden a detectar, prevenir y corregir los delitos informáticos.

Instrucciones: Le pedimos de favor tomarse unos minutos para contestar el presente cuestionario marcando con una X la respuesta. Consulte cualquier duda que tenga con el investigador, de antemano agradecemos su fina colaboración.

A. ASPECTOS GENERALES

1. Cuenta la empresa con:
   - Departamento de Informática _____
   - Departamento de Auditoria de Sistemas _____

Objetivo: Conocer la existencia de un departamento específico para el área de trabajo.

2. ¿Cuántas personas hay en cada departamento y cuál es su nivel académico promedio?

   No. De personas Nivel Académico

   - Depto. De Informática _____
   - Depto. De Auditoria _____

Objetivo: Saber si cuenta con el personal idóneo para la ejecución del trabajo dentro del área.

3. ¿Se capacita continuamente al personal?
   - Solo Depto. De Informática _____
   - Solo Depto. De Auditoria _____
   - Ambos _____
   - Ninguno _____

Objetivo: Conocer si se prepara el personal dotándolo de los conocimientos necesarios para el desarrollo eficaz y eficiente de su trabajo.

B. DEL SISTEMA DE INFORMACIÓN COMPUTARIZADO

4. ¿Cómo fue adquirido el Sistema de Información utilizado por la empresa para el registro de sus operaciones?

- Compra de sistema estándar _____
- Elaboración de un Sistema a la medida _____
- Donación del Sistema _____
- Arrendamiento del Sistema _____
- Otro _____

Especifique por favor:

_____
_

Objetivo: Saber como fue adquirido el Sistema de información de la empresa.

5. ¿Posee la empresa licencia del Sistema utilizado?
   Si _____ No _____

Objetivo: Indagar si el sistema utilizado es legal.

6. ¿Cómo está estructurado funcionalmente el Sistema que utilizan en su empresa para el registro de sus operaciones?
   - Módulos _____
   - Aplicaciones independientes _____
   - Menús y Submenús _____
   - Otros _____

   Especifique por favor:

   _____

Objetivo: Conocer la forma en que funciona el sistema de información.

7. ¿Posee la empresa los programas fuente para la modificación de las funciones de este?

Si _____ No _____

Objetivo: Verificar la vulnerabilidad en relación con los requerimientos para efectuar cambios en el sistema (programas fuente)

8. ¿Necesita el sistema del uso de internet para el traslado de la información entre usuarios y otros entes externos?

Si _____ No _____

Objetivo: Definir la posibilidad de que la información procesada en el sistema corre el riesgo de ser desviada a otra persona ajena a la empresa y que pueda hacer mal uso de dicha información.

9. ¿Ha presentado alguna falla el sistema de información con respecto de los datos de este?

- Entrada de datos _____
- Procesamiento de datos _____
- Salida de datos _____

¿Qué sucede?

- Los datos se duplican _____
- La información no concuerda con los datos _____
- Los datos o la información se pierden _____
- La información se cruza con otra _____
- Procesa mal los datos _____
- La información que sale del sistema está alterada _____
- No ingresa bien los datos _____
- Otros _____

Especifique _____

Objetivo: Conocer las posibles inconsistencias que posee el sistema con el fin de determinar si existen algunos vacios al

momento de procesarse la información.

C. RESPALDO DE LA INFORMACIÓN (BACKUP)

10. ¿Se hace respaldo de la información generada por el Sistema?

Si _____ No _____

Objetivo: Saber si se respalda la información por algún acontecimiento de daño, pérdida, robo, hurto, etc.

11. ¿Cada cuanto tiempo se respalda la información?

- Diariamente _____
- Semanalmente _____
- Mensualmente _____
- Anualmente _____
- Otros _____ Especifique _____

Objetivo: Conocer el grado de importancia que se de a la información generada por el sistema.

12. ¿En que medios se almacena la información respaldada?

- Disquete _____
- CD _____
- DVD _____
- Memorias USB _____
- Microfilm _____
- Otros _____ Especifique _____

Objetivo: Determinar el grado de seguridad de la información respaldada de acuerdo al medio de almacenamiento.

D. CONTROLES GENERALES DEL SISTEMA DE INFORMACIÓN

13. ¿Qué controles tiene la empresa para el resguardo de la información contenida en su sistema de información?

- Hacer backups _____
- Crear cuentas de usuarios _____
- Hacer varias copias de los respaldos _____
- Restringir el acceso al sistema de información _____

Objetivo: Establecer que tipo de controles se tiene para el resguardo de la información que está contenida dentro del sistema de información que utiliza la empresa para prevenir cualquier alteración de la información.

14. ¿Se crean cuentas de usuarios (nombre y contraseña) para el uso del sistema?

Si _____ No _____

Objetivo: Verificar si en el acceso sistema existen niveles de seguridad definidos.

15. ¿Permite el sistema el ingreso de dos o más personas con una misma cuenta de usuario?

Si _____ No _____

Objetivo: Determinar si varias personas pueden ingresar al sistema usando una misma cuenta de usuario.

16. ¿Se cambia periódicamente la contraseña de usuarios y cada cuanto tiempo?

Si _____ No _____

Especificar tiempo: _____

Objetivo: Saber si se trata de evitar robo de cuentas usuarios.

17. ¿Se tiene definida la distribución de las funciones del sistema de información computarizado de acuerdo al perfil de cada usuario?

Si _____ No _____

Objetivo: Determinar si cada usuario del sistema tiene acceso a las funciones del sistema acorde a las transacciones que realiza.

18. ¿Se hacen revisiones al Sistema de información utilizado por la empresa?

Si _____ No _____

¿Cada cuanto tiempo?

- Semanalmente _____
- Mensualmente _____
- Trimestralmente _____
- Semestralmente _____
- Anualmente _____
- Otro _____ Especifique _____

Objetivo: Determinar si se realizan revisiones al sistema de información para descartar cualquier posibilidad de mal funcionamiento e identificar las posibles causas.

19. ¿Se hacen pruebas del sistema para ver si los comandos realizan las opciones de acuerdo a las funciones programadas para cada botón/pestaña?

Si _____ No _____

Objetivo: Verificar si el sistema funciona correctamente y no ha sido manipulado con respecto de sus funciones.

20. ¿Se hacen pruebas de validación de los datos y la

información generada por el sistema?

- Datos de entrada _____
- Procesamiento de datos _____
- Salida de información _____

Objetivo: Verificar la integridad de los datos y la información generada por el sistema de información.

E. LOS DELITOS INFORMÁTICOS Y LA AUDITORIA DE SISTEMAS

21. ¿Sabe usted qué son los Delitos Informáticos?

Si _____ No _____

Objetivo: Establecer el grado de conocimiento que el personal del área de informática y auditoria de sistemas posee con respecto de los delitos informáticos.

22. ¿Ha sido victima la empresa de algún delito informático?

- No ha sido victima de algún delito _____
- Manipulación del sistema de información _____
- Hurto de información confidencial _____
- Destrucción de la información del sistema _____
- Falsificación de documentos del sistema _____
- Uso no autorizado o indebido del sistema _____
- Alteración de las funciones del sistema _____
- Destrucción de la información del sistema _____
- Implantación de virus en el sistema _____
- Otros _____

Especifique _____

Objetivo: Establecer si la empresa ha sido victima de cualquiera de los delitos informáticos existentes.

23. ¿Qué acción o acciones ha tomado la empresa para evitar ser victima de nuevo de algún delito informático?

- No ha realizado alguna acción _____
- Denunciar el hecho con la policía _____
- Contratar un experto para el control _____
- Mejorar la seguridad del sistema _____
- Implantar nuevos controles de seguridad _____
- Restringir el acceso al sistema _____
- Otra _____

  Especifique _____

Objetivo: Verificar las acciones tomadas por la empresa para evitar la reincidencia de delitos informáticos.

24. ¿Se ejecuta algún plan estratégico de auditoria en relación al sistema de información computarizado?

Si _____ No _____

Si su respuesta es afirmativa, ¿cada cuanto tiempo lo ejecutan?

- Mensual _____
- Trimestral _____
- Semestral _____
- Anual _____
- Otro _____ Especifique _____

Objetivo: Saber si existe un plan definido a seguir para auditar el sistema de información.

25. ¿Posee el sistema de información un registro detallado de las personas que ingresaron al sistema y lo que realizaron en este?

Si _____ No _____

Objetivo: Conocer si existe la forma de poder ver lo que cada usuario hace en el sistema a fin de determinar responsabilidades por cualquier incidente dentro del mismo.

26. ¿Qué medidas se toman con respecto de la auditoria de sistemas para evitar los delitos informáticos en la empresa?

- Realizar pruebas de validación de datos _____
- Realizar pruebas de integridad de la información _____
- Otras _____

  Especifique

  _____

Objetivo: Revisar si las medidas tomadas son adecuadas para evitar delitos informáticos y cumplen con los objetivos de la empresa.

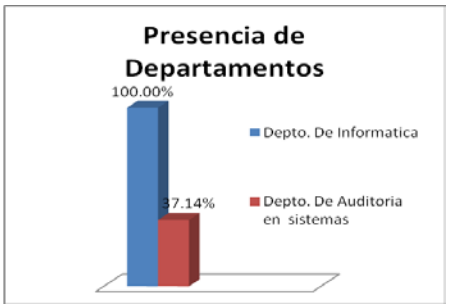
ANEXO No. 2

ANÁLISIS Y TABULACIÓN DE PREGUNTAS

A. ASPECTOS GENERALES

1. Cuenta la empresa con:
   - Departamento de Informática
   - Departamento de Auditoria de Sistemas

Tipo de Departamento	Cantidad	%
Depto. De Informática	35	100.00%
Depto. De Auditoria en sistemas	13	37.14%



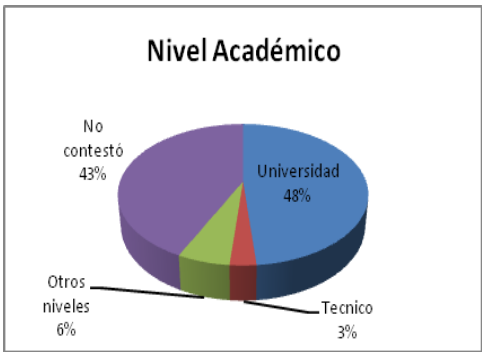
ANALISIS: De acuerdo a los datos recolectados en esta pregunta, se evidencia que existe presencia del departamento de informatica en el 100% de las 35 instituciones seleccionadas como muestra, mientras que solo 13, equivalentes al 37.14% del total de la muestra, posee la presencia de un departamento de audotiria en sistemas.

2. ¿Cuántas personas hay en cada departamento y cuál es su nivel académico promedio?

	No. De personas	Nivel Académico
• Depto. De Informática	_____	_____
• Depto. De Auditoria	_____	_____

Numero de personas por departamento	
Informática	35
Auditoria	24

Nivel Académico	Promedio	%
Universidad	17	48.57%
Técnico	1	2.86%
Otros niveles	2	5.71%
No contestó	15	42.86%

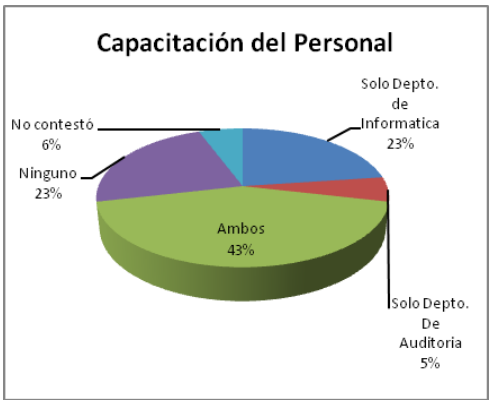


ANALISIS: En esta pregunta se observa que el nivel academico promedio de las personas que hay en ambos departamentos es un nivel Universitario, que equivalen al 48.57%%, aunque el 42.86% del total de la muestra prefirió no contestar respecto del nivel academico.

3. ¿Se capacita continuamente al personal?

- Solo Depto. De Informática _____
- Solo Depto. De Auditoria _____
- Ambos _____
- Ninguno _____

Capacitación del Personal		%
Solo Depto. de Informática	8	22.86%
Solo Depto. De Auditoria	2	5.71%
Ambos	15	42.86%
Ninguno	8	22.86%
No contestó	2	5.71%



ANÁLISIS: Se observa que la mayoría de las instituciones encuestadas capacita a los empleados de ambos departamentos, mas sin embargo, también se ve que hay un 22.86% que solo capacita al departamento de informática e igual porcentaje no capacita a ninguno.

B. DEL SISTEMA DE INFORMACIÓN COMPUTARIZADO

4. ¿Cómo fue adquirido el Sistema de Información utilizado por la empresa para el registro de sus operaciones?

- Compra de sistema estándar _____
- Elaboración de un Sistema a la medida _____
- Donación del Sistema _____
- Arrendamiento del Sistema _____
- Otro _____

  Especifique por favor:

  _____

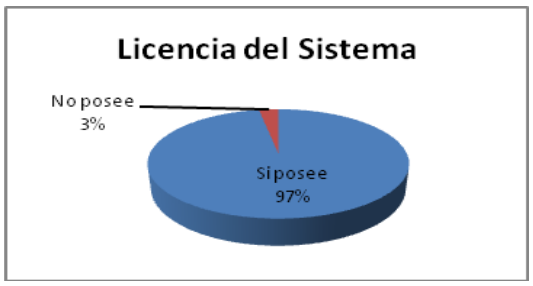
Adquisición del Sistema de Información		**%**
Compra de sistema estándar	16	45.72%
Elaboración de un sistema a la medida	13	37.14%
Donación del sistema	0	0.00%
Arrendamiento del sistema	6	17.14%
Otros	0	0.00%

ANALISIS: Se puede ver que el 45.72% de las instituciones ha comprado el sistema informatico, el 37.14% optó por elaborar un sistema acorde a sus operaciones (a la medida) y el restante 17.14% arrenda el sistema. Es asi que se observa que la mayoria de las instituciones cuenta con un sistema propio.

5. ¿Posee la empresa licencia del Sistema utilizado?

   Si _____ No _____

Licencia del Sistema		
Respuesta	**Cantidad**	**%**
Si posee	34	97.14%
No posee	1	2.86%



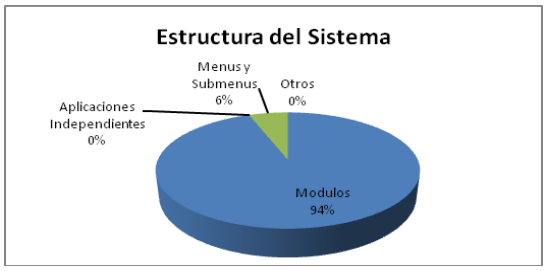
ANALISIS: El 97.14% de la muestra tiene la licencia respectiva del sistema que utilizan para el registro de sus operacioens, es decir, que lo han obtenido con erspaldo del proveedor; sin embargo, una institucion que representa el 2.86% de la muestra no posee la licencia del sistema, por tanto, no tiene un respaldo legitimo para el uso del sistema informatico.

6. ¿Cómo está estructurado funcionalmente el Sistema que utilizan en su empresa para el registro de sus operaciones?

- Módulos _____
- Aplicaciones independientes _____
- Menús y Submenús _____
- Otros _____

  Especifique por favor:_____

Estructura del Sistema		%
Módulos	33	94.29%
Aplicaciones Independientes	0	0.00%
Menús y Submenús	2	5.71%
Otros	0	0.00%



ANALISIS: Se observa que 33 instituciones, equivalente al 94.29% de la muestra, tiene estructurado su sistema de tal forma que funcione por modulos, es decir, que son sistemas integrados; y el restante 5.71% lo ha estructurado de forma que se presenten las funciones como menus y submenus.

7. ¿Posee la empresa los programas fuente para la modificación de las funciones de este?

   Si _____ No _____

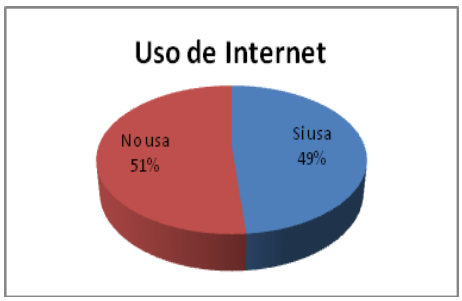
Programas Fuente del Sistema		
Respuesta	**Cantidad**	**%**
Si posee	17	48.57%
No posee	18	51.43%

ANALISIS: Se evidencia claramente que mas de la mitad de las instituciones encuestadas, el 51.43% equivalente a 18 institucioens, no cuenta con los programas fuente del sistema de informacion que utilizan, por ende, no pueden cambiar ninguna funcion dentro del sistema por ellos mismos, sino que dependen de la aprobacion del proveedor para hacer alguna modificación, siendo este ultimo quien la realice.

8. ¿Necesita el sistema del uso de internet para el traslado de la información entre usuarios y otros entes externos?

   Si _____ No _____

Uso de Internet para Trasladar la Información		
Respuesta	**Cantidad**	**%**
Si usa	17	48.57%
No usa	18	51.43%



ANALISIS: Se puede obsevar que en un poco mas de la mitad de las instituciones (el 51.43%), no es necesario el uso de internet juntamente con el sistema para el traslado de la informacion entre usuarios, por ende, hay una menor probabilidad de que la seguridad de su sistema pueda ser violada por alguien ajeno a la empresa a traves de internet; siendo asi menos propensos a los delitos informaticos desde internet.

9. ¿Ha presentado alguna falla el sistema de información con respecto de los datos de este?
   - Si _____
   - No _____
   - No contestó _____

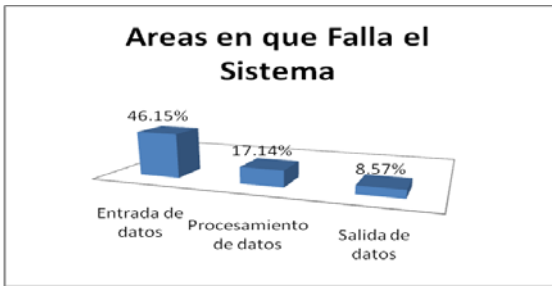
   Áreas de Fallas del Sistema:
   - Entrada de datos _____
   - Procesamiento de datos _____
   - Salida de datos _____

   ¿Qué sucede?
   - Los datos se duplican _____
   - La información no concuerda con los datos _____
   - Los datos o la información se pierden _____
   - La información se cruza con otra _____
   - Procesa mal los datos _____
   - La información que sale del sistema está alterada _____
   - No ingresa bien los datos _____
   - Otros _____

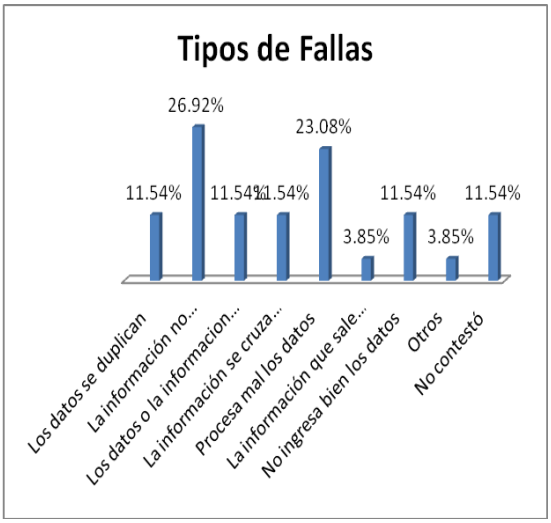
     Especifique _____

Presenta Fallas el Sistema		%
Si	26	74.29%
No	6	17.14%
No contestó	3	8.57%

Fallas del Sistema		%
Entrada de datos	12	46.15%
Procesamiento de datos	14	53.85%
Salida de datos	11	42.31%



Tipos de Fallas del Sistema		%
Los datos se duplican	3	11.54%
La información no concuerda con los datos	7	26.92%
Los datos o la información se pierde	3	11.54%
La información se cruza con otra	3	11.54%
Procesa mal los datos	6	23.08%
La información que sale del sistema está alterada	1	3.85%
No ingresa bien los datos	3	11.54%
Otros	1	3.85%
Se cae el Servidor	1	
No contestó	3	11.54%



ANÁLISIS: Se puede observar que la mayoría de los sistemas informáticos de las empresas presentan fallas (74.29% equivalente a 26 instituciones), y que la mayor cantidad de estas fallas de los datos que se introducen, procesan o salen

del sistema, se observa dentro del procesamiento de los datos, pues representan el 53.85% de las 26 instituciones que presentan fallas en sus sistemas. Además, la falla que mayormente se da es que la información no concuerda con los datos, equivalente a un 26.92% siguiéndole el mal procesamiento de los datos con 23.08% de las 26 instituciones que presentaron fallas en el sistema.

C. RESPALDO DE LA INFORMACIÓN

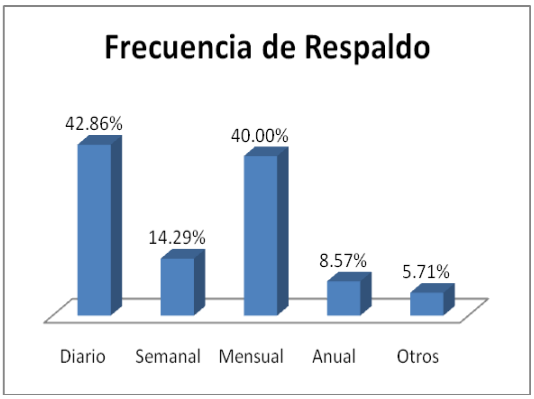
10. ¿Se hace respaldo de la información generada por el Sistema?

Opciones	Respuestas	%
Si	35	100.00%
No	0	0.00%

ANÁLISIS: Según la muestra de 35 encuestas se determinó que el 100% realiza respaldos de la información que genera el sistema

11. ¿Cada cuanto tiempo se respalda la información?

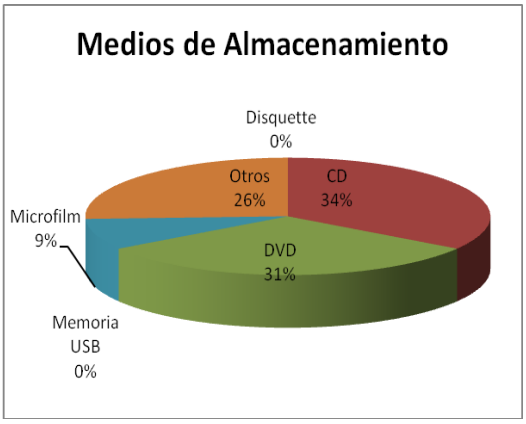
Opciones	Respuestas	%
Diario	15	42.86%
Semana	5	14.29%
Mensual	14	40.00%
Anual	3	8.57%
Otros	2	5.71%
Semestralmente 1		
Depende del volumen de información 1		



ANÁLISIS: De acuerdo a las respuestas obtenidas el 42.86% hace respaldos diarios de su información el 14.29% lo hace cada semana, el 40% mensualmente, el 8.57% anualmente y entre otros se encuentra el 5.71% que lo realiza de forma semestralmente y dependiendo del volumen de información.

12. ¿En que medios se almacena la información respaldada?

Opciones		**Respuestas**	**%**
Disquete		0	0.00%
Cd		12	34.29%
DVD		11	31.43%
Memoria USB		0	0.00%
Microfilm		3	8.57%
Otros		9	25.71%
Tape	2		
Disco Duro	1		
Cinta	1		
Servidor Central	5		

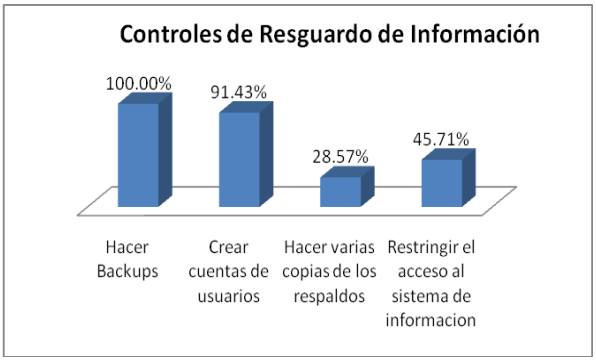


ANÁLISIS: Las Cajas de crédito utiliza diferentes medios para almacenar la información respaldada de acuerdo a la muestra ninguna de ellas lo almacena en diskette, el 34% los almacena en Cd, 31% en DVD, ninguno utiliza memoria USB, 9% en microfilm y otros esta el 26% que son instituciones que almacenan su información en Tape, Disco Duro, Cinta y Servidor Central.

D. CONTROLES GENERALES DEL SISTEMA DE INFORMACIÓN

13. ¿Qué controles tiene la empresa para el resguardo de la información contenida en su sistema de información?

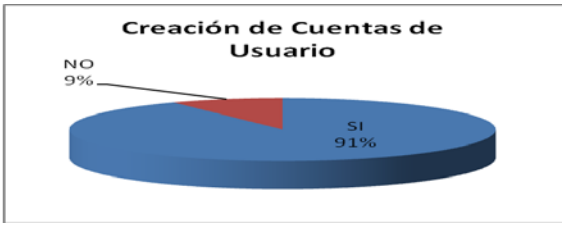
Opciones	Respuestas	%
Hacer Backups	35	100.00%
Crear cuentas de usuarios	32	91.43%
Hacer varias copias de los respaldos	10	28.57%
Restringir el acceso al sistema de información	16	45.71%



ANÁLISIS: Conforme a la muestra tomada, las cajas de crédito poseen diferentes tipos de controles para resguardo de la información contenida en su sistema, el 100.00% hace backups, el 91.43% crea cuentas de usuario, el 28.57% hace varias copias de los respaldos y el 45.71% restringe el acceso al sistema de información.

14. ¿Se crean cuentas de usuarios (nombre y contraseña) para el uso del sistema?

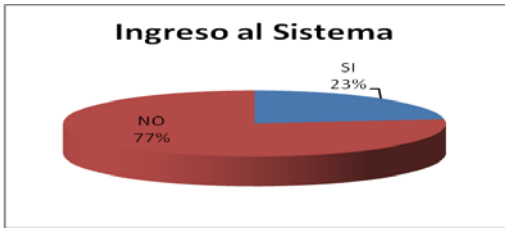
Opciones	Respuestas	%
Si	32	91.43%
No	3	8.57%



ANÁLISIS: Según los resultados de la muestra, el 91% de las instituciones encuestadas crea cuentas de usuario (nombre y contraseña) en sus sistemas para el uso del sistema y el 9% no crean dichas cuentas.

15. ¿Permite el sistema el ingreso de dos o más personas con una misma cuenta de usuario?

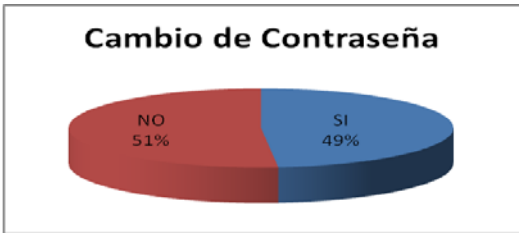
Opciones	Respuestas	%
Si	8	22.86%
No	27	77.14%



ANÁLISIS: Según los resultados el 23% de las cajas de crédito permite el sistema el ingreso de dos o más personas con una misma cuenta de usuario y el 77% no permite el ingreso de dos o más personas.

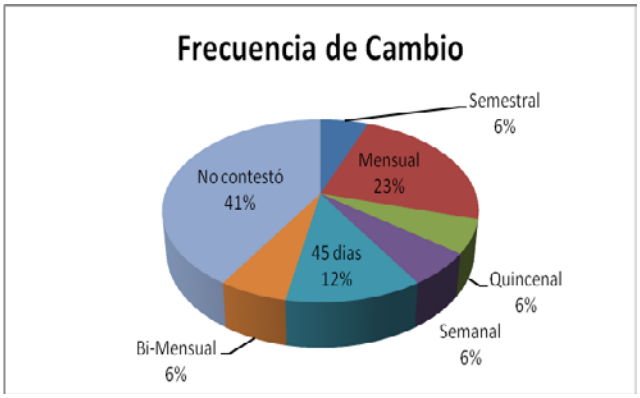
16. ¿Se cambia periódicamente la contraseña de usuarios y cada cuanto tiempo?

Opciones	Respuestas	%
Si	17	48.57%
No	18	51.43%



¿Especificar tiempo?

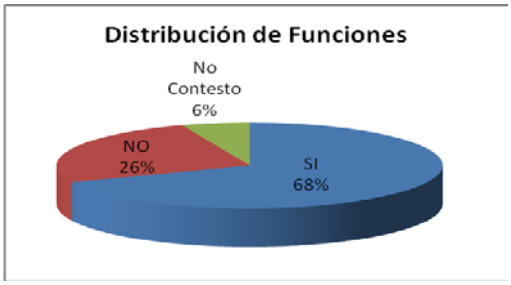
Semestral	1	5.88%
Mensual	4	23.53%
Quincenal	1	5.88%
Semanal	1	5.88%
45 días	2	11.76%
Bi-Mensual	1	5.88%
No contestó	7	41.19%



ANÁLISIS: De acuerdo a la muestra obtenida el 49% de las cajas de crédito cambia periódicamente la contraseña de usuario y el 51% no la cambia. Y de acuerdo al tiempo de cambio de la contraseña la mayoría la cambia mensualmente (23.53% de las instituciones que si lo hacen), aunque la mayoría no contestó en cuanto a la frecuencia de tiempo en que cambian sus contraseñas (41.19%).

17. ¿Se tiene definida la distribución de las funciones del sistema de información computarizado de acuerdo al perfil de cada usuario?

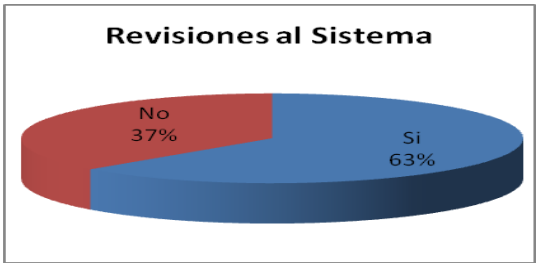
Opciones	Respuestas	%
Si	24	68.57%
No	9	25.71%
No Contestó	2	5.72%



ANÁLISIS: De acuerdo a los resultados el 68 % de los encuestados tiene definida la distribución de las funciones del sistema de información computarizado de acuerdo al perfil de cada usuario, 26% no las tiene definidas y el 6% no contesto.

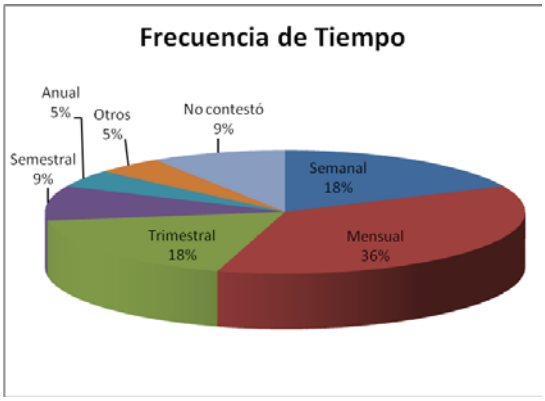
18. ¿Se hacen revisiones al Sistema de información utilizado por la empresa?

Opciones	Respuestas	%
Si	22	62.86%
No	13	37.14%



¿Cada cuánto tiempo?

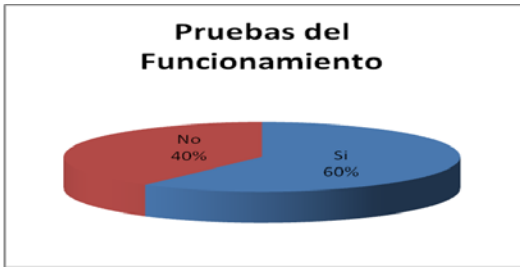
Semanal		4	18.18%
Mensual		8	36.36%
Trimestral		4	18.18%
Semestral		2	9.09%
Anual		1	4.55%
Otros		1	4.55%
A veces	1		
No Contestó		2	9.09%



ANÁLISIS: El 63% de la muestra contestó que hacen revisiones a los sistemas de información y el 37% no realiza ninguna revisión a estos. Además, la mayoría lo hace mensualmente (36.36% de las instituciones que contestaron que si hacen las revisiones)

19. ¿Se hacen pruebas del sistema para ver si los comandos realizan las opciones de acuerdo a las funciones programadas para cada botón/pestaña?

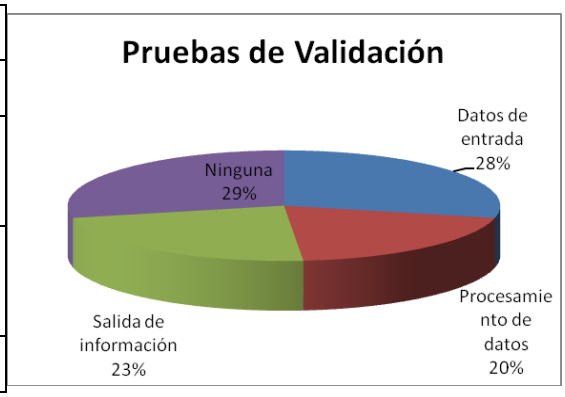
Opciones	Respuestas	%
Si	21	60.00%
No	14	40.00%



ANÁLISIS: En la pruebas de las comandos de los sistemas el 60% de las instituciones encuestadas contestó que si realizan pruebas a los comandos del sistema para ver si funcionan de acuerdo a las especificaciones con las que se programó y el 40% no realiza esas pruebas.

20. ¿Se hacen pruebas de validación de los datos y la información generada por el sistema?

Opciones	Respuestas	%
Datos de entrada	10	28.57%
Procesamiento de datos	7	20.00%
Salida de información	8	22.86%
Ninguna	10	28.57%



ANÁLISIS: con respecto a las pruebas de integridad a la información del sistema el 28%, respondió que no se realiza ninguna prueba, misma cantidad respondió que realiza pruebas a los datos de entrada, 20% realiza pruebas al procesamiento de datos y 23% lo realiza a la salida de datos.

E. LOS DELITOS INFORMÁTICOS Y LA AUDITORIA DE SISTEMAS

21. ¿Sabe usted que son los delitos informaticos?

Repuestas	Cantidad	%
Si	35	100.00%
No	0	0.00%

ANÁLISIS: Se puede ver que el 100% de las instituciones encuestadas tiene conocimiento respecto de que son los delitos informaticos.

22. ¿Ha sido victima la empresa de algún delito informático?

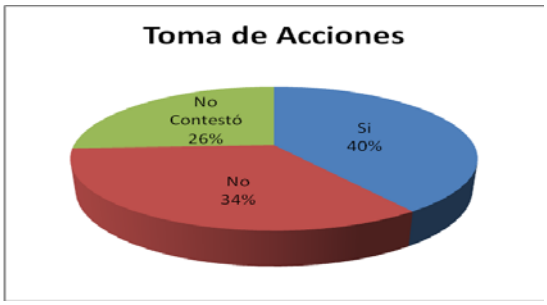
Respuesta	Cantidad	%
Si	11	31.43%
No	23	65.71%
No Contestó	1	2.86%

Tipos de Delitos	Cantidad	%
Manipulación del sistema de información	3	27.27%
Uso no autorizado o indebido del sistema	3	27.27%
Destrucción de la información del sistema	1	9.09%
Implantación de virus en el sistema	3	27.27%
Otros	1	9.10%

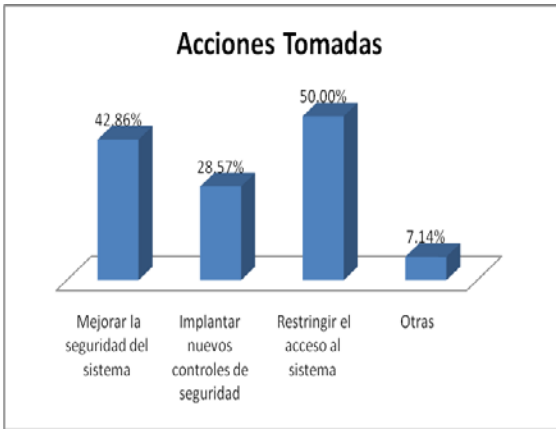
ANÁLISIS: Como se puede observar dentro de la muestra de 35, entre ellas cajas y Bancos de los Trabajadores, el 65.71% de estas no ha sido victima de delitos informáticos, mientras que 11 instituciones (31.43%) si han sido victima de algun delito informatico. Entre los delitos más frecuentes se encuentran: manipulación del sistema de información que muestra un porcentaje de 27.27% de las instituciones que han sido victima de delitos informaticos, igual número ha sido victima del uso sin autorización o indebido de su sistema, al igual que por la implantación de virus en el sistema. Aunque es necesario resaltar que algunos de ellos han sido victima de más de un delito informático.

23. ¿Ha tomado la empresa alguna acción para evitar ser victima de nuevo de algún delito informático?

Respuesta	**Cantidad**	**%**
Si	14	40.00%
No	12	34.29%
No Contestó	9	25.71%



Acciones Tomadas	**Cantidad**	**%**
Mejorar la seguridad del sistema	6	42.86%
Implantar nuevos controles de seguridad	4	28.57%
Restringir el acceso al sistema	7	50.00%
Otras		
Realizar Políticas de Seguridad	1	7.14%



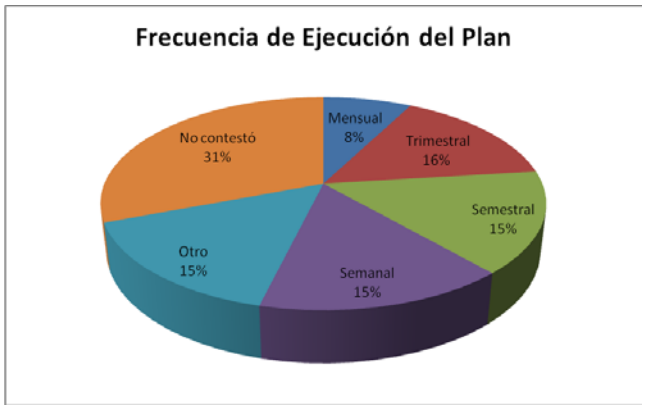
ANÁLISIS: Se observa que el 40% de las instituciones encuestadas ha tomado medidas preventivas para evitar ser victima de algun delito informático, el 34.29% no lo ha hecho y un 25.71% prefirió no contestar. Dentro de las acciones tomadas por las las instituciones, tenemos que la mayoria de ellas (50%) han restringido el acceso al sistema, el 42.86% ha mejorado la seguridad de su sistema y el 28.57% optó por implantar nuevos controles de seguridad para evitar ser victima de los delitos informaticos.

24. ¿Se ejecuta algún plan estratégico de auditoria en relación al sistema de información computarizado?

Pregunta	**Respuesta**	**%**
Si	13	37.14%
No	20	57.14%
No contestó	2	5.72%

Si su respuesta es afirmativa, ¿cada cuánto tiempo lo ejecutan?

Frecuencia de Ejecución	**Cantidad**	**%**
Mensual	1	7.70%
Trimestral	2	15.38%
Semestral	2	15.38%
Semanal	2	15.38%
Otro	2	15.38%
No contestó	4	30.78%



ANÁLISIS: Del 100% de la muestra tomada, el 37.14% respondió que si han realizado un plan estratégico en relacion al sistema información, el 57.14% no posee un plan estratégico para detectar cualquier anomalía dentro de su sistema de información y 5.72% no contestó la pregunta. Además, de las instituciones que contestaron que realizan un plan estratégico, se determinó que el 7.70% ejecuta su plan mensualmente, el 15.38% lo ejecuta trimestralmente, a su vez también un 15.38% dijo que lo ejecuta semestralmente, igual cantidad lo realiza de forma semanal y el 15.38% lo hacen en otro tipo de frecuencia de tiempo y un 30.78% no contestó en cuanto tiempo ejecuta su plan de auditoria.

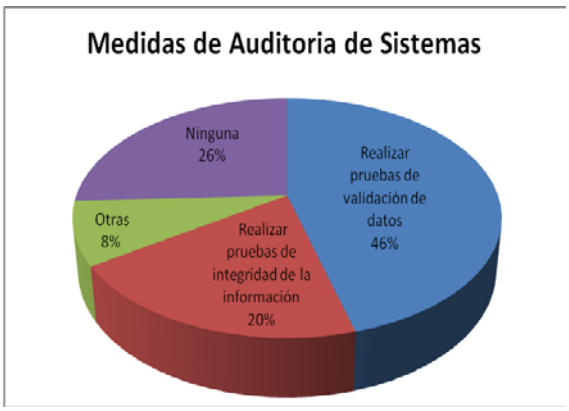
25. ¿Posee el sistema de información un registro detallado de las personas que ingresaron al sistema y lo que realizaron en este?

Respuestas	**Cantidad**	**%**
Si	18	51.43%
No	16	45.71%
No Contestó	1	2.86%

ANÁLISIS: El 51.43% de la instituciones encuestas dijo que su sistema si lleva un registro detallado de las personas que ingresan al sistema y lo que hacen dentro de este, el 45.71% contestó que no se lleva un control de las personas que tienen acceso al sistema y un 2.86% se abstuvo de responder la pregunta.

26. ¿Qué medidas se toman con respecto de la auditoria de sistemas para evitar los delitos informáticos en la empresa?

Repuestas	**Cantidad**	**%**
Realizar pruebas de validación de datos	16	45.71%
Realizar pruebas de integridad de la información	7	20.00%
Otras	3	8.57%
Validación de Claves		
Seguridad Física		
Nadie ajeno a la empresa tiene acceso al Sistema		
Ninguna	9	25.72%



ANÁLISIS: El 45.71% de la muestra tomada realiza pruebas de validación de datos en auditoria, un 20% realiza pruebas de integridad de la información y 8.57% realiza otro tipo de pruebas de auditoria para revisión de la información presentada. Y 25.72% no realiza ningún tipo de pruebas para verificar la integridad de los datos que son dados por el sistema.