UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDICIPLINARIA ORIENTAL

DEPARTAMENTO DE CIENCIAS ECONOMICAS

SECCION DE CONTADURIA PÚBLICA.

“PROPUESTA DE UNA GUIA DE EVALUACION DE SEGURIDAD INFORMATICA A LAS EMPRESAS DISTRIBUIDORAS DE TELEFONIA MOVIL DE LA CIUDAD DE SAN MIGUEL”.

TRABAJO DE GRADUACION PRESENTADO POR:

BOLAINES PORTILLO, ROCIO ELIZABETH.

GOMEZ HERNANDEZ, OSCAR RENE.

MARTINEZ PAIZ, ERNESTO SCARLETT.

PARA OPTAR AL GRADO DE:

LICENCIADO(A) EN CONTADURIA PUBLICA

SAN MIGUEL, EL SALVADOR, CENTRO AMERICA

AUTORIDADES DE LA UNIVERSIDAD DE EL SALVADOR

RECTOR

ING. MARIO ROBERTO NIETO LOVO

VICE - RECTOR ACADÉMICO

MAESTRA ANA MARÍA GLOWER DE ALVARADO

SECRETARIA GENERAL

DRA. ANA LETICIA DE AMAYA

FISCAL

LIC. FRANCISCO CRUZ LETONA

AUTORIDADES DE LA FACULTAD MULTIDISCIPLINARIA ORIENTAL

DECANO

LIC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ

VICE - DECANO

LIC. CARLOS ALEXANDER DÍAZ

SECRETARIO

LIC. JORGE ALBERTO ORTÉZ HERNÁNDEZ

DEPARTAMENTO DE CIENCIAS ECONÓMICAS

JEFE DE DEPARTAMENTO

LIC. HÉCTOR BARRERA ARIAS

COORDINADOR GENERAL DE PROCESO DE GRADUACIÓN

LIC. ARNOLDO ORLANDO SORTO MARTÍNEZ

DOCENTE DIRECTOR

LIC. MIGUEL ÁNGEL MORATAYA PENADO

ASESOR METODOLÓGICO

LIC. RENÉ HUMBERTO RUÍZ RAMÓN

DEDICATORIAS

A Dios Todopoderoso por la oportunidad de llegar a culminar una de las metas más importantes de mi vida; a mis padres Oscar Salvador Bolaines Ortega y María Magdalena Portillo por siempre estar a mi lado apoyándome para seguir adelante, a mi hermana Carolina Bolaines, por estar siempre presente ofreciéndome su ayuda y cariño, a todos los catedráticos que me trasmitieron sus conocimientos durante la carrera, a mis amistades, compañeros y a las personas importantes de mi vida que siempre estuvieron presente en el momento oportuno. A todos infinitas gracias por su paciencia, amor y comprensión.

Rocío Elizabeth Bolaines Portillo

Especial dedicatoria a los seres que mas han influido en mi desarrollo profesional: DIOS fuentes de toda sabiduría e inteligencia, a mis padres por su inmenso apoyo y a todos los compañeros que siempre estuvieron ahí dispuestos y pacientes para brindar su ayuda.

Oscar René Gómez Hernández.

Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio. A mis padres Reyna Margarita Páiz y Carlos Ernesto Martínez, por darme la vida, quererme, creer en mí, porque siempre me apoyaron y por darme una carrera para mi futuro, todo esto se lo debo a ustedes; A mi hermana, Leyda Isolina Martínez, por estar conmigo y apoyarme siempre, y todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

Ernesto Scarlett Martínez Páiz

“PROPUESTA DE UNA GUIA DE EVALUACION DE SEGURIDAD INFORMATICA A LAS EMPRESAS DISTRIBUIDORAS DE TELEFONIA MOVIL DE LA CIUDAD DE SAN MIGUEL.”

INDICE

CAPITULO III
MARCO REFERENCIAL

CAPITULO VI
ANALISIS E INTERPRETACIN DE RESULTADOS

CAPITULO V

PROPUESTA DE LA GUIA DE EVALUACION DE SEGURIDAD INFORMATICA EN LAS EMPRESAS DISTRIBUIDORAS DE TELEFONIA CELULAR DE LA CIUDAD DE SAN MIGUEL.

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

INTRODUCCIÓN

Para muchos la Seguridad Informática sigue siendo el área principal a auditar para los Auditores de Sistemas, debido a la vulnerabilidad de los Sistemas Informáticos.

Cada día es mayor la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de las fallas, los accesos no autorizados, la revelación de la información, y otras incidencias, tienen un impacto mucho mayor que hace unos años: de ahí la necesidad de protecciones adecuadas que se evaluarán o recomendarán en la auditoría de seguridad informática, es decir; la seguridad física y seguridad lógica.

La seguridad informática es el proceso en la auditoría de sistemas que pretende verificar el cumplimiento de los siguientes aspectos: control de datos, políticas de respaldo, políticas y procedimientos, políticas de revisión de bitácoras, control de las licencias de software, control de medios de almacenamiento masivo, control del mantenimiento y evaluación de la configuración del sistema de cómputo. Además de elementos como protección física, aire acondicionado, suministros de energía, detectores de agua y humo, cableado polarizado, extintores, rutas de acceso, manuales, mantenimiento, alarmas contra robos, contra incendios, inundaciones, etc.

El presente trabajo se ha dividido en seis capítulos los cuales se describen a continuación.

En el Capítulo I se hace un breve análisis sobre el Planteamiento del Problema, Enunciado del Problema, Justificación de la Investigación, la Delimitación de la investigación y los Objetivos de la Investigación.

En el Capítulo II se desarrolla la Metodología de Investigación, que contiene el Tipo de Investigación, la Determinación del Universo y la Muestra, las Técnicas de Recolección de datos, los Instrumentos de Recolección de datos, la Presentación de la Información.

En el Capítulo III se presenta el Marco Referencial, este se encuentra dividido en cuatro partes: Marco Histórico, Marco Conceptual, Marco Legal y Marco Técnico. Para la elaboración de este capítulo se tomaron como base aspectos tales como: Generalidades, Antecedentes, Aspectos Legales, Normativa Técnica, entre otros puntos que son de mucha importancia, que permitirán obtener conceptos básicos para el entendimiento del trabajo.

El Capítulo IV se encuentra el Análisis e Interpretación de resultados el cual contiene los datos de los análisis obtenidos de la investigación, presentación de resultados, interpretación y presentación gráfica.

El Capítulo V, contiene la Propuesta de una Guía de Evaluación de Seguridad Informática en las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel, la cual comprende Descripción de la guía, Objetivos y las Etapas de Evaluación de Auditoría de Seguridad Informática.

En el Capítulo VI se presentan las Conclusiones y Recomendaciones, obtenidas a través de la investigación.

CAPITULO I. FORMULACION DEL PROBLEMA

1. FORMULACION DEL PROBLEMA

1.1 PLANTEMIENTO DEL PROBLEMA

En la actualidad las todas las empresas se encuentran sometidas a un constante desarrollo como resultado de las nuevas exigencias del mercado en que se desarrollan, ya que para ser una empresa competitiva y brindar a sus clientes servicios de alta calidad así como también dar cumplimiento a las exigencias legales y normativas a las que se encuentran sometidas, deben estar a la vanguardia en la utilización de nuevas tecnologías, modernización de su infraestructura, innovación de los sistemas de información etc.

El proceso de generar información para la toma de decisiones requiere la interacción de una serie de elementos que integran un sistema. Todos los elementos están interrelacionados y por consecuente comparten información sumamente importante y confidencial que no debe traspasar las barreras de seguridad informática con que cuente una empresa, esto para evitar que terceras personas totalmente ajenas a las operaciones no tengan acceso a estos tipos de información.

Las Empresas distribuidoras de Telefonía Móvil en la ciudad de San Miguel generan día a día grandes volúmenes de datos operativos que son concentrados en Sistemas Informáticos para su procesamiento, almacenamiento y salida en de estos en forma de información útil para la toma de decisiones. Por lo tanto estas empresas poseen mayores riesgos en las diferentes áreas con las que cuentan, entre ellos el riesgo informático.

Uno de los activos más vulnerables para las empresas es su información organizativa y financiera, ya que esta expuesta a que terceras personas con intenciones malignas puedan acceder a ella para cometer delitos informáticos como espionajes, fraudes, etc.

Generar información a través de un sistema automatizado hace vulnerable a las empresas respecto de que esta se filtre hacia terceros. Un ejemplo peculiar es que alguien acceda a las cuentas bancarias de las empresas y cometa estafa informática. Otro caso puede ser la obtención de listas de clientes o proveedores.

La Auditoria de Sistemas consiste en la evaluación, verificación y monitoreo de los procesos informáticos y del ambiente que contribuye a generar información en una empresa; por lo tanto, busca identificar aquellos aspectos de vulnerabilidad de tales sistemas, todo con la finalidad de evitar, prevenir o corregir las desviaciones encontradas, específicamente al evaluar el área de la Seguridad Física y Lógica , para prevenir que se dañen los sistemas informáticos con que cuentan, ya sean éstos daños por desastres naturales, incendios, acciones hostiles(sabotaje, robo, fraude), etc.

Es indispensable mencionar que en dichas empresas no se le ha dado la importancia que requiere una evaluación de la Seguridad Informática(Seguridad Física y Seguridad Lógica) y las actividades que se realizan con los Sistemas de Información Computarizados, que dé lugar a aumentar el valor y mejorar las operaciones de la empresa. Así como también ayudar a que la empresa cumpla con sus objetivos mediante la aplicación de enfoques sistemáticos, modernos y disciplinados para llevar a cabo las respectivas evaluaciones de la Seguridad Física y Lógica y fortalecer la efectividad de los procesos que se llevan a cabo en dichos sistemas informáticos.

Por ello, es necesario que exista Auditoría de Sistemas en las empresas y que el producto final de la evaluación sea un informe que contenga todos aquellos aspectos que deben mejorarse del entorno informático de las empresas, emitido por un Auditor Independiente, que cuente con los conocimientos idóneos, y que a través de las debilidades proponga mejoras en las deficiencias encontradas.

1.2 ENUNCIADO DEL PROBLEMA

¿ES NECESARIA LA PROPUESTA DE UNA GUÍA DE EVALUACIÓN DE SEGURIDAD INFORMÁTICA EN LAS EMPRESAS DISTRIBUIDORAS DE TELEFONÍA MÓVIL DE LA CIUDAD DE SAN MIGUEL?

1.3 JUSTIFICACION DE LA INVESTIGACION

La globalización es un fenómeno que ha llevado a los países y organizaciones a hacer cambios significativos en su estructura y funcionamiento, las empresas no se han quedado atrás y han decidido hacer esos cambios principalmente tecnológicos para el mejor funcionamiento de sus actividades comerciales y para el adecuado procesamiento de información que servirá para la toma de decisiones.

Surge entonces la necesidad de que las empresas cuenten con Auditoría de Sistemas que les permita evaluar de manera confiable la Seguridad Física y Seguridad Lógica, ya que aspectos como los controles de procesamiento, los cuales pueden producir errores en la entrada y salida de información que pueden afectar de alguna manera el funcionamiento de las empresas en su totalidad. Por ello se vuelve una necesidad que dichas empresas cuenten con una Guía de Evaluación de la Seguridad Informática, los cuales ayudarán a saber la confiabilidad de la información que es procesada en forma automatizada principalmente en las empresas en las que su herramienta principal para operar son los sistemas de información; ya que debido a los riesgos informáticos las empresas pueden inducirse a la no continuidad de sus actividades e inclusive llegar a la quiebra, por lo vulnerable que son los sistemas automatizados.

Una Guía para Auditar la Seguridad Informática es novedosa, porque las Empresas Distribuidoras de Telefonía Celular de la ciudad de San Miguel no cuentan con una que les permita evaluar de forma sistemática las medidas de Seguridad Informática, es decir, solamente se llevan a cabo de forma empírica pero no técnicamente por el informático de las empresas en estudio, y en algunos casos no se ha hecho ningún

tipo de evaluación de dicha seguridad por no contar con un instrumento que les permita llevarla a cabo; además, es novedoso porque no se ha realizado un estudio de esta naturaleza en la zona, debido a la poca práctica de auditoría de sistemas por las empresas y por los despachos contables que prestan servicios de auditoría.

Por ello, es necesario evaluar el entorno de los sistemas informáticos, las medidas de seguridad que las empresas implementan para la protección de los equipos, la información producida y almacenada dentro de ellos. A lo que se le denomina Seguridad Física, es decir todas las barreras visibles para la protección, desde la ubicación de los establecimientos hasta el almacenamiento de la información ya procesada.

También se vuelve una necesidad mayor evaluar la ejecución de los sistemas y la confiabilidad de los datos dentro de ellos, la protección a la información, las medidas de seguridad en cuanto al acceso a los módulos que conforman los sistemas, la entrada de los datos, el procesamiento y la salida de éstos. Lo que se conoce como Seguridad Lógica de dichos sistemas.

Es parte esencial para las empresas que producen transacciones de forma automatizada y en donde los sistemas informáticos son una base fundamental para la operacionalización de sus actividades, en este caso las Empresas Distribuidoras de Telefonía Móvil específicamente de la Ciudad de San Miguel.

El tema en estudio es factible porque las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel proporcionarán toda la información que sea relevante considerar para el diseño de la Guía de evaluación de la Seguridad Informática y la disposición a que se realice en sus establecimientos la ejecución del trabajo, también porque se cuentan con las fuentes de información necesarias es decir, tesis, materiales, manuales, sitios web y toda la teoría relacionada a las temáticas incluidas.

La importancia de diseñar y proponer una Guía de Evaluación de Seguridad Informática a las Empresas de Telefonía Móvil de la ciudad de San Miguel es que resultará un instrumento que será de utilidad social porque servirá como guía para evaluar aspectos que midan las deficiencias en el desarrollo de las actividades normales de tales empresas, las cuales posteriormente deberán ser corregidas para operar de forma oportuna y logrando optimización de recursos, también servirá para medir las fortalezas que pueden ser aprovechadas para un mejor funcionamiento y competitividad dentro del mercado.

Además, con la implementación de dicha propuesta se verán beneficiadas las Empresas Distribuidoras de Telefonía Celular de la ciudad de San Miguel, los despachos contables que realizan Auditorías Especializadas como Auditoría de Sistemas en la ciudad de San Miguel y los estudiantes de la carrera de Contaduría Pública que la pueden utilizar como herramienta para la realización de casos prácticos de dicha Auditoría.

1.4 DELIMITACION

1.4.1 DELIMITACION ESPACIAL

La investigación se realizará a las cuatro Empresas Distribuidoras de Telefonía Celular de la ciudad de San Miguel, en las siguientes direcciones:

- Mundo Celular de El Salvador S.A de C.V, ubicada en Avenida Roosevelt Norte número 401, San Miguel
- Celular Star S.A de C.V, ubicada en Avenida Roosevelt Sur, Barrio San Nicolás, número 301, San Miguel.
- Celular Boutique, ubicada en Avenida Gerardo Barrios y Décima Calle Poniente número 507, Barrio San Francisco, San Miguel.
- DISERVI S.A de C.V, ubicada en Plaza Floresta, local número 2, San Miguel.

1.4.2 DELIMITACION TEMPORAL

La investigación sobre la Propuesta de una Guía de Evaluación de Seguridad Informática en las empresas distribuidoras de la ciudad de San Miguel, se hará en el período de Marzo a Septiembre de 2012

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

- Proponer una Guía de evaluación de Seguridad Informática a las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel.

1.5.2 OBJETIVOS ESPECIFICOS

- Diseñar la Planeación para evaluar Seguridad Física y Seguridad Lógica.

- Aplicar procedimientos para la obtención de evidencia en la evaluación de Seguridad Física y Seguridad Lógica.

- Elaborar informe de la evaluación de Seguridad Física y Seguridad Lógica.

CAPITULO II. METODOLOGIA DE LA INVESTIGACION

2. METODOLOGIA DE LA INVESTIGACION

2.1 TIPO DE ESTUDIO

En el desarrollo de la presente investigación se utilizará el Método Inductivo-Hipotético porque parte de datos particulares aceptados como válidos para llegar a una conclusión de tipo general y es de metodología cualitativa-cuantitativa porque se combinarán las técnicas de encuesta y entrevista, consiste en la interpretación del sentido subjetivo de la conducta, ósea, de lo que las personas piensan. Y la cuantitativa, que pretende medir el fenómeno y explicarlo. Utilizando técnicas estadísticas; en la cual para la determinación del número de sujetos a encuestar fue de forma arbitraria.[1]

La investigación se fundamentara en datos obtenidos de fuentes primarias "Son todas aquellas de las cuales se obtiene información directa, es decir, de donde se origina la información."

Información de fuentes secundarias "Es aquella información que se obtiene sobre el tema por investigar, pero que no son una fuente de la situación actual de los hechos del objeto de estudio si no que sirven como referencia. Dentro de las principales fuentes de información secundaria se dispone de libros, revistas, documentos escritos, documentales, noticieros y medios de información." Todo esto permitirá someter a prueba las hipótesis planteadas para determinar la inexistencia de evaluación de la Seguridad Informática en las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel.

[1] Ruiz Olabuenaga, José I. Métodos de Investigación Cualitativa, 1989

De esta manera los resultados de la investigación permitirán elaborar la Propuesta de una Guía de Evaluación de Seguridad Informática a las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel.

2.2 DETERMINACION DEL UNIVERSO Y DE LA MUESTRA

Para el trabajo de campo en las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel, "La población se refiere a la totalidad de los elementos que poseen las principales características objeto de análisis y sus valores son conocidos como parámetros."[2] La cual es finita, debido a esto "La muestra no es más que una parte del todo que llamamos universo y que sirve para representarlo".[3] En la presente investigación se tomara una muestra no probabilística la cual se describe como una muestra dirigida, en donde la selección de elementos depende del criterio del investigador. Sus resultados son generalizables a la muestra en sí. No son generalizables a una población.

Por lo anterior la muestra a evaluar estará constituida por: un Gerente, un Auditor Interno, y un Informático de cada una de las empresas en estudio que son cuatro, haciendo un total de 12 personas.

2.3 TECNICAS DE RECOLECCION DE DATOS

2.3.1 ENCUESTA

Para llevar a cabo el desarrollo del presente trabajo se obtendrá información de los sujetos de estudio a través de una encuesta "técnica que consiste en recopilar información sobre parte de la población denominada muestra", que en este caso será

[2] Rojas soriano, Raúl. Ídem, Pág. 30
[3] Rojas soriano, Raúl. "Guía para realizar Investigaciones Sociales", P y V Editores, México, 40ª Edición 2004, Pág. 286

aplicada a tres responsables de cada una de las empresas en estudio, a la gerencia, auditor interno, y principalmente al Jefe de Informática.

2.4 INSTRUMENTOS DE RECOLECCION DE DATOS

Para llevar a cabo la recopilación de la información de la investigación, se tomará como instrumento el cuestionario, la entrevista y fichas bibliográficas.[4]

2.4.1 CUESTIONARIO

En el cual se formularan preguntas de carácter cerrado, y contendrá preguntas que representarán la fiabilidad de la empresa, donde se mencionarán alternativas de respuestas a la pregunta, que serán fácilmente contestadas por el entrevistado; con el fin de obtener datos para el trabajo de investigación.

2.4.2 ENTREVISTA

En esta se harán preguntas de carácter abierto, es decir para que los entrevistados respondan de forma libre, de acuerdo a los conocimientos y noción que se tenga sobre los temas en cuestión con la finalidad de conocer más detalladamente sobre el manejo de los procesos y la situación actual en las instituciones evaluadas, en cuanto a Seguridad Informática.

2.4.3 FICHA BIBLIOGRÁFICA

Instrumento utilizado para recopilar datos de las normas legales, administrativas, contables, de auditoría, de libros, revistas, periódicos, trabajos de investigación e Internet relacionados con el trabajo de investigación.

[4] Rojas Soriano, Raúl. Guía para realizar Investigaciones Sociales. P y V Editores, México, 30ª Edición 1998.

2.5 PRESENTACION DE LA INFORMACION

2.5.1 TÉCNICAS DE ANÁLISIS DE DATOS:

Los datos se presentarán de forma narrativa para la entrevista y para el cuestionario se presentará en cuadros y gráficos de pastel y las respuestas serán objeto de análisis e interpretación auxiliándose de las siguientes técnicas:

- Análisis documental
- Conciliación de datos
- Representación gráfica
- Interpretación de las respuestas
- Indagación

2.5.2 TÉCNICAS DE PROCESAMIENTO DE DATOS:

En el trabajo de investigación se procesaran los datos con apoyo de las diferentes fuentes, por intermedio de las siguientes técnicas:

- Ordenamiento y clasificación
- Registro manual
- Proceso computarizado con Word

2.5.3 VALIDACION DE DATOS:

Consiste en dar sustento de la veracidad de los datos obtenidos, a través de:

- Confrontación de datos.
- Triangulación de datos.

CAPITULO III. MARCO REFERENCIAL

3. MARCO REFERENCIAL

3.1 MARCO HISTORICO

3.1.1 ANTECEDENTES DE LA AUDITORIA

3.1.1.1 ANTECEDENTES DE LA AUDITORIA A NIVEL MUNDIAL

La auditoría como profesión fue reconocida por primera vez bajo la ley británica de sociedades anónimas en 1862 y su reconocimiento general tuvo lugar durante el periodo de mandato de la Ley, un sistema metódico y normalizado de contabilidad era deseable para una adecuada información y para la prevención del fraude.

Desde 1862 hasta 1905, la profesión de la Auditoria creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. La primera Asociación en Estados Unidos fue la Asociación Americana de Contadores Públicos, se fundó en 1887, la Escuela de Comercio, Contabilidad y Finanzas en el año 1900, la Federación de Sociedades de Contadores Públicos en 1902 y en 1905 la Federación de Sociedades de Contadores Públicos se fusionó con la Asociación Americana de Contadores Públicos; dando como resultado lo que hasta hace poco es El Instituto Americano de Contadores Públicos.

En Inglaterra se hizo hincapié en cuanto a la detección del fraude como objetivo primordial de la auditoria, a los estudiantes se les enseñaba que los objetivos primordiales de la Auditoria eran: La detección y prevención del fraude, La detección y prevención de errores; cerciorarse de la condición financiera y de las ganancias de una empresa.

La auditoría como actividad de control de la función económica financiera de cualquier empresa, surge en el momento en que la propiedad de los recursos financieros asignados a usos productivos ya no estaba en manos de una sola persona; en consecuencia del desarrollo extraordinario de las sociedades anónimas como

forma jurídica de empresa surgió la necesidad de que la información contable facilitada a los accionistas y a los acreedores respondiera realmente a la situación patrimonial y económica-financiera de la empresa.

Hasta inicios del siglo XX el trabajo de los auditores se concentraba principalmente en el balance que los empresarios tenían que presentar a sus banqueros para solicitar préstamos.

Fue a partir de 1900, cuando la Auditoria o Contaduría Pública se le asignó el objetivo de analizar la rectitud de los estados financieros. Después de esa fecha la función del auditor como detective fue quedando atrás y el objetivo principal del trabajo pasó a ser la determinación de la rectitud o razonabilidad que los Estados Financieros reflejaban la situación patrimonial y financiera de la empresa; el resultado de las operaciones a cargo de la auditoría financiera que fue pionera en este campo.

Durante muchas décadas la auditoria permaneció unida a la detección y prevención de fraude y de las irregularidades; pero la evolución económica y social de las últimas décadas ha traído consigo cambios sustanciales en el campo de la auditoria. Con el devenir del tiempo y en una época más reciente surge la auditoria operacional o de gestión, la auditoria gubernamental, la auditoria administrativa.

En los últimos tiempos surgen ya auditorias más específicas como la Auditoria Social, la Auditoria Informática y Auditoria Ambiental; cuyo alcance y objetivos va más allá de las cifras de estados financieros, como la Auditoria de Gestión y su enfoque más conocido de Modelo de Control Interno según COSO que mide el desempeño de la administración a través de factores internos como el ambiente de control, la evaluación de riesgos, las actividades de control, entre otros que orientan a

elementos importantes para la auditoria de riesgos que vulneran los objetivos empresariales.[5]

3.1.1.2 ANTECEDENTES DE LA AUDITORIA EN EL SALVADOR

Un acontecimiento que tuvo importancia e influyó para la profesión de Contador Público se reconociera oficialmente fue la contratación por parte del Ministerio de Hacienda y Crédito, de una Firma de Auditores de origen inglés para estudiar la Contaduría Pública en El Salvador y proponer los medios para corregir sus deficiencias. Esta firma fue la denominada "Layton Bennet Chiene and Tait" la cual, al concluir su trabajo y presentar su informe se marchó a su país de origen y dos de los auditores de esa firma se quedaron en el país ejerciendo la Contaduría Pública en forma independiente fueron ellos: William Braim y Lyon Sullivan, quienes fueron los únicos que durante la década de 1929, 1939 ejercieron de manera profesional la contaduría en El Salvador.

En 1930 un grupo de colegas llenos de optimismo y entusiasmo propios de la juventud de ese tiempo, deseosos de mejorar sus estudios capacidades y desarrollo profesional; se reunieron en el local de la sociedad de empleados de comercio ahora, Asociación de Ejecutivo Profesionales y Empresarios de El Salvador "ASEPES" el cinco de octubre de 1930, a invitación del colega Carlos Valmore Martínez (Q.E.P.E.) Para razonar sobre la conveniencia de organizar una gremial de contadores, y oídas de opiniones de varios concurrentes acordaron unánimemente dar por fundada la denominación de " *Asociación de Contadores de El Salvador"* que posteriormente se modifico a "*Corporación de Contadores de El Salvador".*

En El Salvador se institucionalizó la profesión de la Contaduría Pública a mediados de la cuarta década del siglo XX, para culminar con el Decreto Legislativo No. 57 publicado en el Diario Oficial No. 223 del año 1940; nombrándose pocos días después la primera Junta Directiva de aquel entonces, Consejo Nacional de

[5] Auditoría un Enfoque Integral, décima edición.

Contadores Públicos, iniciándose así el Ejercicio Profesional de la Contaduría Pública.

En el año 1965, se concedió autorización para que las personas con títulos de Tenedor de Libros mediante dos años de estudios pudieran obtener el título de Contador, y así poder ingresar a las Universidades.

En los años 1969 a 1971 la Universidad de El Salvador fundó la Escuela de Contaduría Pública, formando parte de la Facultad de Ciencias Económicas con la finalidad de formar profesionales en la carrera de la Contaduría Pública y Auditoria, ya que quienes ejercían la profesión eran Contadores Públicos Certificados autorizados por la Corporación de Contadores de El Salvador.

La base legal del ejercicio de la Contaduría y Auditoria en el País es considerada en el Código de Comercio artículo No. 235 que entró en vigencia el 1 de abril de 1971.

El 31 de Octubre de 1997 se fundó el Instituto Salvadoreño de Contadores Públicos, el cual nace por acta notarial de fusión otorgada por el Colegio de Contadores Públicos de El Salvador, La Asociación de Contadores Públicos de El Salvador y el Colegio Salvadoreño de Contadores Públicos.

El 26 de enero de 2000 se emite Decreto Legislativo No.826 el cual incluye las reformas de algunos artículos del Código de Comercio, en la misma fecha se emitió Decreto Legislativo

No.828 dando origen a la primera Ley que regularía el ejercicio del Contador Publico; titulada Ley Reguladora del Ejercicio de la Contaduría. Actualmente en El Salvador, el Estado delega en las instituciones de educación superior (universidades estatales y privadas reconocidas oficialmente por el Ministerio de Educación), la facultad de expedir dicho título a quienes hayan cumplido los requisitos académicos necesarios, quedando sujeto el ejercicio de la profesión contable independiente al registro respectivo ante el Consejo de Vigilancia de la Contaduría Pública, conforme a lo establecido en el Art. 290 del Código de Comercio.

El 15 de diciembre de 2000, se estableció que la elaboración y presentación de la información financiera de las empresas en base a Normas Internacionales de Contabilidad, serian de carácter obligatorio a partir del 1 de enero de 2002.

3.1.1.3 ANTECEDENTES DE LA AUDITORÍA DE SISTEMAS.

La palabra auditoría viene del latín "auditorius" y de esta proviene auditor, que 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 el ejecutivo, encaminado a un objetivo específico en el ambiente computacional y los sistemas.

La mayor preocupación de los auditores hoy en día, en especial los que no son auditores de sistemas de información, y algunos de éstos también, es poder utilizar el computador para realizar las auditorías "por dentro del mismo", en la revisión de los datos que contiene; y no se han dado cuenta todavía, (a pesar de estar tan avanzada esta especialización, tanto en métodos, técnicas, pronunciamientos, tecnología, y herramientas, así como en el tiempo), que ésta tarea es muy sencilla y que, más que todo es parte sustancial de la Auditoría Financiera.[6]

3.1.1.4 ANTECEDENTES DE LA ASOCIACION DE AUDITORIA Y CONTROL DE SISTEMAS DE LA INFORMACION (ISACA)

[6]NARANJO, ALICE. "Auditoria de Sistemas". http://www.monografias.com

Information Systems Audit and Control Association (ISACA) es una asociación profesional internacional cuyo objetivo principal es la promoción de la capacitación profesional para el desarrollo y la optimización del conocimiento y las habilidades relacionadas con la auditoria y la seguridad en el campo de las Tecnologías de la Información y las Comunicaciones (TICs).

ISACA comenzó en 1967, cuando un pequeño grupo de personas con trabajos similares—auditar controles en los sistemas computacionales que se estaban haciendo cada vez más críticos para las operaciones de sus respectivas organizaciones—se sentaron a discutir la necesidad de tener una fuente centralizada de información y guías en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de *EDP Auditors Association* (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TI.

Hoy, los miembros de ISACA – más de 95,000 en todo el mundo – se caracterizan por su diversidad. Los miembros viven y trabajan en más de 160 países y cubren una variedad de puestos profesionales relacionados con TI – sólo por nombrar algunos ejemplos, auditor de SI, consultor, profesional de la educación, profesional de seguridad de SI, regulador, director ejecutivo de información y auditor interno. Algunos son nuevos en el campo, otros están en niveles medios de la gerencia y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, firmas de auditoria y consultoría, gobierno y sector público, servicios públicos y manufactura. Esta diversidad permite que los miembros aprendan unos de otros, e intercambien puntos de vista comunes sobre una variedad de tópicos profesionales. Esta ha sido considerada durante mucho tiempo como una de las fortalezas de ISACA. Previamente conocida como la Asociación de Auditoria y Control de Sistemas de la Información, ISACA ahora

identificada ya por su acrónimo, para reflejar el amplio rango de profesionales del gobierno de las TI a los que sirve.[7]

3.1.1.5 ANTECEDENTES DE LA SEGURIDAD INFORMATICA.

Desde tiempos inmemorables el hombre ha resguardado y protegido con celo sus conocimientos debido a la ventaja y poder que éste le producía sobre otros hombres o sociedades.

En la antigüedad surgen las bibliotecas, lugares donde se podía resguardar la información para trasmitirla y para evitar que otros la obtuvieran, dando así algunas de las primeras muestras de protección de la información.

Sun Tzu en El arte de la guerra y Nicolás Maquiavelo en El Príncipe señalan la importancia de la información sobre los adversarios y el cabal conocimiento de sus propósitos para la toma de decisiones.

Durante la Segunda Guerra Mundial se crean la mayoría de los servicios de inteligencia del mundo con el fin de obtener información valiosa e influyente, creándose grandes redes de espionaje. Como forma de protección surge la contrainteligencia.

Con el devenir de los años al incrementarse el alcance de la tecnología, el cuidado de la información se ha vuelto crucial para los hombres, las organizaciones y las sociedades.

3.1.1.6 ANTECEDENTES DE LA SEGURIDAD FÍSICA Y ELECTRÓNICA.

La historia de la seguridad inicia siempre con una materia prima para su existencia: un riesgo, un peligro, una amenaza. En este sentido, el escenario de la seguridad física se desarrolla en el contexto de la guerra contra un enemigo, que no busca otra cosa que vulnerar las estrategias de control y contención, entre otras, que tiene el objetivo atacado, para apoderarse de éste.

[7] www.isaca.com

De acuerdo con los teóricos, existen cuatro categorías de seguridad física:

a) **las obstrucciones físicas,**
b) **las técnicas de vigilancia,**
c) **los sistemas de inteligencia y**
d) **los guardias o personal de seguridad.**

Estas cuatro categorías representan la caracterización de la seguridad misma en el mundo tangible, que aún hoy por hoy existen y que cuentan, todas ellas con su referente en el mundo lógico.

3.1.1.7 ANTECEDENTES DE LA SEGURIDAD LÓGICA Y LA SEGURIDAD DE LA INFORMACIÓN.

La evolución normal del concepto de seguridad en una sociedad de la información y el conocimiento, hace que las estrategias de seguridad de la antigüedad cobren vida en un mundo regido por los "bits y bytes." Todas las condiciones de seguridad analizadas en el aparte anterior tienen sus equivalentes en el mundo de la informática y la tecnología.

Si en la antigüedad los activos a proteger eran de condición tangible y real, como el oro, los semovientes y las personalidades, entre otras, hoy el activo fundamental se llama información. Esa pieza de datos procesados y analizados que constituyen la nueva moneda y pasaporte para vivir en la sociedad actual. La información se convierte en el activo de carácter intangible (por aquello que no es posible verlo a simple vista en su estado natural) y susceptible de manipulación, que hace que cada uno de sus dueños muestre interés en su protección y control.[8]

[8] AGUIRRE, JORGE. "Seguridad Informática y Criptografía". Ed. Universidad Politécnica de Madrid. Versión 4.1. 2006.

3.1.2 ANTECEDENTES DE LA TELEFONIA CELULAR

3.1.2.1 ANTECEDENTES DE LA TELEFONIA CELULAR A NIVEL MUNDIAL

Aunque hoy en día pueda parecer extraño, el teléfono es un invento que tardó bastante tiempo en consolidarse, la rápida implantación y difusión del telégrafo hizo que a priori no existiera un excesivo interés por investigar un nuevo aparato que permitiera transmitir sonidos a distancia.

El interés de Bell por el teléfono es una historia bastante curiosa. Mientras investigaba un "telégrafo armónico" que transmitiera mensajes múltiples por un mismo hilo y pudiera ser válido para los sordomudos (el gran objetivo de Bell era descubrir una aparato que le permitiera hablar a su esposa sordomuda), Bell escucha la vibración de una lengüeta metálica. Muy pronto se da cuenta de que una lámina adherida a un electroimán es capaz de emitir no sólo sonidos primarios sino también los de frecuencia múltiple.

Desde que Alexander Graham Bell invento el teléfono y registró la patente en 1876, no se imaginó que sería parte de un estilo de vida, similar a las series de tiras cómicas. Y que aún mejor se convertiría en una necesidad.[9]

3.1.2.2 ANTECEDENTES DE LA TELEFONIA CELULAR EN EL SALVADOR

La telefonía se remonta a tiempos pasados desde que en El Salvador se importaron los primeros teléfonos por el señor Mauricio Duke en el año de 1882 y después el desarrollo de los medios de comunicación se exhibe ante nosotros como un proceso vertiginoso o como manifestación del desarrollo técnico, de alcance mundial y con posibilidades de progreso continuo. La velocidad con que suceden los intercambios y flujos de mensajes, es lo que se identifica hoy en día como una corriente de

[9]Tesis de Telefonía Celular en El Salvador, www.wikipedia.com

información.

Las telecomunicaciones han experimentado un crecimiento extraordinario, al punto de pasar al segundo lugar como el sector más dinámico de la economía desde 1998.
La capacidad máxima que tiene la red para móviles es de 10 millones, según la SIGET. Según la Superintendencia General de Electricidad y Telecomunicaciones (SIGET), en 2007 la cantidad de teléfonos móviles comercialmente activos en el país llego a 6.2 millones. Es un crecimiento bastante rápido el que se ha tenido en las líneas celulares.

Desde junio de 2005 se cuentan cuatro empresas principales de telefonía móvil y una incorporada más reciente, estas empresas participan en el mercado y todas utilizan tecnología digital Global System Mobile Communication (GSM).
La competencia es muy fuerte entre ellas, ya que ofrecen una variedad de planes para atraer a diferentes segmentos del mercado de contratos (individuales, familiares, amigos, corporativos), tarjetas de prepago de diferentes montos; por otra parte, otorgan una variedad de servicios complementarios a la comunicación verbal local, como roaming, mensajes de texto, envío de 20 fotos y envío de correo electrónico. Cada compañía ha sido muy agresiva con respecto a la ampliación de la red de puntos de venta y cobro de los productos y servicios. [10]

3.1.2.3 ANTECEDENTES DE LAS EMPRESAS DE TELEFONIA CELULAR EN EL SALVADOR:

- **CTE-TELECOM-PERSONAL.**

Empezó a ofrecer los servicios de telefonía móvil en 1999, y fue la tercera empresa en el mercado, además del servicio de telefonía fija.
Cuando pasó a manos de América Móvil, sus programas de telefonía móvil fueron

[10] Tesis de Empresas de Telefonía Celular en El Salvador, www.wikipedia

más agresivos, ampliando su cuota de mercado, logrando con ello el primer lugar en líneas en junio de 2005.

- **TELEMÓVIL DE EL SALVADOR.**

Fue la primera empresa del país de capital salvadoreño y con una concesión única, la cual finalizó antes de la privatización. Cuando inició este proceso vendió acciones al grupo inversor Millicom, que adquirió todas las acciones a principios de la presente década. La fuerte competencia presionó a que Millicom fuera la última en migrar a la tecnología GSM (2004), y en 2005 fue relegada al segundo lugar en líneas móviles, superada por Telecom (América Móvil). Luego de que recientemente anunciara sus intenciones de vender todas sus operaciones en América Latina, recibió ofertas de América Móvil y Telefónica, sin llegar a un acuerdo con ninguna.

Esta venta en el mercado salvadoreño podría incidir en una mayor concentración en telefonía móvil.

- **TELEFÓNICA MÓVILES EL SALVADOR.**

Fue la segunda empresa de telecomunicaciones en el país (1998) y ocupaba el segundo lugar en líneas a junio 2005. En el 2004 realizó la migración completa a GSM. Si bien la empresa tiene un apalancamiento de su casa matriz en España, a fines de 2004 experimentaba una "quiebra técnica", de acuerdo con un informe de la calificadora de riesgo Equilibrium (abril 2005).

- **DIGICEL DE EL SALVADOR.**

Fue la cuarta empresa en ingresar al mercado en 2002, y su capital está formado por inversionistas de Estados Unidos y El Salvador. Para competir en el mercado, ofrece cobrar el segundo exacto, a diferencia del resto de operadores que cobran el minuto. Por otra parte, está orientada al segmento de mercado urbano y a personas que llaman a Estados Unidos (en donde viven aproximadamente dos millones de salvadoreños).

- **INTELFON DE EL SALVADOR.**

Fue la última empresa que ingresó al mercado, en octubre 2005, y está compuesta por capital salvadoreño y panameño. Dicha firma ofrece el servicio combinado de radio digital y celular digital en un mismo aparato, utilizando la tecnología IDEM de Motorola. Su nicho de mercado inicialmente está identificado para las flotas de empresas.

3.1.2.4 ANTECEDENTES DE LAS EMPRESA DISTRIBUIDORAS DE TELEFONIA CELULAR DE LA CIUDAD DE SAN MIGUEL.

En la ciudad de San Miguel, según estudios realizados en 2012 se cuentan con los siguientes Distribuidores Autorizados de los Operadores Telefónicos.

- **MUNDO CELULAR DE EL SALVADOR S.A. DE C.V.**

Ubicada en Avenida Roosevelt Norte número 401, la cual consta con diferentes Sucursales en el Centro y Metrocentro de la Ciudad de San Miguel; inicio operaciones el 30 de marzo de 2000, ofreciendo los servicios de venta de saldo, tarjetas prepago, teléfonos, accesorios para celulares, cables, reparación de celulares, etc.

Esta empresa es distribuidora de las Compañías: **CTE-TELECOM-PERSONAL (CLARO), DIGICEL DE EL SALVADOR (DIGICEL)**

- **CELULAR STAR, S.A. DE C.V.**

Ubicada en Avenida Roosevelt Sur, Barrio San Nicolás, número 301, la cual tiene 10 Sucursales que se encuentran dentro y fuera del Departamento de San Miguel, inició sus operaciones el 06 de Mayo de 2008, con los servicios de telefonía, tarjetas prepago, accesorios para celulares, venta de saldo, reparación de celulares, entre otros.

Esta empresa es distribuidora de la Compañía: **TELEMÓVIL DE EL SALVADOR (TIGO)**

- **GUTIÉRREZ HERRERA, S. A. DE C.V.**

Conocida por su nombre comercial: **CELULAR BOUTIQUE,** la cual tiene 16 Sucursales, ubicadas dentro y fuera de la Ciudad de San Miguel, la Casa Matriz se encuentra en la Avenida Gerardo Barrios y Décima Calle Poniente número 507, Barrio San Francisco, inicio operaciones el 01 de Marzo de 2000, ofrece servicios de reparación de celulares, venta de teléfonos, tarjetas prepago, saldo, accesorios, etc.
Esta empresa es distribuidora de la Compañía: **TELEMÓVIL DE EL SALVADOR (TIGO)**

- **DISTRIBUIDORA DE SERVICIOS, S.A. DE C.V. (DISERVI, S.A. DE C.V.)**

Inicio sus operaciones en el mes de Septiembre de 2010, ubicada en Plaza Floresta, local número 2, con los servicios de telefonía, tarjetas prepago, accesorios para celulares, venta de saldo, reparación de celulares, entre otros.
Esta empresa es distribuidora de la Compañía: **TELEFÓNICA MÓVILES EL SALVADOR. (MOVISTAR)**[11]

3.2 MARCO CONCEPTUAL

3.2.1 CLASIFICACION DE LA AUDITORIA DE SISTEMAS

La Auditoría de Sistemas se clasifica en las siguientes áreas:

a) Auditoría Informática de Producción o Explotación

[11] www.siget.gob.sv

b) Auditoría Informática de Desarrollo de Proyectos

c) Auditoría Informática de Sistemas

d) Auditoría Informática de Comunicaciones y Redes

e) Auditoría de la Seguridad Informática:

e.1) Seguridad Física

e.2) Seguridad Lógica

e.3) Seguridad Organizativo-Administrativa

e.4) Seguridad Jurídica

f) Auditoría Informática para Aplicaciones en Internet.

3.2.1.1 AUDITORIA DE LA SEGURIDAD INFORMÁTICA

La expresión de seguridad informática, que es la mas usada, puede llegar a relacionarse solo con los equipos y entornos técnicos, como si la información en otros soportes y ambiente no requiera protección, cuando son las propias operaciones de la entidad, el negocio de la entidades con animo de lucro, lo que requiere protección.

Sino existen medidas y adecuada protección se puede perder información vital, o por lo menos no estar disponibles en el momento requerido, las decisiones tomadas pueden ser erróneas, o se pueden incumplir contratos ala propia legislación, lo que puede traducirse en grandes multas o infracciones graves, o algo que es aun peor: la inmovilización de ficheros previstos.

3.2.2 CLASIFICACION DE LA AUDITORIA DE SEGURIDAD INFORMATICA

3.2.2.1 SEGURIDAD FISICA:

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

a) **Desastres Naturales (terremotos, erupciones volcánicas, incendios accidentales, tormentas e inundaciones.)**
b) **Amenazas ocasionadas por el hombre.(robo, fraudes, hacker, virus)**
c) **Disturbios (sabotajes internos y externos deliberados.)**

a) TIPOS DE DESASTRES:

a.1) INCENDIOS

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un “falso piso” instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.

- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles.
- Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

a.2) INUNDACIONES

Se les define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas:

- Construir un techo impermeable para evitar el paso de agua desde un nivel superior y
- Acondicionar las puertas para contener el agua que bajase por las escaleras.

a.3) CONDICIONES CLIMATOLOGICAS

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

a.4) TERREMOTOS

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

b) OTRAS AMENAZAS A LA SEGURIDAD FISICA:

b.1) FALTA DE SEGURIDAD DEL EQUIPAMIENTO

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Recomendaciones:

- El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.
- Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

- Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.
- Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

b.2) SEÑALES DE RADAR

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiado desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

b.3) INSTALACION ELECTRICA

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

b.4) PICOS Y RUIDOS ELECTROMAGNETICOS

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el

funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

b.5) CABLEADO

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

b.5.1) Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.

b.5.2) Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

b.5.3) Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

b.6) CABLEADO DE ALTO NIVEL DE SEGURIDAD

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreo de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

b.7) PISOS DE PLACAS EXTRAIBLES

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo.

b.8) SISTEMA DE AIRE ACONDICIONADO

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

b.9) EMISIONES ELECTROMAGNETICAS

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas.

Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

b.10) ERGOMETRIA

“La **Ergonomía** es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.”

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

La ergonomía es básicamente una tecnología de aplicación práctica e interdisciplinaria, fundamentada en investigaciones científicas, que tiene como objetivo la optimización integral de Sistemas Hombres-Máquinas, los que estarán siempre compuestos por uno o más seres humanos cumpliendo una tarea cualquiera con ayuda de una o más "máquinas" (se define con ese término genérico a todo tipo de herramientas, máquinas industriales propiamente dichas, vehículos, computadoras, electrodomésticos, etc.).

b.11) TRANSTORNOS OSEOS Y/O MUSCULARES

Una de las maneras de provocar una lesión ósea o muscular es obligar al cuerpo a ejecutar movimientos repetitivos y rutinarios, y esta posibilidad se agrava enormemente si dichos movimientos se realizan en una posición incorrecta o antinatural.

En el ambiente informático, la operación del teclado es un movimiento repetitivo y continuo, si a esto le sumamos el hecho de trabajar con una distribución ineficiente de las teclas, el diseño antinatural del teclado y la ausencia (ahora atenuada por el uso del mouse) de movimientos alternativos al de tecleado, tenemos un potencial riesgo de enfermedades o lesiones en los músculos, nervios y huesos de manos y brazos.

En resumen, el lugar de trabajo debe estar diseñado de manera que permita que el usuario se coloque en la posición más natural posible. Como esta posición variará de acuerdo a los distintos usuarios, lo fundamental en todo esto es que el puesto de trabajo sea ajustable, para que pueda adaptarse a las medidas y posiciones naturales propias de cada operador.

b.12) TRANSTORNOS VISUALES

Los ojos, sin duda, son las partes más afectadas por el trabajo con computadoras.

La pantalla es una fuente de luz que incide directamente sobre el ojo del operador, provocando, luego de exposiciones prolongadas el típico cansancio visual, irritación y lagrimeo, cefalea y visión borrosa.

Si a esto le sumamos un monitor cuya definición no sea la adecuada, se debe considerar la exigencia a la que se someterán los ojos del usuario al intentar descifrar el contenido de la pantalla. Además de la fatiga del resto del cuerpo al tener que cambiar la posición de la cabeza y el cuello para acercar los ojos a la misma.

Para prevenir los trastornos visuales en los operadores podemos tomar recaudos como:

- Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
- Usar de pantallas antirreflejo o anteojos con protección para el monitor, es una medida preventiva importante y de relativo bajo costo, que puede solucionar varios de los problemas antes mencionados.

b.13) SALUD MENTAL

La carga física del trabajo adopta modalidades diferentes en los puestos informatizados. De hecho, disminuye los desplazamientos de los trabajadores y las

tareas requieren un menor esfuerzo muscular dinámico, pero aumenta, al mismo tiempo, la carga estática de acuerdo con las posturas inadecuadas asumidas.

Además, **el estrés informático** está convirtiéndose en una nueva enfermedad profesional relacionada con el trabajo, provocada por la carga mental y psíquica inherente a la operación con los nuevos equipos.

b.14) AMBIENTE LUMINOSO

Se parte de la base que las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las empresas y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

b.15) AMBIENTE CLIMATICO

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente.

b.16) ACCIONES HOSTILES

b.16.1) ROBO

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada.

b.16.2) FRAUDE

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

b.16.3) SABOTAJE

El peligro más temido en los centros de procesamiento de datos, es el sabotaje.

Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

b.17) CONTROL DE ACCESO

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

b.17.1) VERIFICACION DE VOZ

La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.).

Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

b.17.2) PROTECCION ELECTRONICA

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la

central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

b.17.3) BARRERAS INFRAROJAS Y DE MICRO-ONDAS

Transmiten y reciben haces de luces infrarrojas y de micro–ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa. Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

b.17.4) DETECTOR ULTRASONICO

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

b.17.5) CIRCUITOS CERRADOS DE TELEVISION

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

b.17.6) EDIFICIOS INTELIGENTES

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos.

El Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

La seguridad es un factor de suma importancia en los centros de cómputos instalados o a instalar. Esta consideración se refleja en la elección de las normas a considerar para la ubicación del procesador, materiales utilizados para su construcción, equipo de detectores y protección contra incendios, sistema de aire acondicionado, instalación eléctrica, sistema de control de acceso y el entrenamiento al personal u operadores.

3.2.2.2 SEGURIDAD LOGICA

a) SEGURIDAD LÓGICA Y CONFIDENCIAL

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado “virus” de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización (“piratas”) y borra toda la información que se tiene en un disco.

Al auditar los sistemas se debe tener cuidado que no se tengan copias “piratas” o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificarla información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

a.1) El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos

- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

a.2) Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- Identificar aquellas aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.
- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- La justificación del costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo,
- **Se debe preguntar lo siguiente:**
    - ¿Que sucedería si no se puede usar el sistema?
    - Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riesgo.
- **La siguiente pregunta es:**
    - ¿Que implicaciones tiene el que no se obtenga el sistema y cuanto tiempo podríamos estar sin utilizarlo?
    - ¿Existe un procedimiento alterno y que problemas nos ocasionaría?

- ¿Que se ha hecho para un caso de emergencia?

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medias preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.

a.3) Para clasificar la instalación en términos de riesgo se debe:

- Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.

- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.

- Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

b) CONTROLES DE ACCESO

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la Seguridad Lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

c) IDENTIFICACION Y AUTENTIFICACION

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina **Identificación** al momento en que el usuario se da a conocer en el sistema; y **Autenticación** a la verificación que realiza el sistema sobre esta identificación.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. **Esta administración abarca:**

c.1) Proceso de solicitud:

Establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

c.2) La identificación de los usuarios:

Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

c.3) Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos:

Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

c.4) Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas:

La actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

c.5) Detección de actividades no autorizadas:

Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

c.6) Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado:

Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

c.7) Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización:

Llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

d) ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

e) TRANSACCIONES

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

f) LIMITACIONES A LOS SERVICIOS

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización

simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

g) MODALIDAD DE ACCESO

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

g.1) Lectura:

El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.

g.2) Escritura:

Este tipo de acceso permite agregar datos, modificar o borrar información.

g.3) Ejecución:

Este acceso otorga al usuario el privilegio de ejecutar programas.

g.4) Borrado:

Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

g.5) Todas las anteriores.

g.6) Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

g.6.1) Creación:

Permite al usuario crear nuevos archivos, registros o campos.

g.6.2) Búsqueda:

Permite listar los archivos de un directorio determinado.

h) CONTROL DE ACCESO INTERNO

h.1) PALABRAS CLAVES (PASSWORDS)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

h.2) ENCRIPTACION

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

h.3) LISTAS DE CONTROL DE ACCESO

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

h.4) LIMITES SOBRE INTERFASES DE USUARIO

Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

h.5) ETIQUETAS DE SEGURIDAD

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

i) CONTROL DE ACCESO EXTERNO

i.1) DISPOSITIVOS DE CONTROL DE PUERTOS

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

i.2) FIREWALLS O PUERTAS DE SEGURIDAD

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.

j) ADMINISTRACION

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

3.2.2.3 SEGURIDAD ORGANIZATIVA- ADMINISTRATIVA (PERSONAL)

Es la responsabilidad que este toma sobre la información y las medidas y protocolos de conducta. Pretende cubrir el hueco dejado por las dos anteriores y viene, cierto modo a complementarlas.

Difícilmente se puede lograr de forma eficaz la seguridad de la información si no existen claramente definidas las políticas siguientes:

a) **Políticas de seguridad.**
b) **Políticas de personal**
c) **Políticas de contratación Análisis de riesgos.**
d) **Planes de Contingencia**

3.2.2.4 SEGURIDAD JURIDICA

La seguridad jurídica pretende, a través de la aprobación de normas legales, fijar el marco jurídico necesario para proteger los bienes informáticos.

3.2.3 EVALUACION DE LA SEGURIDAD

PARA REALIZAR UNA EVALUACIÓN DE LA SEGURIDAD, ES IMPORTANTE CONOCER CÓMO DESARROLLAR Y EJECUTAR LA IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD.

Desarrollar un Sistema de Seguridad implica: planear, organizar, coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa.

3.2.3.1 LAS CONSIDERACIONES DE UN SISTEMA INTEGRAL DE SEGURIDAD DEBEN CONTEMPLAR:

- **a)** Definir elementos administrativos
- **b)** Definir Políticas de Seguridad: A nivel departamental, a nivel institucional
- **c)** Organizar y dividir las responsabilidades
- **d)** Contemplar la Seguridad Física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- **e)** Definir prácticas de Seguridad para el personal: Plan de emergencia, Plan de evacuación, Uso de recursos de emergencia (extinguidores, etc.)
- **f)** Definir el tipo de Pólizas de Seguros
- **g)** Definir elementos técnicos de procedimientos: Técnicas de aseguramiento del sistema
- **h)** Codificar la información: Criptografía

i) Contraseñas difíciles de averiguar (letras mayúsculas, minúsculas, números y símbolos) que deben ser cambiadas periódicamente
j) Vigilancia de Red: Tecnologías repelentes o protectoras (Cortafuegos (firewalls), sistema de detección de intrusos, etc.)
k) Anti-spyware, antivirus, llaves para protección de software, etc.
l) Mantener los sistemas de información (sistemas operativos y programas) con las actualizaciones que más impacten en la Seguridad
m) Definir las necesidades de Sistemas de Seguridad para hardware y software
n) Flujo de energía
o) Cableados locales y externos
p) Aplicación de los Sistemas de Seguridad, incluyendo datos y archivos
q) Planificación de los papeles de los Auditores internos y externos
r) Planificación de programas de contingencia o recuperación de desastre y sus respectivas pruebas (Simulación)
s) Planificación de Pruebas al Plan de Contingencia con carácter periódico
t) Política de Destrucción de basura, copias, fotocopias, discos duros, etc.

3.2.3.2 CONSIDERACIONES PARA ELABORAR UN SISTEMA DE SEGURIDAD

Para dotar de medios necesarios al elaborar su sistema de seguridad, se debe considerar los siguientes puntos:

a) Sensibilizar a los ejecutivos de la organización en torno al tema de Seguridad
b) Se debe realizar un Diagnóstico de la situación de riesgo y Seguridad de la información en la organización a nivel software, hardware, recursos humanos y ambientales
c) Elaborar un Plan para un Programa de Seguridad

3.2.3.3 ETAPAS PARA IMPLANTAR UN PLAN DE SEGURIDAD

Para que su Plan de Seguridad entre en vigor y los elementos empiecen a funcionar, se observen y acepten las nuevas políticas del nuevo Sistema de Seguridad, se deben seguir los siguientes pasos:

- **a)** Introducir el tema de Seguridad en la visión de la empresa
- **b)** Definir los procesos de Flujo de Información y sus Riesgos en cuanto a todos los recursos participantes
- **c)** Capacitar a los Gerentes y Directivos, contemplando el enfoque global
- **d)** Designar y capacitar a Supervisores de área
- **e)** Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas
- **f)** Mejorar las comunicaciones internas
- **g)** Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel
- **h)** Capacitar a todos los trabajadores en los elementos básicos de Seguridad y Riesgo para el manejo del software, hardware y con respecto a la Seguridad Física

3.2.3.4 BENEFICIOS DE UN SISTEMA DE SEGURIDAD

Los beneficios de un Sistema de Seguridad bien elaborados son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- **a)** Aumento de la productividad
- **b)** Compromiso con la misión de la compañía
- **c)** Ayuda a formar equipos competentes
- **d)** Mejora de los climas laborales para los Recursos Humanos

3.2.3.5 DISPOSICIONES QUE ACOMPAÑAN LA SEGURIDAD

Desde el punto de vista de Seguridad, se debe contar con un conjunto de disposiciones o acción para llevarse a cabo en caso de presentarse situaciones de riesgo:

- **a)** Obtener una especificación de todas las aplicaciones, los programas y archivos de datos
- **b)** Medidas y Planes de Contingencia en caso de desastre como pérdida total de datos, abuso, etc.
- **c)** Prioridades en cuanto a acciones de seguridad de corto y largo plazo
- **d)** Verificar el tipo de acceso que tienen las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de Operación y viceversa
- **e)** Que los operadores no sean los únicos en resolver los problemas que se presentan

3.2.3.6 RAZONES QUE IMPIDEN LA APLICACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir directrices de Seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito; la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas Políticas de Seguridad Informática.

Esta situación ha llevado a que muchas empresas con activos muy importantes se encuentren expuestas a problemas de seguridad y riesgos innecesarios los cuales, en muchos casos, comprometen información sensible y, por ende, la imagen corporativa.

Ante esta situación, los encargados de la Seguridad deben confirmar que las personas entienden los asuntos importantes de la Seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos. Si se quiere que las Políticas de Seguridad sean aceptadas deben integrarse a las estrategias del negocio, a

su misión y visión, con el propósito de que quienes toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Es importante señalar que las Políticas, por sí solas, no constituyen una garantía para la Seguridad de la organización. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer, en los mecanismos de Seguridad Informática, factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

3.2.4 CONTROL INTERNO INFORMATICO

3.2.4.1 CONTROL INTERNO EN AMBIENTE COMPUTARIZADO.

Comprende el plan de organización, métodos y procedimientos que se coordinan y adaptan en una entidad para salvaguardar sus activos, prevenir sabotajes, errores e irregularidades, verificar la razonabilidad y confiabilidad de su información financiera, produciendo el cumplimiento de sus políticas.

Considerando las Normas Internacionales de Auditoría en relación al control interno este puede dividirse en: Controles Generales y de Aplicación. Esta división se establece en la Declaración Internacional de Practica de Auditoría 1008 sobre la Evaluación del Riesgo y el Control Interno en un Ambiente SIC.

3.2.4.2 CONTROLES GENERALES EN UN AMBIENTE SIC.

El control interno en un ambiente SIC tiene como objetivo reducir el riesgo asociado a este ambiente. Para contribuir a ello los controles generales establecen un marco de referencia de control global sobre las operaciones para proporcionar un grado de certeza razonable sobre el cumplimiento de estos.

Los controles generales pueden incluir:

a) **Controles de Organización y Administración.**

a.1) Considera aspectos en los cuales se relaciona la organización con las actividades del ambiente de información por computadora.

a.2) Políticas y procedimientos relativos a funciones de control.

a.3) Segregación apropiada de las funciones.

b) Desarrollo de sistemas de aplicación y controles de mantenimiento.

Establecen una razonable certeza de que los sistemas se desarrollan y mantienen de manera eficiente y autorizada; a través de implementar controles sobre:

b.1) Implementación, conversión, pruebas y documentación de sistemas nuevos y usados.

b.2) Cambios a sistemas de aplicación.

b.3) Acceso a documentación de sistemas.

b.4) Adquisición de sistemas de aplicación con terceros.

c) Controles de operación de computadoras.

Señala la necesidad de establecer controles para tener certeza razonable de que el tipo de operación de los sistemas es:

c.1) Para propósitos autorizados.

c.2) El acceso a la información de la computadora es restringido.

c.3) El uso de programas autorizados.

c.4) Los errores de procesamientos son detectados y corregidos.

d) Controles de software de sistemas.

Considera la conveniencia de implementar medidas que proporcionen razonable certeza de que el software del sistema se adquiere y desarrolla de manera establecida y eficiente en lo referente a:

d.1) La autorización, aprobación, pruebas, implementación y documentación de software(s) nuevo(s) y modificado(s).

d.2) Restricciones de acceso a software a personal no autorizado.

e) **Controles de entrada de datos y de programas**

Estos controles tratan de disminuir el riesgo a través del establecimiento de una estructura de autorización sobre las transacciones que alimentan al sistema. Así como también, limitar el acceso a datos y programas a personal autorizado.

Además de los controles anteriores existen medidas de salvaguarda los cuales también contribuyen a la continuidad del procesamiento de datos en un ambiente SIC.

3.2.4.3 CONTROLES DE APLICACIÓN EN UN AMBIENTE SIC.

Los controles generales tratan de establecer medidas de seguridad en toda la entidad, tratando de conseguir un ambiente propicio para implementar los controles de aplicación, los cuales establecen procedimientos específicos de control sobre las aplicaciones contables, los cuales son:

a) **Controles sobre datos de entrada.**

Estos controles se enmarcan desde establecer la autorización para procesar por la computadora las transacciones, su integridad, exactitud de los datos ingresados hasta rechazarlos al faltar cuando sea necesario, y volverlos a establecer oportunamente.

b) **Controles sobre el procesamiento y sobre archivos de datos de la computadora.**

Incluye aquellos controles que le permiten a la empresa conocer si se procesan las transacciones por la computadora en forma congruente, así como también si estos no son perdidos, añadidos, duplicados o combinación inapropiada; de tal manera que facilite identificar estas anomalías y corregirlas oportunamente.

c) **Controles sobre los datos de salida.**

Son diseñados para lograr obtener al final del procesamiento de los datos resultados exactos así como también restringirle el acceso a personal autorizado y finalmente que pueda servir oportunamente para la toma de decisiones.

3.2.5 LOS RIESGOS INFORMATICOS

3.2.5.1 Beneficios:

- **a)** Aumentar la confianza
- **b)** Identificación de bienes, vulnerabilidades y controles
- **c)** Aumento de conocimientos básicos para la toma de decisiones
- **d)** Justificación de erogaciones/gastos de seguridad

3.2.5.2 Fases del Análisis de Riesgos:

- **a)** Identificación y clasificación de riesgos
- **b)** Pronóstico y evaluación de las consecuencias
- **c)** Estimación de la probabilidad de ocurrencia
- **d)** Evaluación de la exposición al riesgo

a) Identificación y Clasificación de Riesgos:

a.1) Identificación de los bienes: Hardware, Software, Datos, Personal y Documentación.

a.2) Identificación y clasificación de los riesgos: Sobrecarga, destrucción, robo, copiado, pérdida, etc.

b) Pronóstico y evaluación de las consecuencias:

Una vez identificado el riesgo, se puede:

b.1) Prevenirlo:

Minimizar su probabilidad de ocurrencia

b.2) Retenerlo:

Minimizar sus consecuencias (plan de recuperación)

b.3) Transferirlo:

Seguro de pérdidas, convenios con otros usuarios, etc.

3.2.5.3 RIESGOS RELACIONADOS CON LA INFORMATICA:

- **a)** Seguridad Física**.**
- **b)** Control de Accesos.
- **c)** Protección de los Datos.
- **d)** Seguridad en las Redes

3.2.5.4 RIESGOS INFORMATICOS RELACIONADOS CON LOS NEGOCIOS:

a) Riesgos de Integridad:

Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización.

b) Riesgos de relación:

Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación.

c) Riesgos de acceso:

Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información.

d) Riesgos de utilidad:

Estos riesgos se enfocan en tres diferentes niveles de riesgo:

Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.

3.2.5.5 TÉCNICAS DE RECUPERACIÓN/RESTAURACIÓN USADAS PARA MINIMIZAR LA RUPTURA (RIESGOS) DE LOS SISTEMAS:

a) Back ups y planes de contingencia controlan desastres en el procesamiento de la información.

b) Riesgos en la infraestructura:

Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (*hardware, software, redes, personas y procesos)* para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

c) Riesgos de seguridad general:

Requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo.

3.2.5.6 OTROS RIESGOS QUE AFECTAN A LA PROTECCIÓN INFORMÁTICA PUESTO QUE AUMENTAN LOS PUNTOS DE VULNERABILIDAD DE LOS SISTEMAS:

a) Dependencia en el personal clave:

Además del peligro que encierra algún desastre en los sistemas informáticos, existen otras situaciones potencialmente riesgosas de las cuales la más importante es, quizá, la dependencia hacia individuos clave.

b) Concentración de procesamiento de aplicaciones más grandes y de mayor complejidad:

Una de las causas más importantes del incremento en los riesgos informáticos probablemente sea el aumento en la cantidad de aplicaciones o usos que se le da a las computadoras y la consecuente concentración de información y tecnología de

software para el procesamiento de datos, generalmente la información y programas están concentrados en las manos de pocas personas.

c) Desaparición de los controles tradicionales*:*

Muchas de las nuevas y extensas aplicaciones omiten las auditorías tradicionales y los controles impresos por razones de volumen. Las aplicaciones contienen verificadores automáticos que aseguran la integridad de la información que se procesa.

d) Huelgas, terrorismo e inestabilidad social:

El nivel actual de riesgo en computación se debe revisar también dentro del contexto de inestabilidad social en muchas partes del mundo. Ha habido ataques físicos a diversas instalaciones, sin embargo algunas veces se trata de la incursión de personal interno y no de agitadores.

e) Mayor conciencia de los proveedores:

Hasta hace pocos años este tema no constituía motivo de gran preocupación para los proveedores, pero la conciencia acerca de la exposición a los riesgos los ha obligado a destinar presupuestos considerables para la investigación acerca de la seguridad. Como resultado, se dispone de un mayor número de publicaciones de alta calidad para los usuarios, lo que permite mejorar la estructura y el enfoque para la seguridad de las computadoras; asimismo, ha intensificado el interés por reducir en forma progresiva el riesgo causado por un desastre en las computadoras.

3.2.6 PROBLEMAS DE SEGURIDAD DE LOS SISTEMAS INFORMATICOS:

- **a)** VULNERABILIDAD
- **b)** BIENES INFORMÁTICOS SENSIBLES: Software y Hardware
- **c)** BIENES NO INTRÍNSECAMENTE INFORMÁTICOS

3.2.6.1 PRINCIPALES PROBLEMAS DE LA SEGURIDAD EN INTERNET:

a) VIRUS
b) BACKDOORS
c) BUG
d) HOAX
e) SPAM
f) TROYANO
g) MALWARE
h) SPYWARE
i) WORNS (GUSANOS)
j) KEYLOGGER
k) ADWARE
l) DIALER
m) EXPLOIT
n) ROOTKIT

3.2.6.2 TECNICAS UTILIZADAS POR LOS ATACANTES

a) INGENIERIA SOCIAL

b) PHISHING

c) PHARMING

d) SKIMMING

e) SNIFFING

f) SPOOFING

g) TRASHING

h) ATAQUE DE MONOTORIZACION

i) ATAQUE DE AUTENTICACION

j) DENEGACION DE SERVICIO

k) TAMPERING O DATA DIDDLING

l) BOMBAS LOGICAS

3.2.6.3 EL USUARIOS ES A VECES EL MÁS DEBIL

a) **CONTRASEÑA SEGURA:**

La manera básica de averiguar una contraseña es probando diferentes intentos hasta dar con la que funcione. Existen programas y suele atacar de 2 formas:

b) **ATAQUE POR DICCIONARIO:**

El programa tiene cargado un diccionario de palabras y prueba con cada palabra del diccionario.

c) **COMBINATORIA O POR FUERZA BRUTA:** el programa genera combinaciones secuenciales de caracteres y prueba con todos.

3.2.6.4 INTRUSOS

Personas tanto internas como externas de la organización:

a) Por el abuso en el manejo de los sistemas informáticos.

b) Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos

3.2.6.5 MEDIDAS DE SEGURIDAD

a. Lógicas

b. Físicas

c. Administrativas

d. Legales

3.2.7 TECNICAS Y HERRAMIENTAS DE SEGURIDAD USADAS POR EL AUDITOR DE SISTEMAS

3.2.7.1 Técnicas:

a. Revisiones cruzadas
b. Modularidad, encapsulado y sombreado (Qué y no Cómo)
c. Pruebas independientes
d. Gestión de configuración – Control de Cambios

3.2.7.2 HERRAMIENTAS

a) Actividad en Internet:

a.1) Internet Cleanup

a.2) Internet Manager

a.3) Internet Risk Management

a.4) NetFocus

a.5) System Activity Manager

a.6) Web Spy

b) Análisis de Red:

b.1) Event Log Monitor

b.2) Expert Observer

b.3) Kane Security Analyst

c) Anti-Espionaje:

c.1) Ad-Search

c.2) Hook Protect

c.3) Iprotect

c.4) PC Security Guard

c.5) Top Secret Office

d) Anti-Virus y Troyanos:

d.1) AVX

d.2) eSafe Protect

d.3) F-Secure

d.4) Kaspersky Anti-Virus

d.5) MAM Soft

d.6) Mcfee Virus Scan

d.7) Norton Antivirus

d.8) Panda Antivirus Platinum

d.9) Protector Plus

d.10) Quick Heal RAV AntiVirus

d.11) Trojan Defense Suite

d.12) ViruSafe Web

e) Arranque:

e.1) Access Denied

e.2) MindSoft Custody

e.3) Screen Lock

e.4) Xlock

f) Auditoria:

f.1) File Audit

f.2) Log Monitor

f.3) Security Charge

g) Backup:

g.1) @Backup Adsm

g.2) Arc Serve

g.3) AutoSave

g.4) Backup ATM Network

g.5) Backup Exec

g.6) Connected Online Backup

h) Control Remoto:

h.1) AMI Server Manager

h.2) Control IT

h.3) Net Support Manager

h.4) Pc Anywhere

i) Cookies

i.1) Cookie Crusher

i.2) Cookie Pal

i.3) Cyber Clean

i.4) The Watchman

j) Detectores de Agujeros de Seguridad

j.1) Intruder Alert

j.2) Lan Guard Network Scanne

k) Encriptación de Comunicaciones:

k.1) F-Secure VPN

k.2) Go Secure

k.3) Intel VPN

k.4) Power VPN

k.5) Safe Guard VPN

k.6) Sidewinder

k.7) SmartGate

l) Encriptación de Software

l.1) Absolute Security

l.2) Best Crypt

l.3) Data Safe

l.4) Encrypted Magic Folders

l.5) File Protector

l.6) File Disk Protector

l.7) Fly Crypt

l.8) Folder Guard

l.9) Norton Secret Stuff

l.10) PC Safe

l.11) Security BOX

l.12) Security Manager

l.13) WINZAP

m) Espionaje:

m.1) Activity Monitor

m.2) Key Logger

m.3) Keyboard Monitor

m.4) KeyKey

m.5) MyGuardian

m.6) PC Spy

m.7) Spy Anywhere

m.8) System Spy

m.9) Win Guardian

n) Filtros de Internet:

n.1) e-Sweeper

n.2) Smart Filter

n.3) WEB sweeper

n.4) Firewalls

n.5) Fire Proof Firewall KIT System

n.6) Norton Personal Firewall

n.7) Smart Wall

n.8) Gestión de Accesos

n.9) IKey

n.10) Panda Security

n.11) Personal Protector

n.12) Safe Guard Easy

n.13) Smart Lock

o) Mantenimiento:

o.1) Diskeeper

o.2) More Space

o.3) Partition Commander

o.4) Partition Magic

o.5) Security Setup

o.6) System Commander

o.7) Windows Commander

p) Ocultación:

p.1) Black Board File Wipe

p.2) Boss

p.3) Camouflage

p.4) Web Password

p.5) Wipe Clean

q) Recuperación de Datos:

q.1) Easy Recovery

q.2) Esupport

q.3) GoBack

q.4) Instant Recovery

r) Seguridad en Comercio Electrónico:

r.1) Commerce Protector

r.2) Net Secure

r.3) Safety Net

s) Suites de Seguridad Informática:

s.1) F-Secure Workstation Suite

s.2) Mcafee Office 2000 Pro

s.3) NetMax Professional Suite

s.4) Norton Internet Security 2000

s.5) Observer Suite

3.2.8 PROCESO GENERAL DE LA AUDITORIA DE SISTEMAS

a) Identificar el origen de la auditoria

b) Realizar una visita preliminar al área que será evaluada

c) Establecer los objetivos de la auditoria

d) Determinar los puntos que serán evaluados en la auditoria

e) Elaborar planes, programas y presupuestos para realizar la auditoria.

f) Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para realizar la auditoria

g) Asignar los recursos y sistemas computacionales para la auditoria.

3.2.8.1 Investigación preliminar.

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización. Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

3.2.8.2 Recopilación de Información con la Administración.

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

3.2.8.3 Para analizar y dimensionar la estructura por auditar se debe solicitar a nivel del Area de Informática:

a) Objetivos a corto y largo plazo.

b) Recursos materiales y técnicos.

c) Solicitar documentos sobre los equipos, número de ellos, localización y características.

d) Estudios de viabilidad.

e) Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)

f) Fechas de instalación de los equipos y planes de instalación.

g) Contratos vigentes de compra, renta y servicio de mantenimiento.

h) Contratos de seguros.

i) Convenios que se tienen con otras instalaciones.

j) Configuración de los equipos y capacidades actuales y máximas.

k) Planes de expansión.

l) Ubicación general de los equipos.

m) Políticas de operación.

n) Políticas de uso de los equipos.

o) Aplicación de Auditoria de Sistemas de Información

3.2.8.4 Para analizar y dimensionar la estructura por auditar se debe solicitar a nivel del Sistema

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

a) Manual de formas.

b) Manual de procedimientos de los sistemas.

c) Descripción genérica.

d) Diagramas de entrada, archivos, salida.

e) Salidas.

f) Fecha de instalación de los sistemas.

g) Proyecto de instalación de nuevos sistemas.

3.2.8.5 FUENTES DE LA AUDITORIA.

Las fuentes estarán relacionadas con los objetivos, y entre ellas pueden estar:

a) Políticas, estándares, normas y procedimientos.

b) Planes de seguridad.

c) Contratos, pólizas de seguros.

d) Organigrama y descripción de funciones.

e) Documentación de aplicaciones.

f) Descripción de dispositivos relacionados con la seguridad.

g) Manuales técnicos de sistemas operativos o de herramientas.

h) Inventarios: de soportes, de aplicaciones.

i) Topologías de redes.

j) Planos de instalaciones.

k) Registros: de problemas, de cambios, de vistas, de accesos lógicos producidos.

l) Entrevistas a diferentes niveles.

m) Ficheros.

n) Programas.

o) La observación no figura en los manuales para la consideramos importante.

p) Actas de reuniones relacionadas.

q) Documentación de planes de continuidad y sus pruebas.

r) Informes de suministradores o consumidores

3.3 MARCO LEGAL

3.3.1 CODIGO PENAL

DE LOS DELITOS RELATIVOS A LA INTIMIDAD

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 esté 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 archivo o registro público o privado, será sancionado con multa de cincuenta a cien 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 público 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 artificios 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.

REVELACIÓN DE SECRETO PROFESIONAL

Art. 187.- El que revelare un secreto del que se ha impuesto en razón de su profesión u oficio, será sancionado con prisión de seis meses a dos años e inhabilitación especial de profesión u oficio de uno a dos años.

PIRATERÍA DE SOFTWARE

DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL

VIOLACIÓN DE DERECHOS DE AUTOR Y DERECHOS CONEXOS

Art. 226.- El que a escala comercial reprodujere, plagiare, distribuyere al mayoreo o comunicare públicamente, en todo o en parte, una obra literaria o artística 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 dos a cuatro años.

En la misma sanción incurrirá, el que a escala comercial 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 prisión de cuatro a seis 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 A MEDIDAS TECNOLÓGICAS EFECTIVAS

Art. 227-A.- Será sancionado con prisión de dos a cuatro años, el que con fines de lograr una ventaja comercial o ganancia financiera privada:

a) Evadiere, sin autorización del titular del derecho, cualquier medida tecnológica efectiva que controle el acceso a una obra, interpretación, ejecución o fonograma protegido u otra materia objeto de protección;
b) Fabricare, importare, distribuyere, ofreciere al público, proporcionare o traficare dispositivos, productos o componentes; u ofreciere al público o proporcionare servicios al público, siempre que los dispositivos, productos o componentes, o los servicios:
1) Sean promocionados, publicitados o comercializados con el propósito de evadir una
Medida tecnológica efectiva;
2) Tengan únicamente un propósito limitado o uso de importancia comercial diferente al de evadir una medida tecnológica efectiva; o
3) Sean diseñados, producidos o ejecutados principalmente con el fin de permitir o facilitar la evasión de cualquier medida tecnológica efectiva.

Se excluyen de responsabilidad penal, al que ejecute las actividades exceptuadas conforme se establece en el artículo 85-D de la Ley de Propiedad Intelectual.

VIOLACIÓN A LA INFORMACIÓN SOBRE GESTIÓN DE DERECHOS

Art. 227-B.- Será sancionado con prisión de dos a cuatro años, el que con fines de lograr una ventaja comercial o ganancia financiera privada y a sabiendas que este acto podría inducir, permitir, facilitar o encubrir una infracción de un derecho de autor o derecho conexo:
a) A sabiendas suprimiere o alterare cualquier información sobre gestión de derechos;
b) Distribuyere o importare para su distribución la información sobre gestión de derechos, teniendo conocimiento que dicha información ha sido suprimida o alterada sin autorización del titular del derecho; o
c) Distribuyere, importare para su distribución, transmisión, comunicación o puesta a disposición del público copias de obras, interpretaciones o ejecuciones o fonogramas,

teniendo conocimiento que la información sobre gestión de derechos ha sido suprimida o alterada sin autorización del titular del derecho.

VIOLACIÓN AL DERECHO SOBRE SEÑALES DE SATÉLITE

Art. 227-C.- Será sancionado con prisión de dos a cuatro años, el que:

a) Fabricare, ensamblare, modificare, importare, exportare, vendiere, arrendare o distribuyere por cualquier medio, un dispositivo o sistema tangible o intangible, sabiendo o teniendo razones para saber que el dispositivo o sistema sirve primordialmente para descodificar una señal de satélite codificada portadora de programas, sin la autorización del distribuidor legítimo de dicha señal;

b) Recibiere y subsiguientemente distribuyere una señal portadora de programas que se haya originado como una señal de satélite codificada, teniendo conocimiento que ha sido descodificada sin la autorización del distribuidor legítimo de dicha señal

FRAUDE DE COMUNICACIONES

Art. 238-A.- El que interfiere, alterare, modificare o interviniere cualquier elemento del sistema de una compañía que provee servicios de comunicaciones con el fin de obtener una ventaja o beneficio ilegal, será sancionado con prisión de tres a seis años. Asimismo, el que activare o configurare ilegalmente teléfonos celulares u otros aparatos de comunicación robados, hurtados, extraviados provenientes de acciones ilícitas se aplicará una sanción de cuatro a ocho años de prisión y además una multa de ciento cincuenta a doscientos días multa.

INTERFERENCIA E INTERVENCIÓN DE COMUNICACIONES TELEFÓNICAS

Art. 302.- El que interceptare o interviniere las comunicaciones telefónicas o usare artificios técnicos de escucha o grabación de dichas comunicaciones o lo ordenare o permitiere, será sancionado con prisión de dos a cuatro años, e inhabilitación especial

para el ejercicio del cargo o empleo por igual tiempo, si fuere funcionario o empleado público.

En el marco de una investigación judicial o de la Fiscalía General de la República, no se considerará como interferencia o intervención telefónica, ni violación al derecho de intimidad, cuando se estuviere recibiendo amenazas, exigiendo rescate de una persona que estuviere privada de libertad o secuestrada o se pidiere el cumplimiento de determinados hechos a cambio de la liberación de dicha persona, o a cambio de no intentar ninguna acción penal o se trate de delitos de crimen organizado, y la víctima, el ofendido o su representante, en su caso, solicitaren o permitieren por escrito a la Fiscalía General de la República, la escucha y grabación de las conversaciones o acciones en que se reciban tales amenazas o exigencias. La escucha y grabación así obtenida podrá ser utilizada con fines probatorios en juicio y, en este caso, deberá ser valorada por el juez.

3.3.2 LEY ESPECIAL CONTRA ACTOS DE TERRORISMO

DELITO INFORMÁTICO

Art. 12.- Será sancionado con pena de prisión de diez a quince años, el que para facilitar la comisión de cualquiera de los delitos previstos en esta Ley:

a) Utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos, programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades nacionales, internacionales o de otro país;

b) Creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos a que se refiere el literal a, de este artículo

3.3.3 LEY DE PROPIEDAD INTELECTUAL

Art. 7.- El derecho económico del autor es el derecho exclusivo de autorizar o prohibir el uso de sus obras, así como la facultad de percibir beneficios económicos de la utilización de las obras, y comprende especialmente las siguientes facultades:

c) La de difundir la obra por cualquier medio que sirva para transmitir los sonidos y las imágenes, tales como el teléfono, la radio, la televisión, el cable, el teletipo, el satélite o por cualquier otro medio ya conocido o que se desarrolle en el futuro;

Art. 9.- Comunicación pública es el acto mediante el cual la obra se pone al alcance del público por cualquier medio o procedimiento, así como el proceso necesario y conducente a que la obra se ponga al alcance del público.

Son actos de comunicación pública los siguientes:

d) La transmisión de cualesquiera obra al público por hilo, cable, fibra óptica u otro procedimiento análogo;

PROGRAMAS DE ORDENADOR

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.

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.

Art. 49.- No constituye modificación de la obra, la adaptación de un programa de ordenador realizada por el propio usuario y para su utilización exclusiva.

Art. 89.- Constituye violación de los derechos de autor, todo acto que en cualquier forma menoscabe o perjudique los intereses morales o económicos del autor, tales como:

n) La comunicación, reproducción, transmisión o cualquier otro acto violatorio de los derechos previstos en esta ley, que se realice a través de redes de comunicación digital; en cuyo caso tendrá responsabilidad solidaria el operador o cualquier otra persona natural o jurídica que tenga el control de un sistema informático interconectado a dicha red, siempre que tenga conocimiento o haya sido advertido de la posible infracción, o no haya podido ignorarla sin negligencia grave de su parte.

TIPOS DE LICENCIAS.

- **LICENCIA PÚBLICA GENERAL (GNU GPL).** El autor conserva los derechos de autor (copyright), y permite la redistribución y modificación bajo términos diseñados para asegurarse de que todas las versiones modificadas del software permanecen bajo los términos más restrictivos de la propia GNU GPL.
- **LICENCIAS ESTILO BSD.** El autor, bajo tales licencias, mantiene la protección de copyright únicamente para la renuncia de garantía y para requerir la adecuada atribución de la auditoria en trabajos derivados, pero permite la ~~libre~~ redistribución y modificación, incluso si dichos trabajos tienen propietario.
- **LICENCIAS ESTILO MPL Y DERIVADAS.9** Esta licencia es de software libre. Se utilizan en gran cantidad de productos de software libre de uso

cotidiano en todo tipo de sistemas operativos. Estas licencias son denominadas de copyleft débil.

- **LICENCIAS OEM** (Fabricantes de equipos originales): existen dos formas de articular las licencias OEM, una para fabricantes de equipos originales multinacionales y otra para fabricantes de equipos locales. Ambos tipos de fabricantes de equipos pueden distribuir PC con sistemas operativos.
- **LICENCIAS CAL (client Access License – Licencia de Acceso para clientes).** Para poder acceder al software del servidor de manera legal, las estaciones de trabajo necesitan una client Access License o CAL. No es un software; es una licencia que le da al usuario el derecho a utilizar los servicios de un servidor. Existen varios tipos de Licenciamiento CAL; pero el que aplica para un Centro de Computo es el Licenciamiento por Asiento:
- **LICENCIAMIENTO POR ASIENTO:** para que cualquier número de PC's o dispositivos licenciados puedan conectarse al servidor. Se debe adquirir una CAL para cada PC o para cada dispositivo cuando sea necesario que estos utilicen los servicios; como compartir o imprimir archivos o acceder a aplicaciones Microsoft Server.

3.3.4 LEY DE TELECOMUNICACIONES

ABREVIATURAS Y DEFINICIONES

Art. 6. ENCRIPTACIÓN: es el sistema mediante el cual, con la ayuda de técnicas o programas informáticos, se cifra o codifica determinada información con la finalidad de volver inaccesible o ininteligible para alguien no autorizado a acceder a ella.

SERVICIOS DE INFORMACIÓN: Significa ofrecer una capacidad para generar, adquirir, almacenar, transformar, procesar, recuperar, utilizar o hacer disponible la información a través de las telecomunicaciones, e incluye la publicidad electrónica, sin incluir el uso de cualquiera de estas capacidades para la administración, control u

operación de un sistema de telecomunicaciones o la administración de un servicio de telecomunicaciones.

CONCESION PARA EL SERVICIO PÚBLICO DE TELEFONIA

Art. 7. La telefonía es un servicio público.

Los operadores interesados en proveer servicios de telefonía deberán solicitar a la SIGET una concesión para la explotación del servicio, la cual les será otorgada automáticamente por un plazo de treinta años con el solo cumplimiento de los requisitos de inscripción que se establecerán en el reglamento de esta Ley. Además, tales concesiones se otorgarán sin limitación alguna en cuanto a cantidad y ubicación, pudiendo existir más de una concesión en la misma área geográfica.

ACCESO A INFORMACIÓN DE RESGUARDO

Art. 42-C. Los operadores de redes comerciales de telecomunicaciones pondrán a disposición de las autoridades las bases de datos que contengan la información mencionada en el Artículo anterior, sin que esto afecte el manejo, control u operaciones de la red de telecomunicaciones del operador del servicio de telefonía.

ENCRIPTACIÓN

Art. 42-D. Los operadores de redes comerciales de telecomunicaciones deberán descriptar o asegurar que las autoridades puedan descriptar, cualquier comunicación de un suscriptor o cliente, con el propósito de obtener la información a que se refieren los dos Artículos anteriores, en los casos en que la encriptación haya sido proveída por el operador de servicio.

3.3.5 CODIGO DE COMERCIO.

Art. 435.- El comerciante está obligado a llevar contabilidad debidamente organizada de acuerdo con alguno de los sistemas generalmente aceptados en materia de Contabilidad y aprobados por quienes ejercen la función pública de Auditoria.

Los comerciantes deberán conservar en buen orden la correspondencia y demás documentos probatorios.

Los comerciantes podrán llevar la contabilidad en hojas separadas y efectuar las anotaciones en el Diario en forma resumida y también podrán hacer uso de sistemas electrónicos o de cualquier otro medio técnico idóneo para registrar las operaciones contables.

3.3.6 LEY REGULADORA DEL EJERCICIO DE LA CONTADURIA PÚBLICA.

CAPITULO I

DE LA PROFESION DE LA CONTADURIA PUBLICA Y DE LA AUDITORIA DE LOS CONTADORES PUBLICOS Y DE LA FUNCION DE AUDITORIA

Art.1. La presente ley tiene por objeto, regular el ejercicio de la profesión de la Contaduría Pública, la función de la Auditoría, y los derechos y obligaciones de las personas naturales o jurídicas que las ejerzan.

Para efectos de esta ley, deberá entenderse como:

AUDITORIA EXTERNA: una función pública, que tiene por objeto autorizar a los comerciantes y demás personas que por ley deban llevar contabilidad formal, un adecuado y conveniente sistema contable de acuerdo a sus negocios y demás actos relacionados con el mismo; vigilar que sus actos, operaciones, aspectos contables y financieros, se registren de conformidad a los principios de contabilidad y de auditoría aprobados por el Consejo; y velar por el cumplimiento de otras obligaciones que conforme a la ley fueren competencia de los auditores.

CAPITULO II

DE LA FUNCION DE AUDITORIA

Art.4. Sólo quienes sean autorizados para ejercer la contaduría pública podrán ejercer la función pública de auditoría.

Con el objeto de ser autorizados para el ejercicio de **auditorías externas especializadas**, los auditores también deberán cumplir los requisitos que establezcan otras leyes y ser inscritos en los registros correspondientes

3.4 MARCO TECNICO

3.4.1 NORMAS INTERNACIONALES DE AUDITORIA REALTIVAS A LA AUDITORIA DE SISTEMAS.

3.4.1.1 NORMA INTERNACIONAL DE AUDITORÍA 210. ACUERDO DE LOS TÉRMINOS DEL ENCARGO DE AUDITORÍA

Esta Norma Internacional de Auditoría (NIA) trata de las responsabilidades que tiene el auditor al acordar los términos del encargo de auditoría con la dirección y, cuando proceda, con los responsables del gobierno de la entidad. Ello incluye determinar si concurren ciertas condiciones previas a la auditoría cuya responsabilidad corresponde a la dirección y, cuando proceda, a los responsables del gobierno de la entidad.

3.4.1.2 NORMA INTERNACIONAL DE AUDITORÍA 265. COMUNICACIÓN DE LAS DEFICIENCIAS EN EL CONTROL INTERNO A LOS RESPONSABLES DEL GOBIERNO Y A LA DIRECCIÓN DE LA ENTIDAD

Esta Norma Internacional de Auditoría (NIA) trata de la responsabilidad que tiene el auditor de comunicar adecuadamente, a los responsables del gobierno de la entidad y a la dirección, las deficiencias en el control interno que haya identificado durante la realización de la auditoría de los estados financieros.

Objetivo

El objetivo del auditor es comunicar adecuadamente a los responsables del gobierno de la entidad y a la dirección las deficiencias en el control interno identificadas durante la realización de la auditoría y que, según el juicio profesional del auditor, tengan la importancia suficiente para merecer la atención de ambos.

Requerimientos

- El auditor determinará si, sobre la base del trabajo de auditoría realizado, ha identificado una o más deficiencias en el control interno.
- Si el auditor ha identificado una o más deficiencias en el control interno, determinará, sobre la base del trabajo de auditoría realizado, si, individualmente o de manera agregada, constituyen deficiencias significativas.
- El auditor comunicará a los responsables del gobierno de la entidad, por escrito y oportunamente, las deficiencias significativas en el control interno identificadas durante la realización de la auditoría.
- El auditor también comunicará oportunamente y al nivel adecuado de responsabilidad de la dirección.

3.4.1.3 NORMA INTERNACIONAL DE AUDITORÍA 300. PLANIFICACIÓN DE LA AUDITORÍA DE ESTADOS FINANCIEROS

Esta Norma Internacional de Auditoría (NIA) trata de la responsabilidad que tiene el auditor de planificar la auditoría de estados financieros. Esta NIA está redactada en el contexto de auditorías recurrentes. Las consideraciones adicionales en un encargo de auditoría inicial figuran separadamente.

La función y **el momento de realización de la planificación.**

La planificación de una auditoría implica el establecimiento de una estrategia global de auditoría en relación con el encargo y el desarrollo de un plan de

auditoría. Una planificación adecuada favorece la auditoría de estados financieros en varios aspectos, entre otros los siguientes:

- Ayuda al auditor a prestar una atención adecuada a las áreas importantes de la auditoría.
- Ayuda al auditor a identificar y resolver problemas potenciales oportunamente.
- Ayuda al auditor a organizar y dirigir adecuadamente el encargo de auditoría, de manera que éste se realice de forma eficaz y eficiente.
- Facilita la selección de miembros del equipo del encargo con niveles de capacidad y competencia adecuados para responder a los riesgos previstos, así como la asignación apropiada del trabajo a dichos miembros.
- Facilita la dirección y supervisión de los miembros del equipo del encargo y la revisión de su trabajo.
- Facilita, en su caso, la coordinación del trabajo realizado por auditores de componentes y expertos.

3.4.1.4 NORMA INTERNACIONAL DE AUDITORIA 315. IDENTIFICACIÓN Y EVALUACIÓN DE LOS RIESGOS DE ERROR MATERIAL MEDIANTE EL ENTENDIMIENTO DE LA ENTIDAD Y SU ENTORNO.

Riesgos que se originan de TI.

El uso de TI afecta la forma en se implementan las actividades de control. Desde la perspectiva del auditor, los controles sobre los sistemas de TI son efectivos cuando mantienen la integridad de la información y la seguridad de los datos que procesan dichos sistemas, e incluye controles generales de TI y controles de las aplicaciones efectivos.

Los controles generales de TI son políticas y procedimientos que se relacionan con muchas aplicaciones y soportan el funcionamiento efectivo de la aplicación de los controles. Aplican a entornos de servidores centrales, como al micro- computadoras y de usuarios terminales. Los controles generales de TI que mantienen la integridad de la información y la seguridad de los datos comúnmente incluyen controles sobre:

- Centro de datos y operaciones en red.
- Adquisición, cambio y mantenimiento de software del sistema.
- Cambio de programas.
- Seguridad del acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de aplicación.

Los controles de las aplicaciones son procedimientos manuales o automatizados que, en general, operan al nivel de proceso del negocio y aplican al procesamiento de transacciones por aplicaciones individuales. Los controles de las aplicaciones pueden ser de prevención o de detección en naturaleza y están diseñados para asegurar la integridad de los registros contables.

En consecuencia, los controles de las aplicaciones se relacionan con procedimientos utilizados para iniciar, registrar, procesar y reportar transacciones u otros datos financieros. Estos controles ayudan a asegurar que las transacciones ocurrieron, están autorizadas, registradas y procesadas en forma completa y exacta. Los ejemplos incluyen verificaciones de edición de datos alimentados, y secuencias numéricas de cheques con seguimiento manual de reportes de excepción o corrección en el punto de alimentación de datos.

3.4.1.5 NORMA INTERNACIONAL DE AUDITORIA 330. RESPUESTA DEL AUDITOR A LOS RIESGOS EVALUADOS.

Respuestas generales

El auditor deberá planear e implementar respuestas generales para tratar los riesgos evaluados de representación errónea de importancia relativa a nivel estado financiero.

Uso de evidencia de auditoría obtenida en auditorías previas

Al determinar si es apropiado usar evidencia de auditoría sobre la efectividad operativa de los controles obtenida en auditorías previas, y, si es así, la duración del periodo que puede pasar antes de volver a someter a prueba un control, el auditor deberá considerar lo siguiente:

- La efectividad de otros elementos de control interno, incluyendo el entorno del control, el monitoreo de controles por la entidad, y el proceso de evaluación del riesgo de la entidad;
- Los riesgos que se originen de las características del control, incluyendo si es manual o automatizado;
- La efectividad de los controles generales de TI;
- La efectividad del control y su aplicación por la entidad, incluyendo la naturaleza y extensión de las desviaciones en la aplicación del control que se observaron en auditorías previas, y si ha habido cambios de personal que afecten de manera importante la aplicación del control;
- Así la falta de un cambio de un control particular plantea un riesgo debido a las circunstancias cambiantes; y
- Los riesgos de representación errónea de importancia relativa y el grado de dependencia del control.

Controles sobre riesgos importantes.

Si el auditor planea apoyarse en los controles sobre un riesgo que el auditor ha determinado que es un riesgo importante, el auditor deberá poner a prueba esos controles en el periodo actual.

Evaluación de la efectividad operativa de los controles.

3.4.1.6 NORMA INTERNACIONAL DE AUDITORÍA 500. EVIDENCIA DE AUDITORÍA

Esta Norma Internacional de Auditoría (NIA) explica lo que constituye evidencia de auditoría en una auditoría de estados financieros, y trata de la responsabilidad que tiene el auditor de diseñar y aplicar procedimientos de auditoría para obtener evidencia de auditoría suficiente y adecuada que le permita alcanzar conclusiones razonables en las que basar su opinión.

Esta NIA es aplicable a toda la evidencia de auditoría obtenida en el transcurso de la auditoría.

El objetivo del auditor es diseñar y aplicar procedimientos de auditoría de forma que le permita obtener evidencia de auditoría suficiente y adecuada para poder alcanzar conclusiones razonables en las que basar su opinión.

3.4.1.7 NORMA INTERNACIONAL DE AUDITORÍA 530. MUESTREO DE AUDITORÍA

Esta Norma Internacional de Auditoría (NIA) es de aplicación cuando el auditor ha decidido emplear el muestreo de auditoría en la realización de procedimientos de auditoría. Trata de la utilización por el auditor del muestreo estadístico y no estadístico para diseñar y seleccionar la muestra de auditoría, realizar pruebas de controles y de detalle, así como evaluar los resultados de la muestra.

3.4.1.8 NORMA INTERNACIONAL DE AUDITORIA 620. USO DEL TRABAJO DE UN EXPERTO

Esta Norma Internacional de Auditoría (NIA) se refiere a las responsabilidades del auditor con respecto al trabajo de una persona u organización en un **campo de especialidad distinto al de la contabilidad o la auditoría**, cuando ese trabajo se utiliza para ayudar al auditor a obtener suficiente evidencia apropiada de auditoría.

3.4.2 DECLARACIONES INTERNACIONALES DE PRÁCTICAS DE AUDITORÍA (DIPA`s)

3.4.2.1 DIPA 1001: Ambientes de SIC-Microcomputadoras independientes.

Describe los efectos que tienen las microcomputadoras independientes sobre:

- El sistema de contabilidad
- Los controles internos relacionados
- Los procedimientos de auditoría

3.4.2.2 DIPA 1002: Ambientes de SIC-Sistema de computadoras en línea.

Describe los efectos de un sistema de computadoras en línea sobre:

- El sistema de contabilidad
- Los controles internos relacionados
- Los procedimientos de auditoría

Los sistemas de computadoras en línea son sistemas de computadora que posibilitan a los usuarios el acceso a datos y programas directamente a través de aparatos terminales. (Computadoras o una red de microcomputadoras interconectadas)

3.4.2.3 DIPA 1003: Ambientes de SIC-Sistema de Base de Datos.

Describe los efectos de un sistema de base de datos sobre:

- El sistema de contabilidad
- Los controles internos relacionados

- Los procedimientos de auditoría

"Una base de datos es una colección de datos que se comparten y se usan entre diferentes usuarios para diferentes fines."

3.4.2.4 DIPA 1008: Evaluación del riesgo y el control interno – características y consideraciones del SIC.

"De acuerdo con NIA`s, existe un entorno SIC cuando hay implicada una computadora de cualquier tipo o tamaño en el procesamiento de información financiera de importancia."

La aplicación de controles deseados en SIC, se ve influida por:

- El tamaño del negocio (si es pequeño);
- Cuando se usan microcomputadoras independientemente del tamaño del negocio; y
- Cuando los datos son procesados por un tercero. (Servicios externos de procesamiento de datos)

3.4.2.5 DIPA 1009: Técnicas de Auditoría con Ayuda del Computador (TAAC`s).

"Son programas y datos de computadora que el auditor usa como parte de los procedimientos de auditoría para procesar datos importantes para la auditoría contenidos en los sistemas de información de una entidad"

3.4.3 NORMAS GENERALES PARA LOS SISTEMAS DE AUDITORÍA DE LA INFORMACIÓN

Emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información (ISACA). Vigentes desde el 25 de Julio de 1997.

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

010 Título de auditoría

010.010 Responsabilidad, autoridad y rendimiento de cuentas

La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

020 Independencia 020.010 Independencia profesional

En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

020.020 Relación organizativa

La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

030 Ética y normas profesionales

030.010 Código de Ética Profesional

El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

030.020 Atención profesional correspondiente

En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

040 Idoneidad

040.010 Habilidades y conocimientos

El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

040.020 Educación Profesional Continua

El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

050 Planificación

050.010 Planificación de la auditoría

El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

060 Ejecución del trabajo de auditoría

060.010 Supervisión

El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

060.020 Evidencia

Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

070 Informes

070.010 Contenido y formato de los informes

En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

080 Actividades de seguimiento

080.010 Seguimiento

El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

3.4.4 NORMAS DE AUDITORÍA DE SI DE LA ASOCIACIÓN DE AUDITORÍA Y CONTROL DE LOS SISTEMAS DE INFORMACIÓN (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, ISACA)

Esta Asociación ha emitido Estándares (Requisitos), Directrices (Guías) y Procedimientos (Ejemplos), para facilitar el trabajo de Auditoria de Sistemas

- **Estándares**

Definen requisitos obligatorios para la auditoría de SI y el informe correspondiente.

- **Directrices**

Proporcionan guías sobre la aplicación de los Estándares de Auditoría de SI. El objetivo es proporcionar mayor información con respecto al cumplimiento de los Estándares de Auditoría de SI.

- **Procedimientos**

Proporcionan ejemplos de procedimientos que podrían seguir un auditor de SI en el curso de una auditoría. El objetivo es proporcionar mayor información con respecto a cómo cumplir con los Estándares de Auditoría de SI.

3.4.4.1 ESTÁNDARES:

S1: El Estatuto de Auditoría.

El propósito de este Estándar de Auditoría de SI es establecer y proporcionar asesoramiento con respecto al Estatuto de Auditoría utilizado durante el proceso de auditoría.

S2: Independencia.

El propósito de esta Norma de Auditoría de SI es establecer estándares y guías relacionadas con la independencia durante el proceso de auditoría.

S3: Ética y Estándares profesionales.

El propósito de esta Norma de Auditoría de SI es establecer un estándar y proporcionar una guía para el auditor de SI con el fin de que cumpla con el Código de Ética Profesional de ISACA y ejerza el debido cuidado profesional al realizar tareas de auditoría.

S4: Competencia profesional.

El propósito de esta Norma de Auditoría de SI es establecer y brindar asesoría a fin de que el auditor de SI logre y mantenga un nivel de competencia profesional.

S5: Planeación.

El propósito de esta Norma de Auditoría de SI es establecer normas y brindar asesoría sobre la planeación de una auditoría.

S6: Ejecución de la auditoría.

El propósito de este Estándar de Auditoría de SI es establecer normas y proporcionar asesoría con respecto a la realización de las labores de auditoría.

S7: Reporte.

El propósito de esta Norma de Auditoría de SI es establecer y proporcionar asesoría sobre la generación del informe, a fin de que el auditor de SI pueda cumplir con esta responsabilidad.

S8: Actividades de seguimiento.

El propósito de esta Norma de Auditoría de SI es establecer normas y proporcionar asesoría con respecto a las actividades de seguimiento realizadas durante un proceso de auditoría de SI.

S9: Irregularidades y acciones ilegales.

El propósito de este estándar de ISACA es establecer y proporcionar asesoría sobre irregularidades y acciones ilegales que el auditor de SI debe tener en cuenta durante el proceso de auditoría.

S10: Gobernabilidad de TI.

El propósito de este estándar de ISACA es establecer y proporcionar asesoría en las áreas de gobernabilidad de TI que el auditor de SI debe tener en cuenta durante el proceso de auditoría.

S11: Uso de la evaluación de riesgos en la planeación de auditoría.

El propósito de este estándar es establecer normas y proporcionar asesoría con respecto al uso de la evaluación de riesgos en la planeación de auditoría.

S12: Materialidad de la auditoría.

El propósito de este estándar de auditoría de SI es establecer y proporcionar una guía con respecto al concepto de materialidad de la auditoría y su relación con el riesgo de auditoría.

S13: Uso del trabajo de otros expertos.

El propósito de este Estándar de Auditoría de SI es establecer y proporcionar asesoramiento al auditor de SI que utilice el trabajo de otros expertos durante una auditoría.

S14: Evidencia de auditoría.

El propósito de este estándar es establecer estándares y proporcionar una guía sobre lo que constituye evidencia de auditoría, y la calidad y cantidad de evidencias de auditoría que deberá obtener el auditor de SI.

S15: Controles de TI.

El propósito de este estándar de ISACA es el de establecer normas y proporcionar guías relativas a los controles de TI.

S16: Comercio electrónico.

El propósito de este estándar de ISACA es el de establecer normas y proporcionar guías relativas a la revisión de entornos de comercio electrónico.

3.4.4.2 DIRECTRICES

G1 Uso del Trabajo de Otros Auditores

G2 Requerimientos de Evidencia de Auditoría

G3 Uso de Técnicas de Ayuda con Computadora (TAAC)

G4 Servicio externo de actividades de SI para otras organizaciones

G5 Carta de Auditoría

G6 Conceptos de materialidad para auditar de SI

G7 Debido Cuidado Profesional

G8 Documentación de Auditoría

G9 Consideraciones de Auditoría para Irregularidades y Actos Ilegales

G10 Muestreo de Auditoría

G11 Efectos de controles generalizados de SI

G12 Relación Organizacional e Independencia

G13 Uso de la Evaluación de Riesgos en la Planeación de Auditoría

G14 Revisión de Sistemas de Aplicación

G15 Planeación revisada

G16 Efectos de terceros en una organización de controles de TI

G17 Efecto del rol de no auditor en la Auditoría de y Aseguramiento de la Independencia Profesional

G18 Gobierno de TI

G19 Irregularidades y actos ilegales

G20 Reporte

G21 Revisión de Sistemas de Recursos de Planeación Empresarial

G22 Revisión de Comercio Electrónico: Empresa–Consumidor

G23 Revisión del Ciclo de Vida de Sistemas

G24 Banca electrónica

G25 Revisión de redes virtuales privadas

G26 Revisión de proyectos de re-ingeniería procesos de negocios

G27 Equipos de Computación Móviles

G28 Informática Forense

G29 Revisión posterior a la implementación

G30 Competencia

G31 Privacidad

G32 Revisión de perspectivas del Plan de Continuidad de Negocios

G33 Consideraciones generales en el uso de internet

G34 Responsabilidad, Autoridad y Rendición de Cuentas

G35 Actividades de Seguimiento

G36 Controles biométricos

G37 Procesos de administración de la configuración

G38 Controles de acceso

G39 Organización de TI

G40 Revisión de la Gestión de Prácticas de Seguridad

G41 Retorno de la Inversión en Seguridad

G42 Aseguramiento continúo

3.4.4.3 PROCEDIMIENTOS

P1 Evaluación de Riesgos de SI

P2 Firma digital

P3 Detección de Intrusos

P4 Virus y otros códigos maliciosos

P5 Auto evaluación del Riesgo de Control

P6 Cortafuegos

P7 Irregularidades y Actos Ilegales

P8 Evaluación de la Seguridad Exámenes de Penetración y Análisis de Vulnerabilidad

P9 Evaluación de Controles de Administración de Metodologías de Encriptación

P10 Control de cambios de Aplicaciones de Negocios

P11 Transferencia Electrónica de Fondos

3.4.5 CODIGO DE ETICA PROFESIONAL DE LA ASOCIACIÓN DE AUDITORÍA Y CONTROL DE LOS SISTEMAS DE INFORMACIÓN (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, ISACA)

ISACA establece este Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de la asociación y/o de los portadores de las certificaciones.

Los miembros y los portadores de las certificaciones de ISACA deberán:

- Apoyar la implementación de y alentar al cumplimiento de los **estándares, procedimientos y controles** apropiados para los sistemas de información.
- Realizar sus funciones con **objetividad, debida diligencia y celo profesional**, de acuerdo con las normas y mejores prácticas profesionales.
- Servir a los **intereses de las partes relevantes** de manera diligente, leal y honesta, manteniendo altos estándares de conducta y carácter, y no ser parte de ninguna actividad deshonrosa para la profesión.

- Mantener la **privacidad y confidencialidad** de la información obtenida en el transcurso de sus funciones a menos que la autoridad legal requiera su divulgación. Dicha información no deberá ser usada para beneficio personal ni divulgada a las partes que no correspondan.
- Mantener la **competencia** en sus respectivos campos y acordar realizar sólo aquellas actividades que de modo razonable puedan esperar cumplir con competencia profesional.
- Informar a las partes apropiadas los **resultados del trabajo realizado**; revelando todos los hechos significativos de los que tengan conocimiento.
- Apoyar la **educación profesional** de los interesados para mejorar su comprensión en seguridad y control de sistemas de información.

El incumplimiento de este Código de Ética Profesional puede resultar en una investigación de la conducta del miembro y/o del portador de la certificación y, finalmente, en medidas disciplinarias.

3.4.6 FASES DE LA AUDITORIA DE SISTEMAS

3.4.6.1 FASE PRE-INICIAL DE AUDITORIA

a) Aceptación del Cliente y/o Continuación (en este caso para Auditoria Externa)

Es importante que el auditor acepte el trabajo sólo cuando exista una seguridad razonable que se pueda confiar en la administración.

En relación con un nuevo cliente, el auditor deberá obtener información acerca de la integridad de la administración si se comunica con el auditor anterior, si esto es posible y después de haber realizado investigaciones con terceros. Con referencia a un cliente que ya se tenía previamente, el auditor revisará su experiencia anterior con los administradores del cliente.

b) Comunicación con el Auditor Anterior:

Respecto a un cliente, que haya auditado, el conocimiento de la administración de éste obtenido por el auditor anterior se considera como una información importante para el nuevo auditor. Antes de aceptar el trabajo se requiere que el nuevo auditor tome la iniciativa de comunicarse, ya sea en forma oral o escrita con el auditor anterior. La comunicación deberá realizarse con el permiso del cliente y debe pedirse a este que autorice al auditor anterior a que conteste plenamente las preguntas del sucesor. La autorización se requiere, dado que el código de ética profesional prohíbe a un auditor revelar, sin el permiso de su cliente, información confidencial obtenida durante una auditoría.

En la comunicación, el nuevo auditor deberá hacer preguntas específicas y razonables con respecto a asuntos que pudieran afectar su decisión de aceptar el trabajo tales como:

- Integridad de la Administración.
- Inconformidades con la administración acerca de principios de contabilidad generalmente aceptados y procedimientos de auditoría.
- La compresión del auditor anterior en relación con el cambio de auditores.

Si el cliente no otorgara la autorización para comunicarse con el auditor anterior o bien el auditor se negara a dar la información solicitada, se deberá pensar seriamente si se acepta o no al nuevo cliente.

c) Investigaciones con Terceras Personas:

También se podrá obtener información acerca de la integridad de la administración, a través de personas conocedoras, tales como abogados, banqueros y otros, dentro de la comunidad financiera y de los negocios, quienes mantienen relaciones comerciales con el futuro cliente.

d) Estudio de Clientes Actuales:

Cuando se va a renovar un contrato de auditoría, se debe de tener presente la experiencia previa que se ha tenido con el mismo. Por ejemplo se deben considerar los errores significativos o irregularidades o actos ilegales descubiertos de auditorías anteriores. Durante un examen, el auditor realizará investigaciones respecto a la administración concernientes a asuntos tales como la existencia de contingencias, lo adecuado o inadecuado de las actas de las juntas del consejo de administración (junta directiva) y el cumplimiento con los requerimientos reguladores.

e) Identificación de las Razones que tiene el Cliente para la Auditoria.

Luego de haber tenido una aceptación del cliente para brindarle el servicio requerido de auditoria de sistemas, es necesario conocer los objetivos que el mismo tiene, o el producto que él espera al final de la auditoria o el motivo por el cual él desea contratar una auditoría. Son muchas las razones para requerir una auditoria de sistemas y aunque reconociendo que en nuestros medios no existe una exigencia legal para el requerimiento de esta auditoria, se puede mencionar una razón y quizá de gran importancia, es que la información financiera y administrativa manipulada o administrada en los últimos tiempos a través de computador es de mucha importancia no solo para la empresa, sino también para terceros que la requieren.

Otra razón para requerir este servicio es el continuo avance de la tecnología que a la vez aumenta el riesgo inherente de la información manejada sobre base de datos.

f) Carta Compromiso:

Debe determinarse los objetivos, responsabilidades y alcance de la auditoría para evitar malos entendidos, respecto del trabajo.

Según La NIA 210 “Términos de Los Trabajos de Auditoria”: La carta compromiso de un auditor a su cliente documenta y confirma su aceptación del nombramiento, el objetivo y alcance de la auditoría, el grado de sus responsabilidades para con el cliente y la forma de cualesquier informes.

Es de interés del cliente como del contador publico y auditor, que el auditor envíe una carta compromiso documentando los términos clave del nombramiento. Una carta compromiso confirma la aceptación por el auditor del nombramiento y ayuda a evitar malos entendidos, respecto de asuntos como los objetivos y alcance del trabajo, el grado de las responsabilidades del auditor y las formas de informe que deben emitirse.

Asuntos que deben incluirse en la carta compromiso.

- Una lista de procedimientos que deben realizarse según se convino entre las partes.
- Una declaración de que la distribución del informe de resultados de hechos debería ser restringida a las partes especificadas que han convenido en que los procedimientos se realicen.
- Además el auditor puede considerar anexar a la carta compromiso un borrador del tipo de informe de resultados de hechos que se emitirá.

3.4.6.2 PLANEACION DE AUDITORIA DE SISTEMAS

a) Objetivos de la Planeación de Auditoria de Sistemas

- Antecedentes de la Empresa y del Centro de Cómputo
- Evaluación administrativa del área de procesos electrónicos.
- Evaluación de los sistemas y procedimientos.

- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos, de los sistemas y de los equipos de cómputo.
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Estos objetivos son los que garantizan una buena auditoria informática, es necesario utilizarlos de guía para determinar lo que ocurre en lo relacionado al procesamiento de datos y así el auditor pueda desempeñar su trabajo con la calidad y la efectividad esperada.

b) Evaluacion de Control Interno

El Control Interno se evalúa en informática a través de:

- **Cuestionarios**
- **Check List**
- **Entrevistas**
- **Bitácoras de acceso**

c) Identificación de Áreas Críticas

La evaluación del control interno proporciona la base para determinar el riesgo existente en cada área a examinar, así mismo conocer sus incidencias en el funcionamiento del sistema, y de las políticas y procedimientos establecidos para los sistemas de información computarizados.

Después de analizar los sistemas de información computarizados de la compañía, determinamos los riesgos en las principales áreas de los sistemas y se bebe poner énfasis en las áreas críticas o de mayor riesgo.

Para establecer un área crítica el auditor debe considerar la fragilidad de acuerdo a los niveles de seguridad; a través de las fallas de control interno, las fallas del sistema y la probabilidad de error.

- **Ejemplo de las principales áreas críticas de los sistemas**

Entre las principales áreas críticas en los sistemas se encuentran: **las operaciones de procesamiento, debido a que se considera como un punto susceptible además de vital importancia en la generación de información confiable y para los cuales debe contarse con controles encaminados a minimizar riesgos en los sistemas y su entorno; así también se consideran áreas críticas la seguridad lógica y la seguridad física de los sistemas.**

d) Evaluacion del Riesgo Informático

De acuerdo con la NIA 315 "Evaluación del riesgo y control interno", el auditor debería hacer una evaluación de los riesgos inherentes y de control, además el auditor debería considerar el ambiente SIC al diseñar los procedimientos de auditoria para reducir el riesgo de a un nivel aceptablemente bajo.

Al determinar que áreas funcionales deben auditarse, el auditor de sistemas debe evaluar todos los riesgos que pueden existir.

Existen tres motivos por los que se utiliza la evaluación de riesgos, estos son:

- Permitir que la gerencia asigne recursos necesarios para la auditoria.
- Garantizar que se ha obtenido la información pertinente
- Garantiza que las actividades de la función de auditoria se dirigen correctamente a las áreas de alto riesgo.

El nivel de importancia se determinará a juicio del auditor y dependerá del área del sistema de información que se está evaluando, por lo que se incluirán aquellos componentes que tengan materialidad sobre la evaluación.

El nivel de riesgo de detección se establecerá de acuerdo al nivel de riesgo inherente y al nivel de riesgo de control.

La determinación del riesgo se realiza de diversas formas, una de ellas es utilizando una matriz de riesgo.

e) Programas de Auditoria

Se requieren varios pasos para realizar una auditoria; el auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoria que consta de objetivos de control y procedimientos de auditoria que deben satisfacer esos objetivos. El proceso de auditoria exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoria que presente esos temas en forma objetiva a la gerencia.

Asimismo, la gerencia de auditoria debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoria además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

e.1) Aspectos del ambiente informático que afectan el enfoque de la auditoria y sus procedimientos.

- Complejidad de los sistemas.
- Uso de lenguajes.
- Metodologías, son parte de las personas y su experiencia.
- Centralización de funciones.
- Controles del computador.
- Controles manuales y controles automatizados (procedimientos programados).
- Confiabilidad electrónica.
- Debilidades de las máquinas y tecnología.

- Transmisión y registro de la información en medios magnéticos, óptico y otros.
- Almacenamiento en medios que deben acceder a través del computador mismo.
- Centros externos de procesamiento de datos.
- Dependencia externa.

Un programa de auditoria es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoria planificados. El esquema típico de un programa de auditoria incluye lo siguiente:

- Tema de auditoria: Donde se identifica el área a ser auditada.
- Objetivos de Auditoria: Donde se indica el propósito del trabajo de auditoria a realizar.
- Planificación previa: Donde se identifican los recursos y destrezas que se necesitan para realizar el trabajo; así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
- Procedimientos de auditoria:
    - Recopilación de datos.
    - Identificación de lista de personas a entrevistar.
    - Identificación y selección del enfoque del trabajo
    - Identificación y obtención de políticas, normas y directivas.
    - Desarrollo de herramientas y metodología para probar y verificar los controles existentes.
    - Procedimientos para evaluar los resultados de las pruebas y revisiones.
    - Procedimientos de comunicación con la gerencia.
    - Procedimientos de seguimiento.

El programa de auditoria se convierte también en una guía para documentar los diversos pasos de auditoria y para señalar la ubicación del material de evidencia.

f) Personal Asignado

El perfil que se requiere para llevar a cabo auditorias de sistemas de información no esta regulado, pero es evidente que son necesarias una formación y sobre todo una experiencia acordes con la función, e incluso con las áreas a auditar seguridad física, sistemas operativos concretos, determinamos gestores de bases de datos o plataformas, e incluso lenguajes si hubiera que llegar a revisar programas, además de ser imprescindibles en el perfil otras características o circunstancias comunes, como independencia respecto a los auditados, madurez, capacidad de análisis y de síntesis, e intereses no meramente económico.

En el seno de la citada ISACA existe un certificado relacionado: CISA (Certified Information Systems Auditor).

g) Programación de la Auditoria

Dentro de la planeación de auditoria a los sistemas de información computarizados, es necesario incluir la programación del trabajo, en la cual se estipulan los procedimientos a seguir para identificar el cumplimiento del control interno, la calidad del funcionamiento del sistema y las evidencias que permitan formular una conclusión acertada sobre el funcionamiento del sistema en las fechas claves que debe hacerse.

3.4.6.3 EJECUCION DE AUDITORIA

En esta fase se realizan pruebas y análisis a los sistemas de información computarizados, para determinar su funcionabilidad y razonabilidad; a través de los diferentes componentes en la fase de ejecución, entre estos se encuentran:

- **Las pruebas de auditoria.**
- **Técnicas de muestreo.**

- **Obtención de evidencias de auditoria.**
- **Elaboración de Papeles de trabajo.**
- **Determinación de Hallazgos de auditoria.**

Se detectan los errores, si los hay, se evalúan los resultados de las pruebas y se identifican los hallazgos.

En ésta fase se elaboran las conclusiones y recomendaciones que se comunicarán a las autoridades de la entidad auditada.

Aunque las tres fases son importantes, esta fase viene a ser el centro de lo que es el trabajo de auditoria, donde se realizan todas las pruebas y se utilizan todas las técnicas o procedimientos para encontrar las evidencias de auditoria que sustentarán el informe de auditoria.

a) Procedimientos Tradicionales y uso de Técnicas de Auditoría Asistidas por Computadora (TAAC) para obtener evidencia suficiente y apropiada.

El auditor obtiene evidencia de auditoría para llegar a conclusiones razonables en las cuales basar la opinión de auditoría mediante el desempeño de procedimientos de auditoría para:

• **Obtener un entendimiento de la entidad y su entorno, incluyendo su control interno, para valuar riesgos de presentación errónea de importancia relativa a los niveles de los estados financieros y de aseveración:**

Estos procedimientos de auditoría desempeñados para este fin se citan en las NIAS como procedimientos de evaluación de riesgo.

• **Cuando es necesario o cuando el auditor haya determinado hacerlo así, hacer pruebas de la efectividad operativa de los controles para prevenir o detectar y**

corregir, representaciones erróneas de importancia relativa al nivel de aseveración.

• **Detectar representaciones erróneas de importancia relativa al nivel de aseveración:**

Por lo tanto la evidencia de auditoria se obtiene de una combinación apropiada de procedimientos de evaluación de riesgo, pruebas de control y de pruebas sustantivas.

Cuando la información esta en forma electrónica, el auditor puede llevar a cabo ciertos procedimientos de auditaría a través de las TAAC´S.

b) El auditor usa una o más tipos de los procedimientos de auditoría que se describen a continuación:

• Inspección de registros o documentos:

Consiste en examinar registros o documentos ya sean internos o externos en forma impresa, electrónica o en otros medios. La inspección de registro de documentos proporciona evidencia de grados variables de confiabilidad dependiendo de su naturaleza y fuente y en el caso de registros de documentos internos, de la efectividad de los controles sobre su producción.

• Inspección de activos tangibles:

La inspección de activos tangibles puede proporcionar evidencia de auditoría confiable respecto a existencia, pero no necesariamente sobre los derechos y obligaciones o valuación de los activos.

• Observación:

Esta consiste en mirar un proceso o procedimiento que es desempeñado por otros.

• Investigación:

Consiste en buscar información de personas bien formada, tanto en lo financiero como en lo no financiero, en la entidad o fuera de ella, se usa de manera extensa en

toda la auditoría y es complementaria al desempeño de otros procedimientos de auditoría.

• **Volver a calcular:**

Este procedimiento consiste en verificar la exactitud matemática de los documentos o registros. El nuevo cálculo puede desempeñarse mediante el uso de tecnología de información.

• **Volver a desarrollar**:

Consiste en la ejecución de por el auditor de procedimientos o controles que originalmente se desarrollaron como parte del control interno de la entidad ya se manual o con el uso de TAAC`s.

• **Procedimientos analíticos:**

Consisten en la evaluación de información financiera hechas por un estudio de relaciones plausibles entre los datos financieros y no financieros.

Según Normas Internacionales de Auditoría las TAACs son programas y datos de computadora que el auditor usa como parte de los procedimientos de auditoría para procesar datos importantes para la auditoría contenidos en un sistema de información de una entidad.

El uso de técnicas de auditoría asistidas por computadora ("TAACs"), puede ser una forma efectiva de evaluar controles automatizados. TAACs incluye, por ejemplo, el desarrollo de una prueba integrada y el procesamiento de transacciones de pruebas en el sistema. La ventaja de utilizar TAACs en pruebas de controles es que es posible revisar cada transacción (bien sea en un archivo maestro o en un archivo de transacciones), para determinar si existen fallas en los controles.

c) Las diferentes TAACs utilizadas son:

- **Lote de Datos de Prueba**
- **Datos de Prueba Integrados**

- **Simulación Paralela**
- **Flujogramas o Diagramas**
- **Dígito Verificador**
- **Imagen del Contenido de la Memoria**
- **Seguimiento o Rastreo**
- **Bitácora y Programas Especiales**
- **Mapeo, Programas Utilitarios y paquetes de Auditoría.**
- **Compilación y Comparación**
- **Registros Extendidos**
- **Correlación**
- **Prueba de Sistemas en línea**
- **Rutina Incorporada**
- **Selección de Transacciones**

d) PROCEDIMIENTOS EN LA EVALUACION DE LA SEGURIDAD FISICA Y LOGICA:

d.1) PROCEDIMIENTOS PARA LA AUDITORIA DE LA SEGURIDAD FÍSICA.

Se evaluaran las protecciones físicas de datos, programas instalaciones, equipos redes y soportes, y por supuesto habrá que considerar a las personas, que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector.

d.2) PROTECCIONES FÍSICAS ALGUNOS ASPECTOS A CONSIDERAR:

- Ubicación del centro de procesos, de los servidores locales, y en general de cualquier elemento a proteger.

- Estructura, diseño, construcción y distribución de los edificios y de sus platas.
- Riesgos a los accesos físicos no controlados.
- Amenaza de fuego, problemas en el suministro eléctrico.
- Evitar sustituciones o sustracción de quipos, componentes, soportes magnéticos, documentación u otros activos.

d.3) PROCEDIMIENTOS PARA LA AUDITORIA DE LA SEGURIDAD LOGICA.

Es necesario verificar que cada usuario solo pude acceder a los recursos que se le autorice el propietario, aunque sea de forma genérica, según su función, y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución, traslado a los sistemas lo que representaríamos en una matriz de accesos.

En cuanto a autenticación, hasta tanto no se abaraten más y generalicen los sistemas basados en la biométrica, el método más usado es la contraseña,

Cuyas características serán acordes con las normas y estándares de la entidad, que podrían contemplar diferencias para según qué sistemas en función de la criticidad de los recursos accedidos.

d.4) ASPECTOS A EVALUAR RESPECTO A LAS CONTRASEÑAS PUEDEN SER:

- Quien asigna la contraseña inicial y sucesivas.
- Longitud mínima y composición de caracteres.
- Vigencia, incluso puede haberlas de un solo uso o dependientes de una función tiempo.
- Control para no asignar las “x” ultimas.
- Numero de intentos que se permiten al usuario.
- Controles existentes para evitar y detectar caballos de Troya.

d.5) AUDITORIA DE LA SEGURIDAD Y EL DESARROLLO DE APLICACIONES.

Todos los desarrollos deben estar autorizados a distinto nivel según la importancia del desarrollo a abordar, incluso autorizados por un comité si los costes o los riesgos superan unos umbrales.

- ***REVISION DE PROGRAMAS***

Por parte de técnicos independientes, o bien por auditores, preparados, a fin de determinar la ausencia de "caballos de Troya", bombas lógicas y similares además de la calidad.

- ***PROTECCION DE LOS PROGRAMAS***

A menos desde dos perspectivas, de los programas que sean propiedad de la entidad, realizados por e personal propio o contratado d e su desarrollo a terceros, como el uso adecuado de aquellos programas de los que se tenga licencia de uso

d.6) AUDITORIA DE SEGURIDAD EN EL AREA DE PRODUCCION.

Las entidades han de cuidar especialmente las medidas de protección en el caso de contratación de servicios: desde el posible marcado de datos, proceso, impresión de etiquetas, distribución, acciones comerciales, gestión de cobros, hasta el outsourcing mas completo, sin descartar que en el contrato se provea la revisión por los auditores, internos o externos, de las instalaciones de la entidad que provee el servicio.

También debe realizarse la protección de utilidades o programas especialmente peligrosos, así como el control de generación y cambios posteriores de todo el software de sistemas, y de forma especial el de control de accesos.

d.7) AUDITORIA DE LA SEGURIDAD DE LOS DATOS.

La protección de los datos puede tener varios enfoques respecto a las características citadas: la confidencialidad, disponibilidad e integridad. Puede haber datos críticos en cuanto a su confidencialidad, como datos médicos u otros especialmente sensibles (sobre religión, sexo, raza) otros datos cuya criticidad viene dada por la disponibilidad: si se pierden o se pueden utilizar a tiempo pueden causar perjuicios

graves y, en los casos mas extremos poner en peligro la comunidad de la entidad y finalmente otros datos críticos atendiendo a su integridad, especialmente cuando su perdida no puede detectarse fácilmente o una vez detectada no es fácil reconstruirlos.

Desde el origen del dato, que puede ser dentro o fuera de la entidad, y puede incluir preparación, autorización, incorporación al sistema: por el cliente, por empleados, o bien ser captado por otra forma, y debe revisarse como se verifican los errores.

- ***Proceso de los datos:***

Controles de validación, integridad, almacenamiento: que existan copias suficientes, sincronizadas y protegidas.

- ***Salida de resultados:***

Controles en transmisiones, en impresión, en distribución.

Retención de la información y protección en funciona de su clasificación: destrucción de los diferentes soportes que la contengan cuando ya no sea necesaria, o bien desmagnetización.

- ***Designación de propietarios:***

Clasificación de los datos, restricción de su uso para pruebas, inclusión de muescas para poder detectar usos no autorizados.

- ***Clasificación de los datos e información:***

Debe revisarse quien la ha realizado y según que criterios y estándares; no suele ser práctico que haya más de cuatro o cinco niveles.

- ***Cliente-servidor:***

Es necesario verificar los controles en varios puntos, y no solo en uno central como en otros sistemas, y a veces en plataformas heterogéneas, con niveles y características de seguridad muy diferentes, y con posibilidad de transferencia de ficheros o de

captación y exportación de datos que pueden perder sus protecciones al pasar de una plataforma a otra.

d.8) AUDITORIA DE LA SEGURIDAD EN COMUNICACIONES Y REDES.

En las políticas de entidad debe reconocerse que los sistemas, redes y mensajes transmitidos y procesados son propiedad de la entidad y no deben usarse para otros fines no autorizados, por seguridad y por productividad, talvez salvo emergencias concretas si allí se ha especificado y mas bien para comunicaciones con voz.

Los usuarios tendrán restricción de accesos según dominios, únicamente podrán cargar los programas autorizados, y solo podrán variar las configuraciones y componentes los técnicos autorizados.

Se revisaran especialmente las redes cuando existan repercusiones económicas por que se trate de transferencia de fondos o comercio electrónico. Puntos a revisar:

- Tipos de redes y conexiones
- Tipos de transacciones.
- Tipos de terminales y protecciones: físicas, lógicas, llamadas de retorno.
- Transferencia de ficheros y controles existentes.
- Consideración especial respecto a las conexiones externas a través de pasarelas (gateway) y encaminadores (routers).
    - ***Internet e Intranet:***

Separación de dominios e implantación de medidas especiales, como normas y cortafuegos (firewall), y no solo en relación con la seguridad sino por acceso no justificados por la función desempeñada, como a páginas de ocio o eróticas, por lo que pueden suponer para la productividad.

- ***Correo electrónico:***

Tanto por privacidad y para evitar virus como para que el uso del correo sea adecuado y referido ala propia función, y no utilizado para fines particulares.

- ***Protección de programas:***

Tanto la prevención del uso no autorizado de programas propiedad de la entidad o de los que tengan licencia de uso.

- ***Control sobre las paginas Web:***
  Quien puede modificarlo y desde donde, finalmente preocupan también los riesgos que pueden existir en el comercio electrónico.

d.9) AUDITORIA DE LA CONTINUIDAD DE LAS OPERACIONES.

Es uno de los puntos que nunca se deberían pasar por alto en una auditoria de seguridad, por las consecuencias que puede tener el no haberlo revisado o haberlo hecho sin la suficiente profundidad: no basta con ver un manual cuyo titulo sea plan de contingencia o denominación similar, sino que es imprescindible conocer si funcionaria con las garantías necesarias y cubrirá los requerimientos en un tiempo inferior al fijado y con una duración suficiente.

En una auditoria de seguridad, las consecuencias que puede tener el no haberlo revisado o haberlo hecho sin la suficiente profundidad: no basta con ver un manual cuyo titulo sea plan de contingencia o denominación similar, sino que es imprescindible conocer si funcionaria con las garantías necesarias y cubriría los requerimientos en un tiempo inferior al fijado y con una duración suficiente.

d.10) EVALUACION DEL PLAN DE CONTINGENCIA O PLAN DE CONTINUIDAD

En la auditoria es necesario revisar si existe tal plan, completo y actualizado, si cubre los diferentes procesos, áreas y plataformas, si existen planes diferentes según

entornos, evaluar en todo caso su idoneidad, los resultados de las pruebas que se hayan realizado, y si permiten garantizar razonablemente que en caso necesario y a través de los medios alternativos, propios o contratados, podría permitir la reanudación de las operaciones en un tiempo inferior al fijado por los responsables del uso de las aplicaciones, que a veces son también los propietarios de las mismas pero podrían no serlo.

Un punto fundamental en la revisión es la existencia de copias actualizadas de los recursos vitales en un lugar distante y en condiciones adecuadas tanto físicas como de protección en cuanto a accesos; entre dichos recursos estarán: bases de datos y ficheros, programas (mejor si existen también en versión fuente), JCL (Job Control lenguaje) o el equivalente en cada sistema, la documentación necesaria, formularios críticos y consumibles o garantías de que se servirían a tiempo, documentación, manuales técnicos, direcciones y teléfonos, los recursos de comunicaciones necesarios; datos y voz cualesquiera otros requeridos para funcionar con garantías.

e) PAPELES DE TRABAJO

Entender los pasos del proceso de auditoria del área de sistemas de información computarizados permite a los administradores del sistema saber lo que deben esperar de la auditoria; de esta forma pueden lograr los objetivos de cumplimiento normativo de su empresa y optimizar el proceso de auditoria para completarlo más eficazmente; posteriormente entregar a la gerencia un informe final con relación a lo auditado.

El legajo de los papeles de trabajo, por su naturaleza y contenido, es el aspecto fundamental para elaborar el informe de auditoria, y su uso es confidencial y exclusivo del auditor de sistemas. El contenido de los papeles de trabajo puede variar de un auditor a otro, ya que en cada auditoria existen técnicas, procedimientos y métodos de evaluación especiales, que obtienen diferente tipo de evidencia.

Entre alguna documentación que forman los papeles de trabajo están:

- Hoja de identificación
- Índice de contenido de los papeles de trabajo
- Resumen de deficiencias de control
- Programas de trabajo de auditoria
- Manual de organización
- Descripción organizacional del centro de cómputo
- Reporte de pruebas y resultados del sistema
- Respaldos (backup) de datos, disquetes, CD y programas de aplicación de auditoria
- Respaldo (backup) de las bases de datos y de los sistemas
- Guía de claves para el señalamiento de los papeles de trabajo
- Diagramas de flujos, de programas y de desarrollo de sistemas
- Testimonios, actas y documentos legales de comprobación y confirmación
- Análisis y estadísticas de resultados, datos y pruebas de comportamiento del sistema
- Otros documentos de apoyo para el auditor

En una auditoria de sistemas los papeles de trabajo representan el sustento para registrar los datos e información que se van recolectando durante la evaluación, por la especialidad de medios que se usan para el registro de la información de las áreas de cómputo, la recopilación de datos se puede realizar en documentos o medios electromagnéticos de captura y resguardo de datos, estos pueden ser discos duros, discos flexibles, cintas, CD-ROM, DVD, y otros medios electromagnéticos.

Existen múltiples formas de elaborar y utilizar los papeles de trabajo, las cuales estarán determinados por la experiencia, habilidad y conocimiento del auditor. La

obtención del legajo de papeles de trabajo dependerá de la astucia del auditor y de la necesidad del documento.

f) HALLAZGOS

Es el resultado de la comparación que se realiza entre un criterio y la situación actual encontrada durante el examen a un área, actividad u operación.

Los requisitos que deben reunir un hallazgo de auditoría son:

- Importancia relativa que amerite ser comunicado.
- Basado en hechos y evidencias precisas que figuran en los papeles de trabajo.

3.4.6.4 INFORME Y CARTA A LA GERENCIA.

a) Informe

En ésta etapa el auditor elaborará el informe de auditoría siendo el producto final de su trabajo, el cual contendrá el desarrollo de los hallazgos sobre aspectos de seguridad, de control interno del área de sistemas y aspectos relacionados, que resulten como producto de la aplicación de los procedimientos de auditoría, asimismo presentará conclusiones y recomendaciones para subsanar las deficiencias obtenidas.

El auditor del área de sistemas generalmente prepara el informe de auditoría con la estructura siguiente: portada, índice, introducción, encabezado, objetivos de la auditoría, áreas a auditar, alcance y limitaciones del trabajo, desarrollo de hallazgos, comentarios de la administración, conclusiones, recomendaciones, fecha, firma del auditor y anexos.

El informe de auditoria un documento formal que utiliza el auditor de sistemas para informar por escrito y de manera oportuna, precisa, completa, sencilla y clara, sobre

los resultados que obtuvo después de haber aplicado las técnicas, métodos y procedimientos apropiados al tipo de revisión que realizó, para fundamentar con ellos su opinión respecto a la auditoría realizada y estar en condiciones de poder emitir un dictamen correcto sobre el comportamiento del sistema, sobre los empleados del área de sistemas y sobre los resultados obtenidos de su operación normal, a fin de que el alto funcionario del cliente que reciba el informe conozca la situación real del área de sistemas auditada.

- **Consideraciones Respecto al Informe.**

En él se harán constar los antecedentes y los objetivos, para que quienes lean el informe puedan verificar que ha habido una comunicaron adecuada, así como que metodología de evaluación de riesgos y estándares se ha utilizado, y una breve descripción de los entornos revisados para que se pueda verificar que se han revisado todas las plataformas y sistemas objeto de la auditoria.

Debe de incluirse un Resumen para la Dirección en términos no técnicos.

Dependiendo de los casos será preferible agrupar aspectos similares; seguridad física, seguridad lógica o bien clasificar los puntos por centros o redes, especialmente en entidades grandes si existen responsables diferentes: en caso de duda será un punto a comentar previamente con quienes van a recibir el informe, ya que con frecuencia prefieren entregar a cada uno la parte que mas le afecte, así como planificar y controlar área por área o por departamentos la implantación de medidas.

Cada punto que se incluya debe explicarse porque es un incumplimiento o una debilidad, así como alguna recomendación, a veces abarcando varios puntos.

El informe ha de ser necesariamente revisado por los auditados, así como discutido si es necesario antes de emitir el definitivo.

En muchos casos, bien en el propio informe o en otro documento, se recogen las respuestas de los auditados, sobre todo cuando la auditoria es interna.

La entidad decide que acciones tomar a partir del informe, y en el caso de los auditores internos estos suelen hacer también un seguimiento de las implantaciones.

Los auditados siempre buscan un informe lo mas benigno posible, mientras que los auditores se proponen llegar a un informe veraz y útil; estos diferentes puntos de vista a veces crean conflictos en el proceso de auditoria y en la discusión del informe.

b) Carta a la Gerencia

Es un documento en el cual, se presenta a la gerencia deficiencias menores que fueron detectadas en la evaluación realizada dentro de la auditoria, las cuales por su naturaleza, frecuencia y materialidad no se reportan como hallazgo en el informe final, seguido de la recomendación para subsanar dichas deficiencias.

CAPITULO IV ANALISIS E INTERPRETACION DE RESULTADOS

4. ANALISIS E INTERPRETACIN DE RESULTADOS.

4.1 SEGURIDAD INFORMATICA.

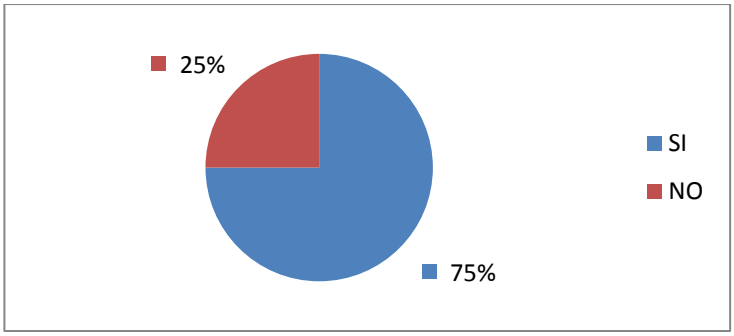
A. PREGUNTA Nº 1: ¿Cuenta con Seguridad Informática en su Empresa?

B. OBJETIVO: Determinar si las Empresas objeto de estudio cuentan con Seguridad Informática.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	9	75%
NO	3	25%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: De acuerdo a los resultados obtenidos en la mayoría de las empresas encuestadas cuentan con Seguridad Informática, el 75% respondió afirmativamente, el 25% respondió que no se cuenta con Seguridad Informática.

F. INTERPRETACION: Por la naturaleza de las operaciones que realizan las Empresas Distribuidoras de Telefonía Móvil, se debe contar con un sofisticado y eficiente sistema de Seguridad Informática, con el objeto de minimizar riesgos y/o amenazas a los Sistemas.

4.2 MANUAL DE SEGURIDAD.

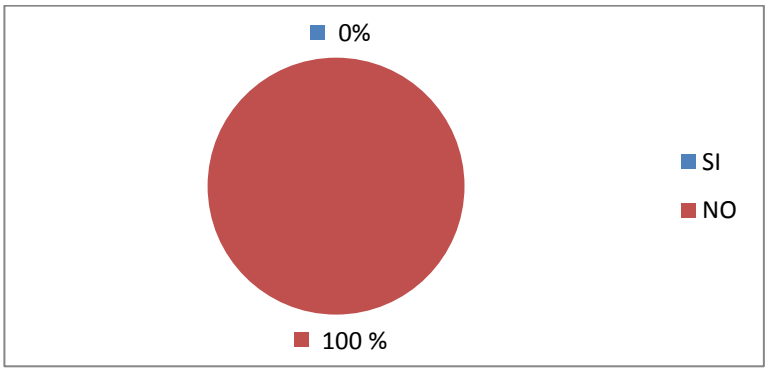
A. **PREGUNTA Nº 2:** ¿Si la repuesta anterior es afirmativa, tiene un Manual por escrito de dicha Seguridad?

B. **OBJETIVO:** Determinar si las Empresas objeto de estudio cuentan con un Manual por escrito de Seguridad Informática.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	0	0%
NO	12	100%
TOTALES.	**12**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** En base a la respuesta obtenida en ninguna de las Empresas encuestadas tienen documentado los mecanismos de Seguridad Informática. Los resultados son el 100% dijo que no cuentan con un Manual por escrito de Seguridad Informática.

F. **INTERPRETACION.** Se hace necesario que una empresa tenga un Instrumento Documental (Manual), que haga referencia a medidas de Seguridad Informática, ya que con ello se pueden prevenir riesgos de pérdida de la información que cotidianamente pueden darse en el desarrollo de las actividades operativas, administrativas y contables.

4.3 SERVICIO INFORMATICO.

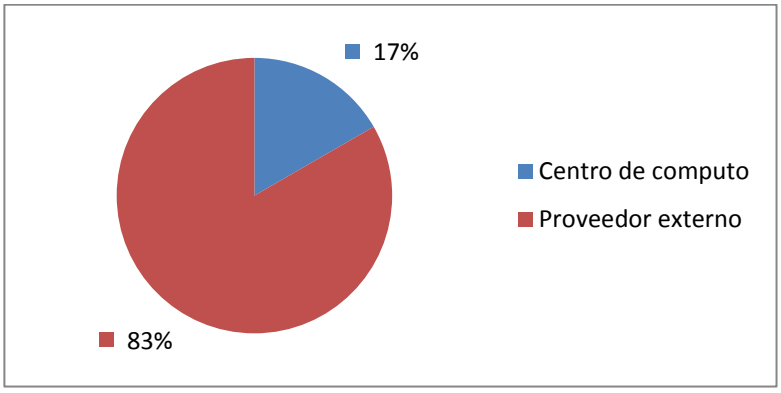
A. **PREGUNTA Nº 3:** ¿Por quién es proporcionado el Servicio Informático de la Empresa en que labora?

B. **OBJETIVO:** Saber quién es el que proporciona el Servicio Informático a las diferentes Empresas encuestadas.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
CENTRO DE COMPUTO	2	17%
PROVEEDOR EXTERNO	10	83%
TOTALES.	**12**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** De acuerdo a los resultados obtenidos el 83% de los encuestados dijo que un Proveedor Externo es quien suministra el Servicio Informático a la Empresa, mientras que el 17% dijo que el Servicio Informático es brindado por el Centro de Cómputo.

F. **INTERPRETACION:** El Servicio Informático puede ser proporcionado por Proveedor Externo o de manera interna (Centro de Cómputo), en ambos casos debe hacerse hincapié sobre la Seguridad Informática.

4.4 PROGRAMAS UTILIZADOS.

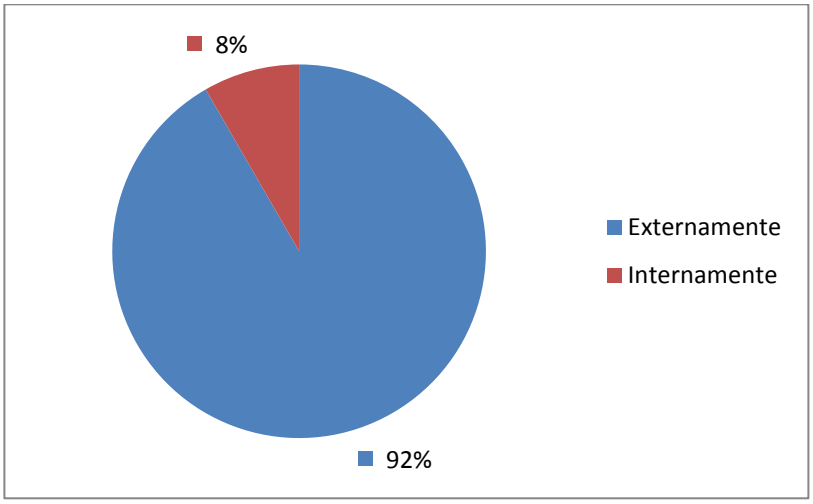
A. PREGUNTA Nº 4: ¿Los Programas utilizados en el Sistema que tiene su Empresa, son creados Internamente o Externamente?

B. OBJETIVO: Determinar quiénes son los responsables de crear los Sistemas que se utilizan para procesar la Información de cada Empresa encuestada.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
EXTERNAMENTE	11	92%
INTERNAMENTE	1	8%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 92% de las Empresas encuestadas manifiesta que los Programas utilizados son creados Externamente, mientras que el 8% de esas Empresas dijo los Programas con creados Internamente.

F. INTERPRETACION: Los Programas Informáticos son de vital importancia para el normal funcionamiento de las Empresas. Si estos son creados externamente se debe tener mas cuidado por la dependencia que se tiene del Proveedor.

4.5 PERSONAL INFORMATICO.

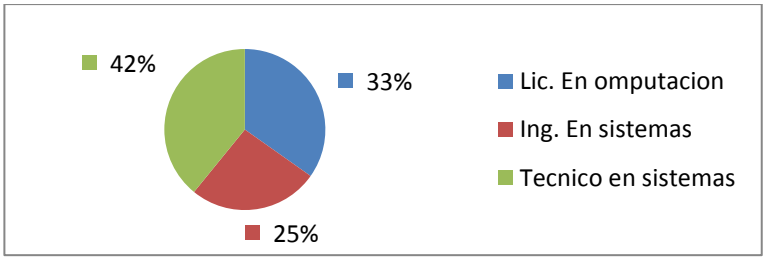
A. PREGUNTA Nº 5: ¿Cuenta con el siguiente Personal Informático en la Empresa: Lic. En Computación, Ing. En Sistemas, Técnico en Sistemas?

B. OBJETIVO: Saber el nivel de preparación de las personas que integran el Centro de Computo de las Empresas encuestadas.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
LIC. EN COMPUTACION	4	33%
ING. EN SISTEMAS	3	25%
TECNICO EN SISTEMAS	5	42%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 42% manifiesta que el personal Informático de la Empresa tiene el grado de Técnico en Sistemas, el 33% dijo que son Licenciado en Computación, mientras que el 25% dijo que el grado académico del personal es Ingeniería En Sistemas.

F. INTERPRETACION: Para que la consecución de actividades Informáticas de una Empresa sean llevadas a cabo de forma efectiva y eficiente debe contar en su mayoría con Personal Informático sean estos Licenciados en Computación e Ingenierías en Sistemas y personal en el nivel de Técnico en Sistemas.

4.6 MEDIDAS DE SEGURIDAD FISICA.

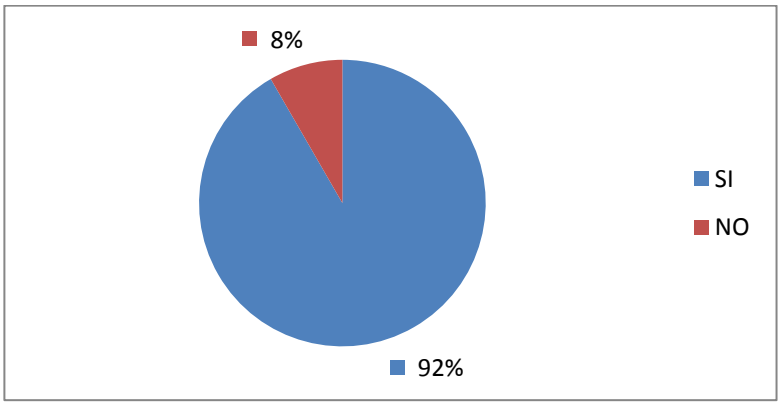
A. PREGUNTA Nº 6: ¿Conoce si existen Medidas de Seguridad Física en la Empresa donde labora?

B. OBJETIVO: Determinar si el personal de las Empresas encuestadas sabe si existen Medidas de Seguridad Física en las instalaciones donde se llevan a cabo las Actividades.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	11	92%
NO	1	8%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: EL 92% de los encuestados enfatiza que en la Empresa si existen Medidas de Seguridad Física, el 8% respondieron que no conocen las Medidas de Seguridad Física.

F. INTERPRETACION: Las Medidas de Seguridad Física, son Mecanismos que se utilizan con el objetivo de proteger los Medios Materiales (Bienes Muebles e Inmuebles) donde la Empresa opera y lleva a cabo en control su Información.

4.7 MEDIDAS DE SEGURIDAD LOGICA.

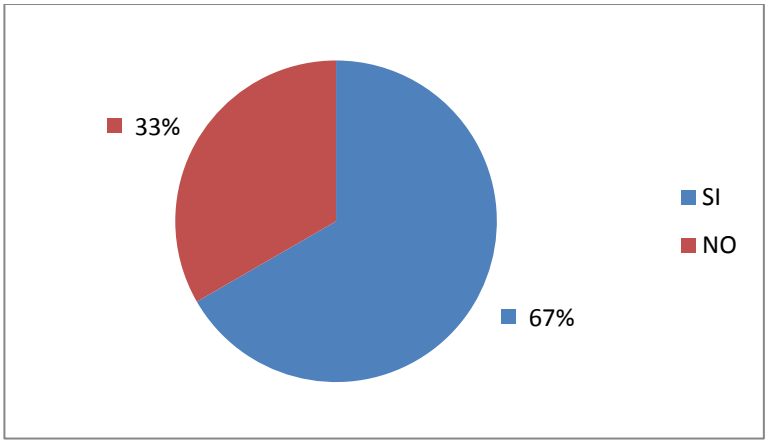
A. PREGUNTA Nº 7: ¿Conoce las Medidas de Seguridad Lógica?

B. OBJETIVO: Saber si el personal tiene conocimiento de las Medidas de Seguridad Lógica que se tiene en la Empresa donde laboran.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	8	67%
NO	4	33%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 67% de los encuestados manifiesta que si conoce las Medidas de Seguridad Lógica de la Empresa. El 33% dijo que no conoce las Medidas de Seguridad Lógica.

F. INTERPRETACION: Las Medidas de Seguridad Lógica, son Mecanismos de Control Interno que se utilizan con el objetivo de proteger los Programas o Sistemas en que la Empresa Opera para el desarrollo de sus actividades. Es importante que el personal de una Empresa conozca las Medidas de Seguridad Lógica que salvaguarden la Información que se obtiene del desarrollo de actividades.

4.8 EQUIPOS PARA LA SEGURIDAD INFORMATICA.

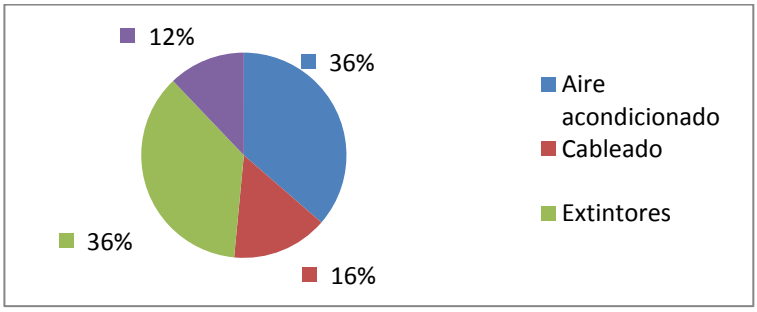
A. **PREGUNTA Nº 8:** ¿Existen las siguientes Equipos en el Centro de Cómputo: Aire Acondicionado, Cableado, Extintores, Suministro de Energía?

B. **OBJETIVO:** Determinar si en la Empresa tienen algunos Equipos que están directamente relacionados con la Seguridad Física en una Empresa.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
AIRE ACONDICIONADO	12	36%
CABLEADO	5	16%
EXTINTORES	12	36%
SUMINISTROS DE ENERGIA	4	12%
TOTALES.	**33**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** El 36% tiene en el Centro de Computo Aire Acondicionado, otro 36% tiene Extintores, el 16% dice que tiene Cableado y el 12% restante Suministros de Energía.

F. **INTERPRETACION:** Los Equipos Electrónicos o no Electrónicos, que debe tener un Centro de Cómputo es para mantener en buen estado los Equipos Informáticos y aquellos que pueden ser de alto grado de vulnerabilidad.

4.9 PROTECCION DEL EDIFICIO.

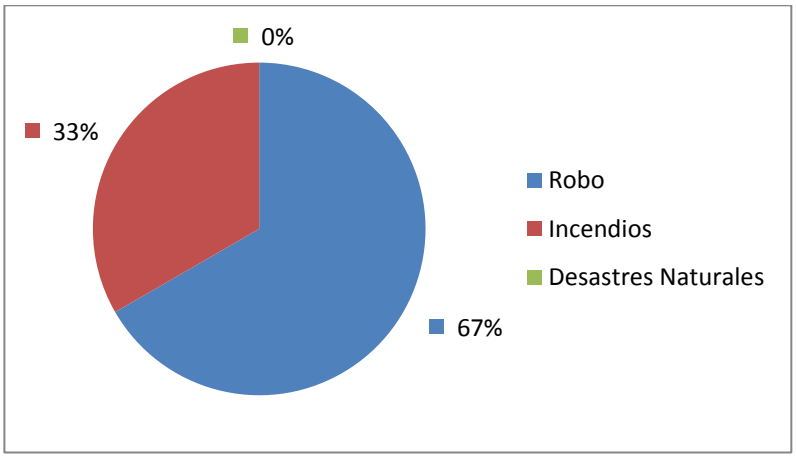
A. PREGUNTA Nº 9: ¿El Edificio de la Empresa, está protegido contra los siguientes siniestros: Robos, Incendios, Desastres Naturales?

B. OBJETIVO: Determinar qué tipo de Medidas toma la Empresa para salvaguardar la infraestructura de su Edificio.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
ROBO	12	67%
INCENDIO	6	33%
DESASTRES NATURALES	0	0%
TOTALES.	**18**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 67% de los encuestados afirma que las Instalaciones de los Edificios están protegidos contra Robo, el 33% están protegidos contra Incendios y el 0% contra Desastres Naturales.

F. INTERPRETACION: La Protección de los Edificios son medidas que se utilizan para prevenir la pérdida de Información en el caso de que ocurran Siniestros Inesperados.

4.10 RIESGOS INFORMATICOS.

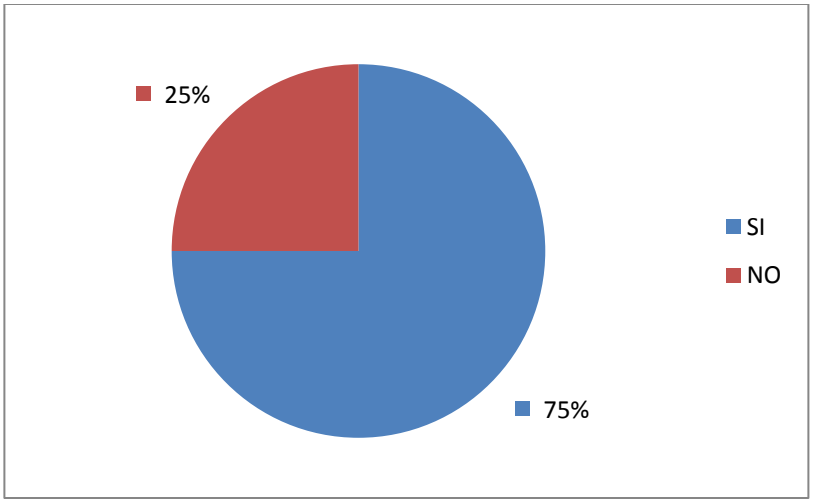
A. **PREGUNTA Nº 10:** ¿Tiene conocimientos sobre los Riesgos Informáticos?

B. **OBJETIVO:** Saber si el personal de las Empresas Distribuidoras de Telefonía Móvil tiene conocimiento sobre Riesgos Informáticos.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	9	75%
NO	3	25%
TOTALES.	**12**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** El 75% de los encuestados tiene conocimiento de Riesgos Informáticos, mientras que un 25% desconoce de tales Riesgos.

F. **INTERPRETACION:** Un Riesgo Informático, es un peligro o inseguridad estimada que puede afectar en la consecución de la Información de una Empresa y puede darse por medio de un Accidente Material o Inmaterial.

4.11 PERDIDAS DE INFORMACION.

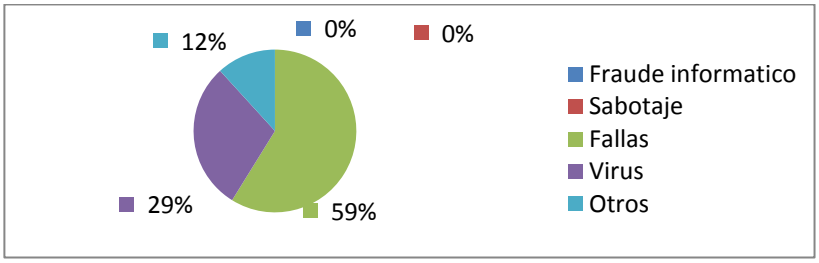
A. **PREGUNTA Nº 11:** ¿Han sufrido Pérdidas de Información ocasionadas por los siguientes factores: Fraude Informático, Sabotaje, Fallas, Virus, Otros?

B. **OBJETIVO:** Determinar qué tipo de Pérdidas de Información han tenido las Empresas Distribuidoras de Telefonía Móvil.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
FRAUDE INFORMATICO	0	0%
SABOTAJE	0	0%
FALLAS	10	59%
VIRUS	5	29%
OTROS	2	12%
TOTALES.	**17**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** El 59% que es por Perdidas de Información por Fallas en el Sistema, el 29% indica que se ha tenido Pérdidas a causa de Virus, el 12% vincula las Perdidas a otros factores no identificados, mientras que nadie se inclina por las Pérdidas de Información a causa de Fraudes Informáticos y Sabotajes.

F. **INTERPRETACION:** Las Pérdidas de Información son accidentes irreparables que se ocasionan por factores Internos y Externos, entre los cuales están: Fraude Informático, Sabotaje, Fallas, Virus, entre otros.

4.12 COMUNICACIÓN.

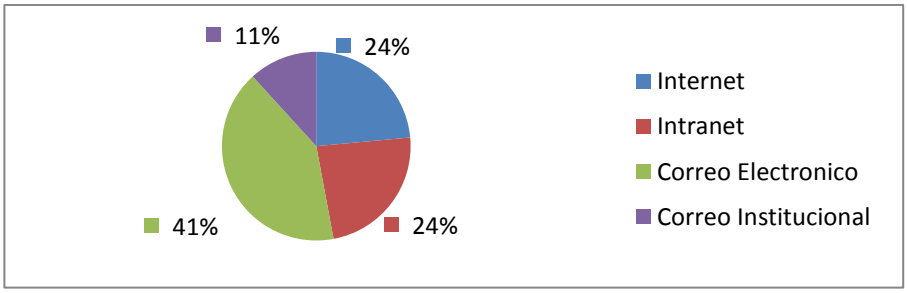
A. **PREGUNTA Nº 12:** ¿Qué tipo de Comunicación utilizan en la Empresa?

B. **OBJETIVO:** Determinar qué tipo de Medios de Comunicación utilizan las Empresas Distribuidoras de Telefónica Móviles.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
INTERNET	4	24%
INTRANET	4	24%
CORREO ELECTRONICO	7	41%
CORREO INSTITUCIONAL	2	11%
TOTALES.	**17**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** El 41% de los encuestados dicen que para Comunicarse internamente utilizan el Correo Electrónico, el 24% de los encuestados dicen que utilizan el Internet, otro 24% respondieron que utilizan el Intranet y solo el 12% de los encuestados dicen que para Comunicarse utilizan el Correo Institucional.

F. **INTERPRETACION:** La comunicación en una Empresa es muy fundamental para el desarrollo de las actividades. Los Medios de Comunicación que se utilizan con más frecuencia son: El Internet, Intranet, Correo Electrónico y el Correo Institucional.

4.13 LICENCIAS DE PROGRAMAS.

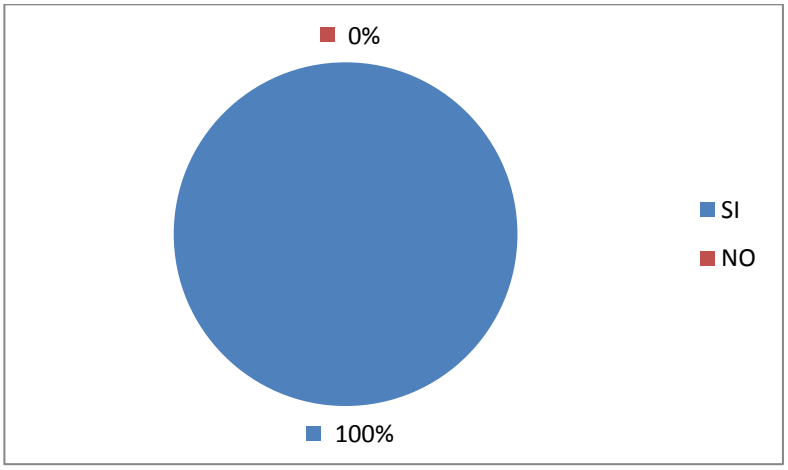
A. PREGUNTA Nº 13: ¿Las Licencias de los Programas están Legalizadas?

B. OBJETIVO: Saber si las Empresas Distribuidoras de Teléfonos Móviles tienen en regla o Legalizados los Programas utilizados para generar Información.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	12	100%
NO	0	0%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 100% de los encuestados revelan que las Licencias de los Programas están debidamente Legalizadas.

F. INTERPRETACION: Para que la generación de Información sea confiable se deben utilizar Programas con Licencias Legalizadas, ya que brindan al usuario mayor confianza para la toma de decisiones y cumplimiento a la Leyes de Propiedad Intelectual y otras afines.

4.14 CLAVES DE ACCESO.

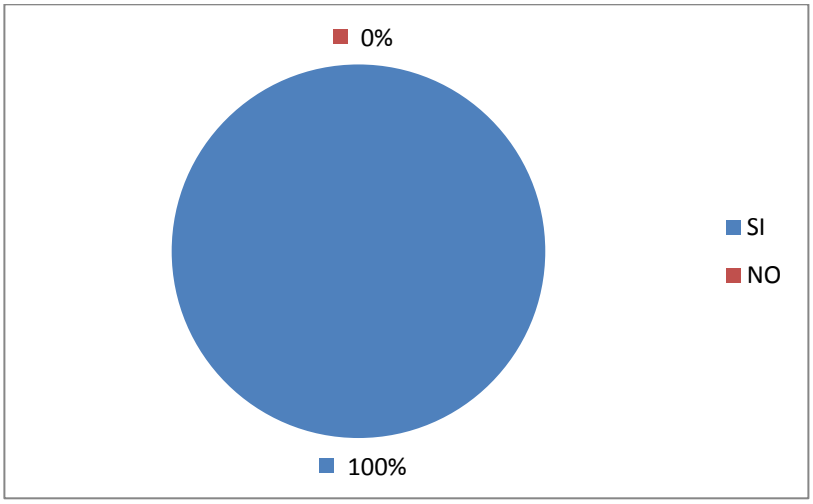
A. PREGUNTA Nº 14: ¿Las Claves de Acceso al Sistema tienen Periodicidad Limitada?

B. OBJETIVO: Saber si las Claves de Acceso al Sistema tienen Periodicidad Limitada.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	12	100%
NO	0	0%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 100% de los encuestados establecen que todas las Claves de Acceso tienen Periodicidad Limitada.

F. INTERPRETACION: Las Claves de Acceso son Pasword que se establecen para mantener con Seguridad la Información principal, y algunas tienen periodicidad limitada, es decir, su cambio es frecuente.

4.15 CAIDAS DE RED.

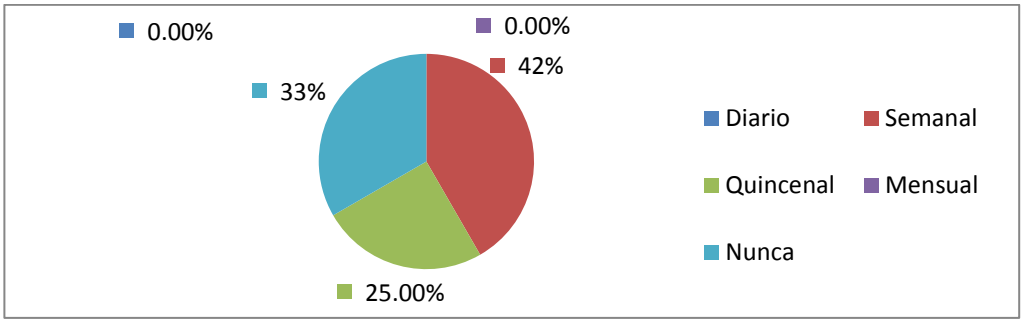
A. **PREGUNTA Nº 15:** ¿Con que Periodicidad se le Cae la Red al Sistema?

B. **OBJETIVO:** Saber la frecuencia en que se Cae el Sistema en las Empresas Distribuidoras de Telefonía Móvil.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
A DIARIO	0	0%
SEMANAL	5	42%
QUINCENAL	3	25%
MENSUAL	0	0%
NUNCA	4	33%
TOTALES.	**12**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** La Periodicidad con que se Cae la Red en el Sistema de las Empresas encuestadas, el 42% dijo que es semanal, el 33% manifestó que nunca se Cae la Red en el Sistema de su Empresa, y el 25% dijo que la Red del Sistema se cae quincenalmente, mientras tanto que nadie adujo que la Red se caiga diariamente o mensualmente.

F. **INTERPRETACION:** Las Caídas de Red son señales de Red Ineficiente e Ineficaz que paralizan la transición de la Información de un lugar a otro, por lo tanto mala imagen para les empresas y usuarios descontentos.

4.16 RESPALDO DE INFORMACION.

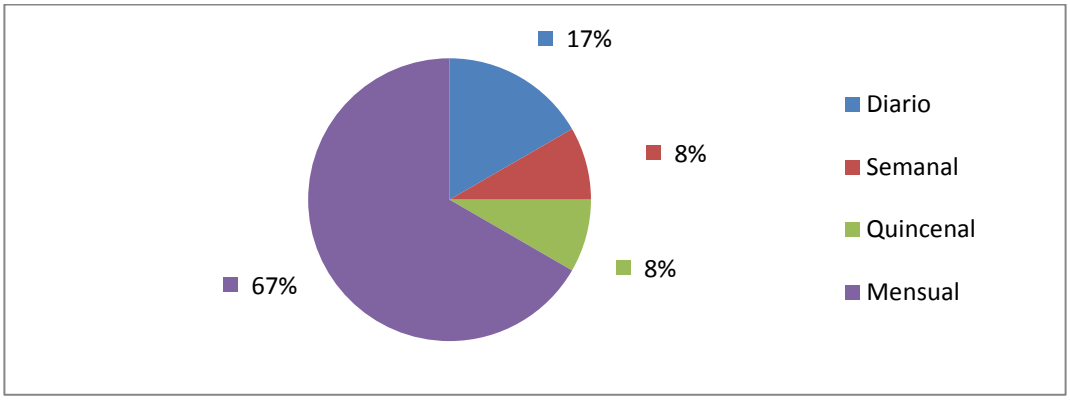
A. **PREGUNTA Nº 16:** ¿Cuánto tiempo se realizan los Respaldos de la Información o Back-Ups?

B. **OBJETIVO:** Saber la Periodicidad de tiempo con que se realizan copias de Respaldo de la Información en las Empresas Distribuidoras de Teléfonos Móviles.

C. **PRESENTACION DE RESULTADOS:**

Opciones.	**Frecuencia.**	**Porcentaje.**
A DIARIO	2	17%
SEMANAL	1	8%
QUINCENAL	1	8%
MENSUAL	8	67%
TOTALES.	**12**	**100%**

D. **PRESENTACION GRAFICA:**



E. **ANALISIS:** El 67% de los encuestados establece que realiza Respaldo de Información cada Mes, el 17% dice que lo realiza a Diario, el 8% dice que respalda Quincenalmente y el 8% Respalda su Información Semanalmente.

F. **INTERPRETACION:** Los Copias de Respaldo de la Información son de gran importancia para las empresas, ya que al suceder cualquier perdida de información se restablecen los datos con esas copias.

4.17 PLAN DE CONTINGENCIA.

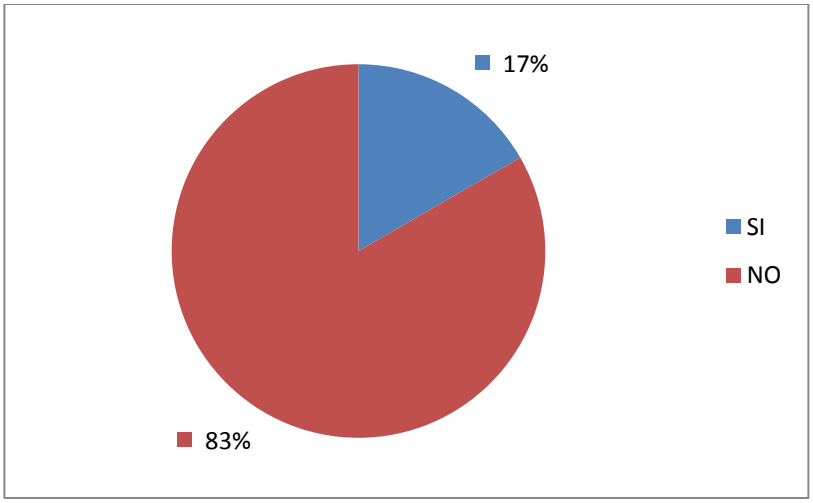
A. PREGUNTA Nº 17: ¿Cuenta con un Plan de Contingencia?

B. OBJETIVO: Saber si las Empresas Distribuidoras de Telefónica Móvil cuentan con un Plan de Contingencia.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	2	17%
NO	10	83%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 83% manifestó que no cuentan con un Plan de Contingencia, mientras que el 17% restante manifestó si tener un Manual de Contingencia.

F. INTERPRETACION: El Plan de Contingencia como Instrumento de Salvaguarda de la Información y de la Integridad del personal, debe existir de manera Documental en cualquier Entidad, y es clave para seguir operando en que el caso que ocurra un siniestro.

4.18 AUDITORIA DE SISTEMAS.

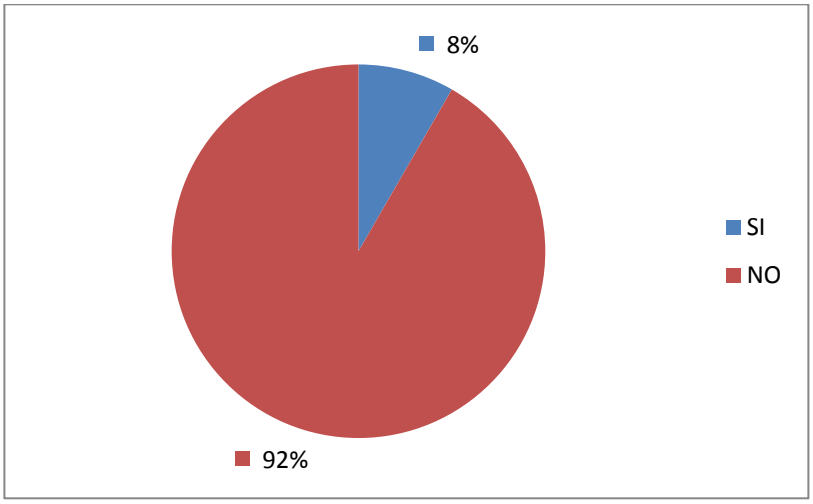
A. PREGUNTA Nº 18: ¿Se le ha practicado en algún tiempo una Auditoria de Sistemas a la Empresa donde labora?

B. OBJETIVO: Determinar si alguna vez se ha efectuado Auditorias de Sistemas en las Empresas Distribuidoras de Teléfonos Móviles.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	1	8%
NO	11	92%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 92% manifestó que no se ha efectuado Auditoria de Sistemas en la Empresa donde labora, el 8% afirmo que si se ha llevado a cabo Auditoria de Sistemas.

F. INTERPRETACION: La Auditoria de Sistemas es la revisión, evaluación y estudio de los sistemas informáticos, con el objeto de dar sugerencias por personas independientes y competentes, sobre el funcionamiento de los sistemas de información.

4.19 PROCESO DE AUDITORIA DE SISTEMAS.

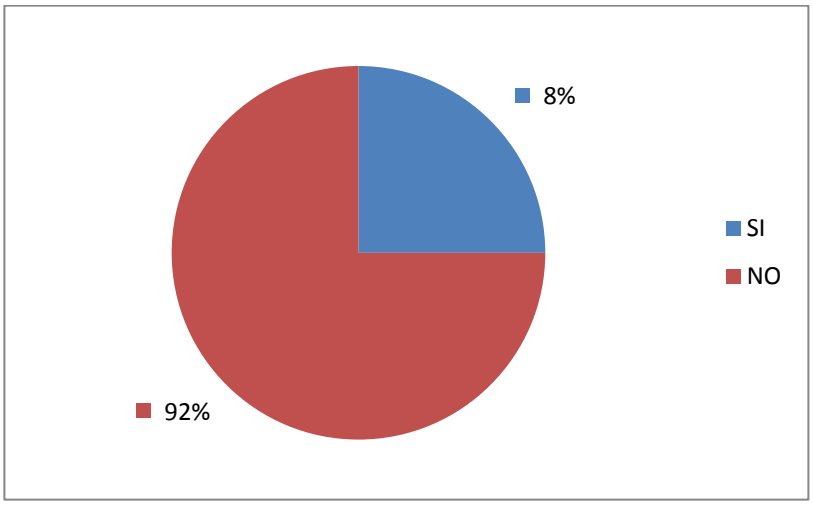
A. PREGUNTA Nº 19: ¿Si la respuesta a la pregunta 18 es afirmativa, conoce el Proceso de Auditoría de Sistemas para la Evaluación de la Seguridad Informática?

B. OBJETIVO: Saber si se conocen los procedimientos que se utilizan para evaluar seguridad informática en una auditoria de sistemas.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	1	8%
NO	11	92%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 92% de los encuestados indicó que no conoce el Proceso de Auditoría de Sistemas y el 8% dijo que si conoce dicho proceso de Auditoria.

F. INTERPRETACION: El proceso de la Auditoria de Sistemas es el de Planificar, Ejecutar y Emitir un Informe. En la Fase de Ejecución se utilizan Técnicas Especializad para obtener Evidencia.

4.20 GUIA PARA EVALUAR SEGURIDAD FISICA Y SEGURIDAD LOGICA.

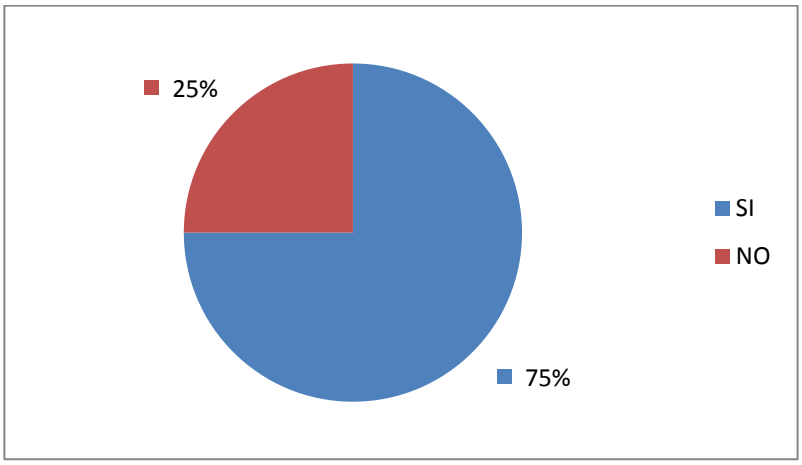
A. PREGUNTA Nº 20: ¿Le gustaría contar con una Guía para Evaluar Seguridad Física y Seguridad Lógica?

B. OBJETIVO: Saber si en las Empresas sienten la necesidad de contar con una Guía que les ayude a Evaluar Seguridad Física y Seguridad Lógica.

C. PRESENTACION DE RESULTADOS:

Opciones.	**Frecuencia.**	**Porcentaje.**
SI	9	75%
NO	3	25%
TOTALES.	**12**	**100%**

D. PRESENTACION GRAFICA:



E. ANALISIS: El 75% de las personas encuestadas manifiesta que si le gustaría que en la Empresa donde labora exista una Guía Práctica para Evaluar Seguridad Informática, mientras que el 25% indicó que no le gustaría.

F. INTERPRETACION: Contar con una Guía Práctica para Evaluar Seguridad Informática es de gran ventaja para una Empresa, ya que podrían evitarse fugas o perdidas de Información de suma importancia. También le serviría de Guía a los Auditores para realizar su trabajo.

CAPITULO V. PROPUESTA DE LA GUIA DE EVALUACION DE SEGURIDAD INFORMATICA EN LAS EMPRESAS DISTRIBUIDORAS DE TELEFONIA CELULAR DE LA CIUDAD DE SAN MIGUEL.

5. GUIA DE EVALUACION DE SEGURIDAD INFORMATICA EN LAS EMPRESAS DISTRIBUIDORAS DE TELEFONIA CELULAR DE LA CIUDAD DE SAN MIGUEL

5.1 DESCRIPCION DE LA GUIA

Esta guía describe la Metodología a utilizar parar realizar la Evaluación de la Seguridad Informática por Auditores Internos o Externos a las Empresas Distribuidoras de Telefonía Celular de la ciudad de San Miguel. En ella se desarrollan ejemplos de los principales procesos y formatos a utilizar para realizar la evaluación de la Seguridad Física y Seguridad Lógica.

Se presenta un Caso Hipotético, donde una Firma de Auditores: "Grupo Profesional de Auditores S. A. de C. V.", es contratada por la Empresa: "Teléfonos Fáciles S.A. de C.V.", para que en el año 2012 le realicen la Auditoría de Sistemas, específicamente a la Seguridad Informática.

5.2 OBJETIVOS

5.2.1 Objetivo General:

- Desarrollar la Metodología para la Evaluación de Seguridad Informática.

5.2.2 Objetivos Específicos:

- Identificar y Aplicar en cada proceso de la Evaluación de la Seguridad Física y Lógica, los procedimientos a utilizar por el Auditor para obtener evidencia

- Diseñar y Completar Papeles de Trabajo (principales formatos) para evaluar la Seguridad Física como Seguridad Lógica.

5.3 ETAPAS DE APLICACIÓN DE LA AUDITORIA DE SEGURIDAD INFORMATICA

5.3.1 ETAPA PRE-INICIAL

5.3.1.1 TERMINOS Y COMPROMISOS DEL TRABAJO DE LA AUDITORIA DE SEGURIDAD INFORMATICA:

a) **CARTA OFERTA DE SERVICIOS**

b) **CONTRATO DE SERVICIOS DE AUDITORIA DE SEGURIDAD INFORMATICA**

c) **CARTA COMPROMISO**

a) CARTA OFERTA DE SERVICIOS

Para poder llevar a cabo la ejecución de la auditoria de seguridad informática en la empresa: "Teléfonos Fáciles S.A. de C.V durante el periodo comprendido desde Julio hasta Septiembre del año 2012, La firma de auditoria "Grupo Profesional de Auditores S.A. de C.V." debe presentar una carta oferta de servicios en la que se palpen los aspectos básicos referentes al trabajo que habrá de realizarse.

Para efectos de tomar un modelo a seguir se presenta un modelo de Carta Oferta de Servicios. **(Anexo # 1)**.

b) CONTRATO DE SERVICIOS DE AUDITORIA DE SEGURIDAD INFORMATICA

Una vez que la gerencia de la empresa ha analizado la Carta Oferta de Servicios que presentó la Firma de Auditoria y aceptando las condiciones mencionadas en esta, se procede a solicitar y a firmar un contrato de servicios de Auditoria de Seguridad Informática. El respectivo contrato contiene las cláusulas que servirán de lineamientos al momento de la realización del trabajo de auditoria, el cual se presenta en el **(Anexo # 2)**

c) CARTA COMPROMISO

Para tener un mayor respaldo del compromiso que asume la firma de auditoria, es menester que exista un documento escrito que ampare el servicio de auditoria que recibirá la empresa: "Teléfonos Fáciles S.A. de C.V."

Según La NIA 210 "Términos de Los Trabajos de Auditoria": La Carta Compromiso de un Auditor a su Cliente documenta y confirma su aceptación del nombramiento, el objetivo y alcance de la auditoría, el grado de sus responsabilidades para con el cliente y la forma de cualesquier informes.

Para tener una noción más clara un modelo de Carta Compromiso se presenta en el **(Anexo # 3),**

5.3.2 ETAPA DE PLANEACION :

a) ANTECEDENTES DE LA EMPRESA, DEL CENTRO DE COMPUTO O UNIDAD DE INFORMATICA Y DE LA SEGURIDAD FISICA Y LOGICA

b) EVALUACION DEL CONTROL INTERNO

c) **DETERMINACION DE LAS AREAS CRÍTICAS**

d) **EVALUACION DEL RIESGO INFORMATICO**

e) **PROGRAMAS DE AUDITORIA**

f) **PERSONAL ASIGNADO**

g) **FECHAS PARA LA AUDITORIA**

a) ANTECEDENTES DE LA EMPRESA, DEL CENTRO DE COMPUTO O UNIDAD DE INFORMATICA Y DE LA SEGURIDAD FISICA Y LOGICA

El Auditor de Sistemas obtiene esta información mediante algunas técnicas de auditoría como:

- Observación
- Indagación

Además se solicita información de tipo administrativa, para conocer la estructura del Centro de Cómputo de la empresa auditada mediante documentos que contengan:

- Organigrama
- Visión
- Misión
- Políticas de Seguridad Informática

Y la información esencial se obtiene a través de: **Entrevistas (Anexo # 4) y se** complementa con el **Organigrama del Centro de Cómputo (Anexo # 5)**

b) EVALUACION DEL CONTROL INTERNO

El auditor realiza la evaluación del Control Interno para evaluar Seguridad Informática a través de:

b.1) Cuestionario de Evaluación de Seguridad Física (Anexo # 6)

b.2) Cuestionario de Evaluación de Seguridad Lógica (Anexo # 7)

La información resultante de los cuestionarios se plasma en **una Matriz de Control Interno**, que permite a la administración evaluar las desviaciones y/o fallas en la administración de la Seguridad Informática.

c) DETERMINACION DE LAS AREAS CRÍTICAS

El Auditor de Sistemas realiza la determinación de las áreas críticas a través de instrumentos como:

c.1) Lista de Verificación (Anexo # 8)

c.2) Lista de Chequeo para el caso de la Seguridad Física en instalaciones de Cómputo (Anexo # 9)

d) EVALUACION DEL RIESGO INFORMATICO

La evaluación del riesgo informático se hace a través de una **Matriz de Riesgo,** para dar cumplimiento a la normativa técnica NIA 315. Esta matriz para evaluar **Seguridad Informática** contiene una colección de diferentes Amenazas (campos verdes) y Elementos de información (campos rojos). Para llenar la Matriz, se tiene que estimar los valores de la Probabilidad de Amenaza (campos azules) por cada Amenaza y la Magnitud de Daño (campos amarillas) por cada Elemento de Información.

Para la estimación de la Probabilidad de amenazas, se trabaja con un valor generalizado, que (solamente) está relacionado con el recurso más vulnerable de los elementos de información, sin embargo usado para todos los elementos.

En el caso de que se determine los valores para la Probabilidad de Amenaza y Magnitud de Daño a través de un proceso participativo de trabajo en grupo (grande), se recomienda primero llenar las fichas de apoyo para los elementos de Información y Probabilidad de Amenaza, y una vez consolidado los datos, llenar la matriz.

Dependiendo de los valores de la Probabilidad de Amenaza y la Magnitud de Daño, la Matriz calcula el producto de ambos variables y visualiza el grado de riesgo. **(Anexo # 10)**

e) PROGRAMAS DE AUDITORIA

El Auditor de Sistemas, realiza la planeación de los procedimientos que utiliza para hacer la evaluación dela Seguridad Informática, por ello es necesario que se plasmen en Programas para cada área a evaluar, dichos programas para Seguridad Informática son:

e.1) Programa de Seguridad Física (Anexo # 11)

e.2) Programa de Seguridad Lógica (Anexo # 12)

f) PERSONAL ASIGNADO

Para la Evaluación de la Seguridad Informática, es necesario contar con personal capacitado para llevar a cabo dicha evaluación, por ello se contará con la participación del cuerpo de Auditores descritos en **(Anexo # 13)**

Además para dar cumplimiento a la Normativa Técnica, NIA 620, es necesario contratar los servicios de un experto; es decir, un Ingeniero en Sistemas, ya que se trata de una Auditoría Especializada que requiere de los conocimientos técnicos de dicho profesional.

El personal idóneo para llevar a cabo la Auditoría de Sistemas debe de cumplir un perfil técnico que le facilite ejecutar dicha Auditoría. **(Anexo # 13)**

d) FECHAS PARA REALIZAR LA AUDITORIA

El Auditor de Sistemas debe hacer una programación de las fechas claves en que realizará los procedimientos de Auditoría, a través de un **Cronograma de Actividades (Anexo # 14).**

EL DOCUMENTO FINAL EN ESTA ETAPA ES EL MEMORÁNDUM DE PLANEACIÓN, PARA DAR CUMPLIMIENTO A LO ESTIPULADO EN LA NORMATIVA TÉCNICA, NIA 300. (ANEXO # 15)

5.3.3 ETAPA DE EJECUCION

5.3.3.1 INSTRUMENTOS Y HERRAMIENTAS PARA LA OBTENCION DE EVIDENCIA EN LA AUDITORIA DE SEGURIDAD INFORMATICA

a) **PROCEDIMIENTOS DE AUDITORIA**
b) **PAPELES DE TRABAJO**
c) **INDICES DE REFERENCIA**
d) **MARCAS DE AUITORIA**
e) **ARCHIVOS DE AUDITORIA**

a) PROCEDIMIENTOS DE AUDITORIA

a.1) PROCEDIMIENTOS DE LA AUDITORIA TRADICIONAL.

El Auditor de Sistemas, se debe de valer de procedimientos tradicionales de auditoría para realizar la Evaluación de la Seguridad Informática, dichas técnicas tradicionales son:

- Observación
- Inspección
- Revisión

(Anexo # 16)

a.2) PROCEDIMIENTOS TECNICOS (TECNICAS DE AUDITORIA CON AYUDA DE LA COMPUTADORA, TAAC)

El Auditor de Sistemas se tiene que auxiliar de TAAC, las cuales pueden ser utilizadas para hacer la auditoría más efectiva y eficiente al:

• Automatizar una prueba de auditoría existente que es realizada manualmente, tal como las pruebas de la precisión matemática de un reporte.

• Realizar pruebas que no es factible realizar manualmente, ej. La revisión de las transacciones de venta para partidas grandes e inusuales aunque sería posible realizar esto manualmente, para la mayoría de las compañías grandes, el número de transacciones que necesitarían revisar sería prohibitivo desde el punto de vista del tiempo.

El uso de técnicas de auditoría asistidas por computadora ("TAACs") puede ser una forma efectiva de evaluar controles automatizados. TAACs incluye, por ejemplo, el desarrollo de una prueba integrada y el procesamiento de transacciones de pruebas en el sistema. La ventaja de utilizar TAACs en pruebas de controles es que es posible revisar cada transacción (bien sea en un archivo maestro o en un archivo de transacciones), para determinar si existen fallas en los controles.

Software de Auditoria

Consiste en programas de computadora usados por el auditor como parte de sus procedimientos de auditoria para procesar datos de importancia de auditoria del sistema de la entidad.

Pueden consistir en Programas de Paquete, Programas Escritos para un Propósito, Programas de Utilería.

Independientemente de la fuente de los programas, ya que lo puede hacer él, si tiene los conocimientos necesarios o comprarlos, pero el auditor deberá verificar su validez para fines de auditoria antes de su uso.

b) PAPELES DE TRABAJO

En esta fase, el Auditor de Sistemas, obtiene la Evidencia mediante de Cédulas o Papeles de Trabajo que le permitan documentar y evidenciar los procedimientos practicados durante la Evaluación de la Seguridad Física y de la Seguridad Lógica.

Algunos de los Papeles de Trabajo que elabora el Auditor de Sistemas según el área son:

Seguridad Física

b.1) Cédula de Inventario de Equipo de Cómputo del área de Informática. **(Anexo #17)**

b.2) Cédula Narrativa de Condiciones de Mobiliario. **(Anexo # 18)**

b.3) Cédula Narrativa de espacio físico de área de local de venta. **(Anexo # 19)**

b.4) Cédula Narrativa de Rutas de Evacuación. **(Anexo # 20)**

b.5) Cédula Narrativa de Alarmas. **(Anexo # 21)**

b.6) Cédula de Suministros de Energía. **(Anexo # 22)**

b.7) Cédula Analítica de Extintores. **(Anexo # 23)**

b.8) Cédula Narrativa de Aire Acondicionado. **(Anexo # 24)**

Seguridad Lógica:

b.9) Cédula Analítica de Inventario de Programas. **(Anexo # 25)**

b.10) Cédula Analítica de Módulos del Sistema. **(Anexo # 26)**

b.11) Cédula Analítica de Aplicaciones de los Módulos. **(Anexo # 27)**

b.12) Sub-Cédula Analítica de Módulos. **(Anexo# 28)**

b.13) Cédula Narrativa de Administración de Seguridad. **(Anexo# 29)**

b.14) Cédula Narrativa de Password. **(Anexo# 30)**

b.15) Cédula Analítica de Inventario de Routers. **(Anexo# 31)**

b.16) Cédula Narrativa de Funcionamiento de Firewall. **(Anexo# 32)**

b.17) Cédula Analítica de Inventario de Antivirus. **(Anexo# 33)**

b.18) Cédula Narrativa de formularios o manuales de funcionamiento del sistema. **(Anexo# 34)**

c) INDICE DE REFERENCIA.

En esta parte se hace la descripción detallada y se pagina el contenido total de los papeles de trabajo, con el propósito de identificar rápidamente la página en donde se encuentra cada una de las partes que integran este legajo de papeles. La única condición que deben de cumplir los índices de referencia es que sea una presentación ordenada y que se identifiquen claramente las páginas y su contenido. Para este caso, el despacho ha decidido referenciar con los siguientes métodos:

- **Alfabético, para los programas (Anexo# 35)**
- **Alfa-Numéricos, para Papeles de Trabajo. (Anexo# 36)**

d) MARCAS DE AUDITORIA

Para dejar comprobación de los hechos, técnicas y procedimientos utilizados en las cédulas, el despacho utilizó una serie de marcas de auditoría para evaluar tanto la Seguridad Física como la Seguridad Lógica de la empresa de telefonía móvil "Teléfonos Fáciles S.A de C.V", las cuales permiten ahorro de espacio y tiempo, las cuales son símbolos especiales creados por el Auditor con una significación especial. **(Anexo# 37)**

e) ARCHIVOS DE PAPELES DE TRABAJO.

Los archivos o legajos de papeles de trabajo se clasifican de acuerdo al uso que se le dé a la información, basado en la vigencia e importancia de su contenido. Por lo tanto para la Evaluación de la Seguridad Informática en la empresa "Teléfonos Fáciles S.A de C.V se desarrollaron tres archivos de papeles de trabajo, que son los siguientes:

e.1) Archivo Administrativo A / A (Anexo # 38)

e.2) Archivo Permanente A / P (Anexo # 39)

e.3) Archivo Corriente P / T (Anexo # 40)

5.3.4 ETAPA DEL INFORME

5.3.4.1 ESTRUCTURA DEL INFORME DE LA AUDITORIA DE SEGURIDAD INFORMATICA

El Auditor como etapa final elabora el Informe de Auditoría, en el cual se detallan los hallazgos encontrados en el proceso de auditoría, para dar a conocer a la dirección de la empresa solicitante las desviaciones encontradas en la empresa y

posteriormente puedan ser corregidas, para un mejor funcionamiento, para este caso los hallazgos resultantes de la Evaluación de la Seguridad Física y Seguridad Lógica a la empresa "Teléfonos Fáciles S.A de C.V". **(Anexo # 41)**

5.3.4.2 ESTRUCTURA DEL INFORME DE CONTROL INTERNO DE LA AUDITORIA DE SEGURIDAD INFORMATICA (CARTA A LA GERENCIA)

En esta fase el Auditor, realiza un informe de deficiencias menores que no son considerados como hallazgos encontrados durante el proceso de Evaluación de la Seguridad Informática, con el objetivo que puedan ser desvanecidas para evitar que puedan perjudicar de alguna forma a la empresa, dicho informe se conoce como Carta a la Gerencia. **(Anexo #42)**

CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES

6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel, no cuentan con un Manual por escrito de Seguridad Informática.

- Las Empresas Distribuidoras de Telefonía Móvil conocen las medidas de Seguridad Física y Lógica, pero no se lleva a cabo la evaluación de dicha Seguridad.

- No todos los responsables de informática de las Empresas Distribuidoras de Telefonía Móvil, conocen los diferentes Riesgos Informáticos existentes.

- Las pérdidas de información que han sufrido las Empresas ha sido por causa de fallas en los Sistemas que utilizan y la mayor causa es por los virus informáticos en dichos sistemas.

- La mayoría de las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel no tienen un Plan de Contingencia que les permita operar en caso de siniestros.

- No se practica Auditoría de Sistemas en la mayoría de las Empresas en estudio, debido que no conocen sobre el Proceso de Auditoría de Sistemas, para llevar a cabo la Evaluación de la Seguridad Informática en las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel.

6.2 RECOMENDACIONES

- Las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel deben tener un Manual de Seguridad Informática, que haga referencia a medidas de Seguridad Informática, ya que con ello se pueden prevenir riesgos de pérdida de la información en el desarrollo de las actividades operativas, administrativas y contables.

- Los Auditores Internos de dichas Empresas, deben de evaluar periódicamente la Seguridad Física y la Seguridad Lógica para evitar posibles Riesgos Informáticos ocasionados por los Sistemas de Información Computarizados y su entorno.

- Capacitar a los responsables de los sistemas informáticos en las Empresas sobre los diferentes tipos de Riesgos Informáticos existentes en los sistemas.

- Las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel, deben de tener un plan adecuado para que en caso de fallas, dar soporte técnico y minimizar el tiempo de inactividad de los sistemas; y utilizar los con antivirus o filtros que detecten los diferentes virus que puedan poner en riesgo los sistemas y su información.

- Diseñar un Plan de Contingencias, que les permita operar de manera normal, en caso de algún tipo de siniestros.

- Dar a conocer el Proceso de Auditoría de Sistemas a los responsables de las empresas en estudio, para que contraten los servicios de éste tipo de Auditoría Especializada, especialmente enfocándose en la Evaluación de la Seguridad Informática.

BIBLIOGRAFIA

- AGUIRRE, JORGE. "Seguridad Informática y Criptografía". Ed. Universidad Politécnica de Madrid. Versión 4.1. 2006.
- COBIT 4.1, ISACA, United States of America 2005.
- Código de Comercio de El Salvador.
- Código de Ética Profesional del ISACA, www.isaca.com
- Código Penal de El Salvador.
- Declaraciones Internacionales de Prácticas de Auditoría. DIPA´S
- EL DIRIGENTE Y LA SEGURIDAD INFORMÁTICA. Curso de Adiestramiento de la Empresa Cubana de Consultoría y Seguridad "Segurmatica", octubre, 2002.
- DE LA CARIDAD PÉREZ TULA, M. Material de estudio para el tema "Seguridad Informática" de la asignatura "Arquitectura y Seguridad Informática", 2003.
- Ley de Propiedad Intelectual.
- Ley de Telecomunicaciones.
- Ley Especial Contra Actos de Terrorismo.
- Ley Reguladora del Ejercicio de la Contaduría Pública y Auditoría
- NARANJO, ALICE. "Auditoria de Sistemas". http://www.monografias.com
- Normas Internacionales de Auditoría. Versión 2009
- Normas Internacionales de Auditoría. Versión 2011
- Normas Internacionales del ISACA, www.isaca.com
- PIATTINI, M. y otros, "Auditoria Informática. Un Enfoque Práctico. 2ª Edición" Ed. RA-MA Editorial, 2001 .
- RABELO PADUA, SONIA. "RED_ISPETP: Red informática educativa del Instituto Superior Pedagógico para la Educación Técnica y Profesional". Tesis

en opción al título de master en Ciencias de la Computación UH La Habana, 2007.

- ROJAS SORIANO, RAÚL. Guía para realizar Investigaciones Sociales. P y V Editores, México, 30ª Edición 1998.
- Ruiz Olabuenaga, José I. Métodos de Investigación Cualitativa, 1989
- www.iscp.org
- www.isaca.com
- www.siget.gob.sv
- www.wikipedia.com

ANEXOS

INDICE DE ANEXOS

Contenido

ANEXO # 1

Grupo Profesional de Auditores, S. A. de C. V.

MODELO DE CARTA OFERTA DE SERVICIOS

01 de Julio de 2012

"TELEFONOS FACILES S.A. DE C.V."
PRESIDENCIA DE JUNTA DIRECTIVA
PRESENTE

De acuerdo con charlas que hemos tenido el agrado de celebrar con ustedes en días pasados, nos permitimos a su consideración nuestra propuesta de honorarios por los servicios de auditoria de seguridad informática para su empresa en el periodo comprendido desde Julio hasta Septiembre del año 2012. Dicha auditoria será llevada a cabo según Normas Internacionales de Auditoria y las Normas Internacionales de Auditoria de Sistemas de Información y además auxiliándonos para aspectos meramente técnicos de profesionales en materia de ciencias informáticas.

Nuestra firma cuenta con personal idóneo y especializado en Auditoría de Sistemas que le permitirá desarrollar un trabajo más completo en cuanto a la evaluación de la seguridad informática de su empresa.

Como resultado de dicho examen, entregaríamos a ustedes, nuestro dictamen sobre auditoria de seguridad informática para los efectos de los señores accionistas y administradores y un informe conteniendo detalles de hallazgos y recomendaciones para mejorar los procedimientos y sistemas de control interno de aquellas áreas que a nuestro juicio, lo ameriten.

La entrega de dicho informe será efectuada en fechas acordadas conjuntamente entre nosotros, básicamente a causa de la planeación del cierre anual de operaciones que,

como ustedes saben, depende de ciertas circunstancias de control que con frecuencias son imprevisibles.

El monto de los honorarios lo hemos estimado tomando en consideración de las horas que nuestro personal técnico debe intervenir para llevar a cabo los trabajos inherentes a la dictaminación, a la luz de la característica organizacional y de flujo de "Teléfonos Fáciles S.A. de C.V.", dicho monto asciende a la cantidad de $XXXXX que serian pagados de acuerdo con bases establecidas también de manera conjunta por ambas partes.

Es importante señalar que durante el desarrollo de nuestra auditoria llegaran a surgir situaciones extraordinarias que motivaran inversiones adicionales de tiempo por parte de nuestro personal, pondríamos a consideración el incremento estimado de honorarios, a fin de contar con su aprobación, antes de llevar a cabo la revisión correspondiente.

Al reiterar nuestro agradecimiento por su atención y por la oportunidad que nos ha brindado de poder presentarles esta propuesta, nos es grato expresarle nuestros mejores deseos.

Atentamente.

Licda. Teresa Barahona

Representante Legal

"GRUPO PROFESIONAL DE AUDITORES S.A. DE C.V."

ANEXO # 2

MODELO DE CONTRATO DE SERVICIOS DE AUDITORIA DE SEGURIDAD INFORMATICA

Contrato de presentación de servicios profesionales en seguridad informática que celebran por una parte "TELEFONOS FACILES S.A. DE C.V."__ representado por " ING. JORGE FLORES PRESIDENTE DE LA JUNTA DIRECTIVA." en su carácter de "REPRESENTANTE LEGAL" y que en lo sucesivo se denomina al Cliente, por otra parte "GRUPO PROFESIONAL DE AUDITORES S.A. DE C.V. representada por la LIC. TERESA BARAHONA a quien se denominara el Auditor, de conformidad con las declaraciones y cláusulas siguientes:

Declaraciones

1.-El cliente declara:

a) Que es una SOCIEDAD ANONIMA DE CAPITAL VARIABLE

b) Que esta representado para este acto por "ING. JORGE FLORES PRESIDENTE DE LA JUNTA DIRECTIVA" y tiene como su domicilio EN LA CIUDAD DE SAN MIGUEL.

c) Que requiere obtener servicios de auditoria en seguridad informática, por lo que ha decidido contratar los servicios del auditor.

2.-Declara el auditor:

a) Que es una sociedad anónima de capital variable, constituida y existente de acuerdo con las leyes y que dentro de sus objetivos primordiales esta el de prestar auditoria en seguridad informática, que comprende la evaluación del software y hardware en el departamento de computo.

b) Que esta constituida legalmente según escritura numero "1212" de fecha 12 DE FEBRERO DE 2000 ante el notario público nº 3001 del domicilio de la CIUDAD DE SAN MIGUEL. LIC. CARLOS ARTURO BONILLA.

c) Que señala como su domicilio LA CIUDAD DE SAN MIGUEL

3.-Declaran ambas partes:

a) Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato que se contiene en las siguientes:

CLAUSULAS

PRIMERA. OBJETIVO

El auditor se obliga a prestar al cliente los servicios de auditoria de seguridad en informática, de manera que pueda llevar a cabo una evaluación detallada de la seguridad física y seguridad lógica de las operaciones que generan información para la toma de decisiones empresariales y de negocio. Lo anterior de acuerdo a lo establecido en la carta oferta propuesta, que, firmada por las partes, forma parte integrante del contrato.

SEGUNDA. ALCANCE DEL TRABAJO

El alcance de los trabajos que llevara a cabo el auditor dentro de este contrato son:

a) Evaluaciones de la dirección de seguridad informática en lo que corresponde a:

-Su organización (Capacitación de personal)

-Estructura (Planes de trabajo)

-Recursos Humanos (Control Interno administrativo)

-Normas y Políticas (Estándares)

b) Evaluación de los sistemas

-Evaluación de los diferentes sistemas en operación, (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).

-Opinión de los usuarios de los diferentes sistemas

-Evaluación de avance de los sistemas en desarrollo y congruencia con el diseño general

-Evaluación de prioridades y recursos asignados (humanos y equipo de cómputo).

-Seguridad física y lógica de los sistemas, su confidencialidad y respaldos.

c) Evaluación de equipos

-Capacidades (Respaldos de equipo)

-Utilización (Seguros)

-Nuevos proyectos (Contratos)

-Seguridad física y lógica (Proyecciones)

d) Elaboraciones de informes que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos a, b y c de esta cláusula.

TERCERA. PROGRAMA DE TRABAJO

El cliente y el auditor convienen el desarrollar en forma conjunta un programa de trabajo en el que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevar a cabo y las fechas de realización.

CUARTA. SUPERVISION

El cliente o quien designe tendrá derecho a supervisar los trabajos que se le han encomendado al auditor dentro de este contrato, y a dar por escrito las instrucciones que estime convenientes.

QUINTA. COORDINACION DE LOS TRABAJOS.

El cliente designara por parte de la organización a un coordinador del proyecto quien será el responsable de coordinar la recopilación de la información que solicite el auditor y de que las reuniones y entrevistas establecidas en el programa de trabajo se lleven a cabo en las fechas establecidas.

SEXTA. HORARIO DE TRABAJO.

El personal del auditor dedicara el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de la celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes y gozaran la libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que estarán sujetos a horarios y jornadas determinadas.

SEPTIMA. PERSONAL ASIGNADO

El auditor designara para el desarrollo de los trabajos objeto de este contrato a socios del despacho quienes, cuando consideren necesario incorporaran personal técnico capacitado de que dispone la firma, en el número que se requieran de acuerdo a los trabajos a realizar.

OCTAVA. RELACION LABORAL.

El personal del auditor no tendrá ninguna relación con el cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el auditor en ningún momento se considera intermediario del cliente respecto al personal que

ocupe para dar cumplimiento de las obligaciones que se deriven de las relaciones entre el y su personal, y exime al cliente de cualquier responsabilidad que a este respecto existiere.

NOVENA. PLAZO DE TRABAJO.

El plazo es estableció por el auditor y debe ser congruente con el alcance y las limitaciones del trabajo de auditoria de seguridad informática. El plazo que se ha previsto para la terminación de la auditoria de seguridad informático es de seis meses, desde julio hasta septiembre del año 2012.

DECIMA. HONORARIOS.

El establecimiento de los honorarios estará en función del plazo y calidad del trabajo realizado.

Por consecuente en atención a los elementos descritos anteriormente se ha establecido la facturación de lo honorarios por un valor de $XXXX

DECIMA SEGUNDA. JURISDICCION

Todo lo no previsto en este contrato se regirá por las disposiciones relativas contenidas en el código civil de EL SALVADOR_ y, en caso de controversia para su interpretación y cumplimiento, las partes se someten a la jurisdicción de los tribunales federales, renunciando al fuero que les pueda corresponder en razón de su domicilio presente o futuro.

Enteradas las partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad en original y tres copias, en la ciudad de SAN MIGUEL EL DIA 1 DE JULIO DEL AÑO 2012.

F._____ **F._____**

Ing. Jorge Flores
"TELEFONOS FACILES S.A DE C.V."

Licda. Teresa Barahona
Representante Legal
"GRUPO PROFESIONAL DE AUDITORES S.A. DE C.V"

ANEXO # 3

MODELO DE CARTA COMPROMISO

"GRUPO PROFESIONAL DE AUDITORES S.A. DE C.V."

01 DE JULIO DE 2012

SEÑORES
JUNTA DIRECTIVA
"**TELEFONOS FACILES S.A. DE C.V."**
SAN MIGUEL
PRESENTE

Estimados señores:

Esta carta es para confirmar nuestro entendimiento de los términos y objetivos de nuestro trabajo, y la naturaleza y limitación de los servicios que proporcionaremos al desarrollar la evaluación denominada "Auditoría a la Seguridad Física y Lógica" de la empresa: "TELEFONOS FACILES S.A. DE C.V.". Nuestro trabajo será desarrollado de acuerdo con Normas Internacionales de Auditoría y Normas Internacionales de Auditoria de Sistemas de Información aplicables a trabajos con procedimientos convenidos, además de lineamientos técnicos en materia de seguridad informática, lo cual se indicara en nuestro informe.

El objetivo de la auditoría, tal como lo expresan los términos de referencia, es el de evaluar el Área de la Seguridad Informática de su Empresa y además obtener un informe que permita a la Junta Directiva determinar la capacidad instalada del

departamento de sistemas para responder a las exigencias de la apertura hacia mercados financieros internacionales.

Hemos convenido en informarle de los resultados de hechos resultantes al realizar nuestro trabajo bajo los procedimientos convenidos con ustedes y que detallamos a continuación:

1. Revisar manuales técnicos y administrativos
2. Revisar planes del centro de computo, así como su presupuestos
3. Se hará evaluación del riesgo informático
4. Evaluación de Seguridad Física (instalaciones, Accesos, Rutas de Evacuación, etc.)
5. Evaluación de Seguridad Lógica (password, firewall, Antivirus, etc.)
6. Evaluar los Controles Generales y los Controles de Aplicación
7. Evaluar los componentes de la Red
8. Realizaremos Inventarios de hardware, software, consumibles, etc.
9. Evaluaremos Bases de Datos
10. Evaluaremos el Plan de Contingencia en el caso de que exista uno.
11. Evaluaremos Planes de Respaldo y Restauración
12. Se evaluara también condiciones Ambientales, Ergonómicas, etc.

Esperamos toda la cooperación de su personal y confiamos en que pondrán a nuestra disposición los registros, documentación, y cualquier otra información que solicitemos en relación a nuestro trabajo.

Al finalizar nuestro trabajo de Evaluación de la Seguridad Informática, estaremos entregando un informe final de Seguridad Física y Seguridad Lógica con los resultados obtenidos del examen y una Carta a la Gerencia con deficiencias menores encontradas.

Nuestros honorarios serán facturados de acuerdo a lo establecido en los términos de referencia de la consultoría. Los cargos por retribución se basan en el tiempo requerido por el personal designado a este trabajo en particular, mas gastos directos e impuestos. Las tarifas por hora individual varían de acuerdo con el grado de responsabilidad involucrado y la pericia y experiencia requerida.

Mucho les agradecemos firmar y regresar la copia anexa de esta carta, para indicar que concuerda con su entendimiento de los términos de trabajo, incluyendo los procedimientos específicos en los que hemos convenido realizar.

Agradecidos por la oportunidad de servirles en este importante trabajo, quedamos a sus apreciables órdenes.

Atentamente,

Licda. Teresa Barahona

Representante Legal

“GRUPO PROFESIONAL DE AUDITORES S.A. DE C.V.”

ANEXO #4

Grupo Profesional de Auditores, S. A. de C. V.

ENTREVISTA PRELIMINAR

Empresa: Teléfonos Fáciles S.A de C.V **Fecha:** 01 de Julio de 2012

Entrevistado: Ing. Carlos Alberto Huezo **Puesto:** Jefe de Informática

Realizado por: Rocío Elizabeth Bolaines Portillo

Recursos Humanos

1. ¿Quién es el administrador de red?
   Ing. Carlos Alberto Huezo

2. ¿Desde cuándo es el administrador de red?
   Desde el año 2006.

3. ¿Funciones del Administrador de red?
   Configurar nuevas cuentas de usuario, creación de usuarios, definir parámetros de los perfiles de usuario, administrar el funcionamiento de la red, instalar el programa base (EXACTUS) en las terminales, verificar el funcionamiento de las bases activas, generación de contraseñas, inclusión de nuevas terminales en el dominio de red de la institución.

4. ¿Poseen manual de funciones y manual de puestos?
   Sí

5. ¿Hay rotación de este cargo?

No

6. ¿Tiene suplente en caso de emergencia la administradora de red?

Sí, vía remota y también hay personal autorizado por el Gerente General para realizar las tareas básicas que son encender el servidor y realizar los backup y el recurso autorizado es el Licenciado Carlos Sosa.

7. ¿El administrador de red atiende otras sucursales?

Si, administra 17 puntos de ventas y la casa matriz.

8. ¿El Administrador de Red/Personal Informático ha recibido capacitaciones?

Si, en Windows 2003 Server, Windows 2007 y otras sobre procesos informáticos.

9. ¿De quién depende el administrador de cargo?

Depende de la unidad de Auditoría Interna y Gerencia General

Centro de Cómputo

1. ¿Tienen Centro de cómputo?

Sí. Red LAN (red de área local)

2. ¿Cuentan con organigrama del centro de cómputo?

Sí

3. ¿Cuántas computadoras poseen?

55 computadoras.

4. ¿Posee la empresa servidor?

Sí.

5. ¿Cuántos servidores posee la institución?

Dos (2). Uno en Casa matriz y otro en San Salvador.

6. Generalidades del Servidor:

Marca:	HP	Marca:	HP
Modelo:	Proliant ML370 BRC520102C	Modelo:	Proliant
Serie:	BRC52310JJ	Serie:	DL380G4

7. ¿El servidor está conectado con otras sucursales?

Sí. Uno es servidor de dominio y el otro es servidor de actualizaciones

8. Descripción del funcionamiento del sistemas

- Sistema Exactus

  El sistema utilizado para todas las transacciones de la empresa
- Control Bancario

  Módulo de Procesamiento de Transferencias Bancarias
- Contabilidad General

  Módulo de Procesamiento de Información Financiera
- Cuentas por Cobrar

  Módulo de Procesamiento de Clientes con Cuentas x Cobrar
- Cuentas por Pagar

  Módulo de Procesamiento de Cuentas por Pagar
- Recursos Humanos

  Módulo dónde se almacena Información de Recursos Humanos
- Control de Nóminas

  Módulo de Procesamiento de Planillas
- Activos Fijos

Módulo utilizado para procesar información sobre Activos de la empresa.

- Control de Inventario

  Módulo para procesar la existencia de inventario y consultas a éste.

- Facturación

  Módulo para procesar ventas, emitir facturas, tickets, y trasladar a Contabilidad.

- Presupuesto Financiero

  Módulo que crea información del presupuesto asignado por área.

- Compras

  Módulo de permite crear formularios e informes de compras.

- Estadísticas de Ventas

  Módulo que genera de forma gráfica resúmenes de ventas y montos.

- Pronóstico de Ventas

  Módulo que crea información relacionada con ventas.

- Caja Chica

  Módulo que procesa informes de Caja Chica

- Control de Vacación

  Módulo para crear informes sobre Control de vacaciones.

9. ¿Qué tipo de reportes que genera el sistema?

Planillas, Presupuestos, Facturas, Reportes Estadísticos, Estados Financieros, etc.

10. ¿Cuáles son los tipos de lenguaje de programación?

Visual Basic

11. ¿El servidor está conectado con la unidad central?
Sí.

12. ¿Cuál es el horario de uso del servidor?
Se enciende a las 7:45 am y se apaga a las 5:15 pm

Programas

1. ¿Qué sistema operativo utiliza el servidor?
WINDOWS 2000 SERVER SP4
WINDOWS SERVER 2003 STANDARD EDITION

2. ¿Qué Lenguaje utilizan para la base de datos?
Visual Basic

Redes

1. ¿Qué tipo de red posee?
Red de Área Local, LAN

2. ¿Qué tipo de conexión poseen?

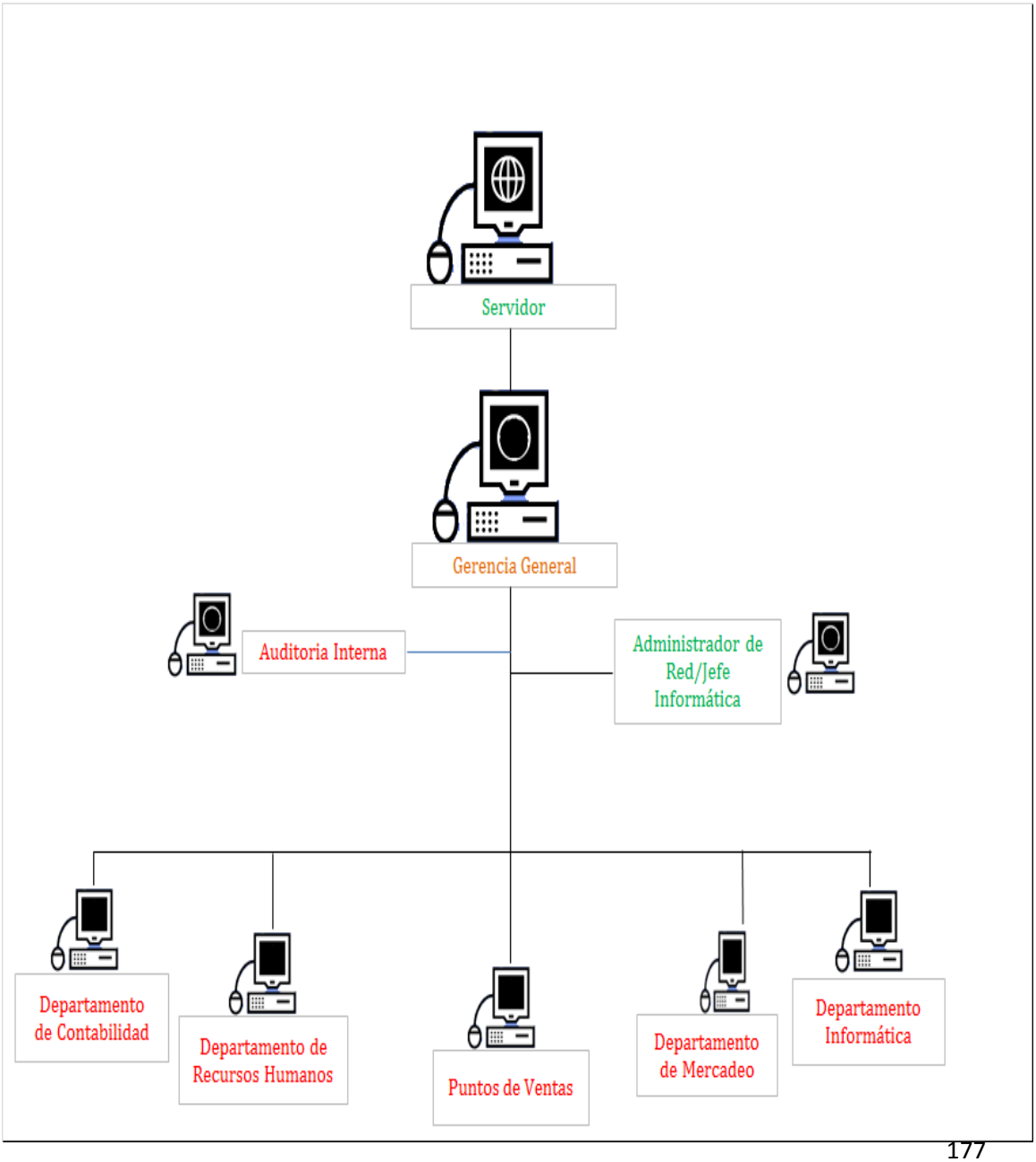
- Modem, marca Motorola, ubicado en Gerencia General
- Router 1605 series, ubicado en Departamento de Informática
- Puerto Interno FORTINET
- 1 Switch 3 Com, modelo 4210G, 48 puertos, ubicado en Informática
- 1 Switch D-Linksys, modelo DES-1016D, 16 puertos, ubicado en Auditoría Interna

3. ¿Qué tipo de enlace tienen?
Vía Modem, proveedor TIGO.

ANEXO # 5

Grupo Profesional de Auditores, S. A. de C. V.

ORGANIGRAMA DE CENTRO DE CÓMPUTO DE TELÉFONOS FÁCILES S.A DE C.V.



ANEXO # 6

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Elaborado por: Rocío Elizabeth Bolaines Portillo

Revisado por: Ernesto Scarlett Martínez Páiz

CUESTIONARIO DE EVALUACION DE SEGURIDAD FISICA

PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1. ¿Se han adoptado medidas de seguridad en el departamento de informática?	**X**			
2. ¿Existen una persona responsable de la seguridad?	**X**			
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?	**X**			
4. ¿Existe personal de vigilancia en la institución?	**X**			
5. ¿La vigilancia se contrata? a) Directamente b) Por medio de empresas que venden ese servicio	 **X**			
6. ¿Se investiga a los vigilantes cuando son contratados directamente?			**X**	

7. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?	**X**			
8. ¿Existe vigilancia en el departamento de cómputo las 24 horas?		**X**		
9. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas? a) Vigilante b) Recepcionista? c) Tarjeta de control de acceso		**X**		
10. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?		**X**		
11. ¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?	**X**			
12. El edificio donde se encuentra la computadora está situado a salvo de:				
a) Inundación	**X**			
b) Terremoto		**X**		
c) Fuego		**X**		
d) Sabotaje	**X**			
13. El centro de cómputo tiene salida al exterior?	**X**			
14. ¿Existe control en el acceso a este cuarto? a) Por identificación personal		**X**		

b) Por tarjeta magnética c) Por claves verbales d) Otras				
15. ¿Son controladas las visitas y demostraciones en el centro de cómputo?		**X**		
16. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?	**X**			
17. Existe alarma para: a) Detectar fuego (calor o humo) en forma automática b) Avisar en forma manual la presencia del fuego c) Detectar una fuga de agua d) Detectar magnéticos e) Otros	**X** **X** **X**	**X** **X** **X**		
18. Dónde están ubicadas estas alarmas a) En el departamento de cómputo b) otros	**X**			
19. ¿Existe alarma para detectar condiciones anormales del ambiente? a) En el departamento de cómputo b) en otros lados		**X**		
20. ¿La alarma es perfectamente audible?	**X**			
21. Esta alarma también está conectada:				

a) Al puesto de guardias		**X**		
b) O algún otro	**X**			
22. Existen extintores de fuego				
a) Manuales	**X**			
b) Automáticos		**X**		
c) No existen				
23. ¿Se ha adiestrado el personal en el manejo de los extintores?		**X**		
24. Los extintores, manuales o automáticos son a base de:				
a) Agua				
b) Gas	**X**			
c) Otros				
25. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?	**X**			
26. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?			**X**	
27. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause más daño que el fuego?			**X**	
28. ¿Si los extintores automáticos son a base de gas, Se ha tomado medidas para evitar que el gas cause más daño que el fuego?			**X**	

29. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?	**X**			
30. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?	**X**			
31. ¿Existe salida de emergencia?		**X**		
32. Esta puerta solo es posible abrirla: a) Desde el interior b) Desde el exterior c) Ambos Lados			**X**	
33. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?			**X**	
34. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?		**X**		
35. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?	**X**			
36. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?	**X**			

37. ¿Se tienen establecidos procedimientos de actualización a estas copias?	**X**			
38. ¿Cuál es el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información?			**2**	
39. ¿Existe departamento de auditoría interna en la institución?	**X**			
40. Este departamento de auditoría interna conoce todos los aspectos de los sistemas?		**X**		
41. ¿Se auditan los sistemas en operación?		**X**		
42. ¿Con que frecuencia? a) Cada seis meses b) Cada año c) Otra (especifique)			**X**	
43. ¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es? a) Usuario b) Director de informática c) Jefe de análisis y programación d) Programador	 **X** **X**			
44. ¿La solicitud de modificaciones a los programas se hacen en forma? a) Oral				

b) Escrita	**X**			
45. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?	**X**			
46. ¿Existe control estricto en las modificaciones?		**X**		
47. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?	**X**			
48. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?	**X**			
49. Se verifica identificación:				
a) De la terminal				
b) Del Usuario	**X**			
50. ¿Existen controles y medidas de seguridad sobre las siguientes operaciones?				
a)Recepción de documentos	**X**			
b) Información Confidencial	**X**			
c)Captación de documentos	**X**			
d)Cómputo Electrónico	**X**			
e)Programas	**X**			
f) Documentos de Salida	**X**			
g) Archivos Magnéticos	**X**			
h) Operación del equipo de computación	**X**			
i) En cuanto al acceso de personal	**X**			
j) Identificación del personal	**X**			
k) Seguros contra robo e incendio	**X**			
l) Cajas de seguridad	**X**			

ANEXO #7

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Elaborado por: Oscar René Gómez Hernández

Revisado por: Ernesto Scarlett Martínez Páiz

CUESTIONARIO DE SEGURIDAD LÓGICA

Objetivo: Identificar el proceso y los mecanismos para el control y manejo de las actividades de Seguridad Lógica realizadas en la empresa.

PREGUNTA	SI	NO	N/A	OBSERVACIONES
1. ¿Existe una persona asignada formalmente (por escrito) como responsable de la seguridad lógica de los equipos de cómputo principales como los servidores de la Institución?		X		
2. ¿Existen claves de usuarios en cada equipo de cómputo como mecanismos de identificación y autenticación?	X			
3. ¿Existen procedimientos escritos para la asignación, modificación y eliminación de claves de los usuarios?		X		No existen procedimientos por escrito pero el Jefe de Informática realiza dichos procesos.
4. ¿Existen procedimientos escritos para la administración de cuentas (creación, modificación, bloqueo y eliminación)?		X		

5. ¿Se ha establecido un estándar en cuanto a la longitud y combinación de caracteres de las claves de usuario?	X			
6. ¿El sistema operativo permite el ingreso solo a usuarios autorizados?	X			
7. ¿Existe una administración en el manejo de cuentas especiales (cuentas sin contraseñas, cuentas predeterminadas, cuentas de invitados, cuentas de acceso de comandos, cuentas de grupo, etc.), si las hay?	X			
8. ¿Existen cambios en las claves de usuario periódicamente?		X		
9. ¿La seguridad de los datos es controlada por el sistema operativo? O existe otro medio?	X			
10. ¿Se restringe el uso de terminales o estaciones de trabajo a través de la clave del usuario?	X			
11. ¿Las claves de usuario pueden ser cargadas en la red una sola vez?		X		
12. ¿Se desactiva o paraliza la terminal del usuario, en caso de estar cierto tiempo sin uso?		X		
13. ¿Son encriptados las claves de usuario, en caso de estar cierto tiempo sin uso?		X		
14. ¿Existen controles para bloquear las terminales o estaciones de trabajo, luego de cierta cantidad de intentos fallidos en el momento de ingresar la clave?	X			

15. ¿Existe una bitácora de acceso a la red, programas o utilitarios donde se pueda observar fecha y hora de ingreso de los usuarios?	X			
16. ¿Existe restricción del acceso a la red y a las aplicaciones de acuerdo con horarios predeterminados?	X			
17. ¿Existe un inventario total del software instalado en los equipos de la institución?	X			
18. ¿Cuenta la Institución con todas las licencias de los software instalados?	X			
19. ¿Alguien está a cargo de revisar que no se instale software ilegal o que no es de importancia para el desarrollo de las actividades dela Institución?	X			
20. ¿Existe algún procedimiento por si se encuentra software no autorizado en los equipos?	X			
21. ¿Cuentan los equipos con algún software antivirus? Cuál es?	X			ESET NOD 32 versión 4.
22. ¿Existen procedimientos que aseguren que el antivirus se encuentra actualizado?	X			
23. ¿Las unidades de disquete y CD instalados en los equipos están habilitadas?	X			
24. ¿Existe algún procedimiento para revisar los medios de almacenamiento contra virus antes de bajar la información del disco duro o de la red?	X			
25. ¿Existen restricciones de	X			

autorización que restrinjan el acceso a un nivel determinado del sistema?				
26. ¿Existen procedimientos contra la alteración no autorizada de información con fines propios?	X			
27. ¿Se cuenta con acceso a internet?	X			Pero sólo los Jefes de Departamento
28. ¿Existen políticas sobre el uso de internet por parte de los empleados?	X			
29. ¿Existen controles para resguardar la información de la organización, en caso de utilizarse acceso a internet?	X			
30. ¿Se restringe el acceso a diferentes sitios de ocio en internet?	x			Todos los sitios de ocio están restringidos

ANEXO # 8

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Elaborado por: Rocío Elizabeth Bolaines Portillo

Revisado por: Ernesto Scarlett Martínez Páiz

LISTA DE VERIFICACIÓN

OBJETIVO: Solicitar y revisar los planes y lineamientos establecidos para garantizar la S**eguridad Física y Lógica en la empresa.**

ITEM A EVALUAR	CUMPLE	NO CUMPLE	OBSERVACIONES
¿La información de la empresa se encuentra siempre disponible para cumplir sus propósitos?	X		
¿Existe algún análisis de riesgos en la organización?		X	
¿La información susceptible de robo, pérdida o daño se encuentra protegida y resguardada?	X		
¿Existe Documentación en cuanto a: políticas aplicables, análisis de riesgos, descripción de procesos, lista de controles.	X		

¿La empresa tiene conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas?		X	
¿Se cuenta con un sistema de control de acceso y autorización?	X		
¿Se mantiene un registro de las actividades que los Administradores y usuarios realizan sobre un sistema?	X		
¿Se aplican barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial?	X		
¿Se cuenta con planes de contingencia y de manejo de incidentes?		X	
¿En la empresa se han contemplado las amenazas ocasionadas por el hombre?	X		
¿La empresa tiene un plan para la realización de backups?		X	

¿Se evalúan y controlan permanentemente la seguridad física de las instalaciones de cómputo y del edificio donde funciona la empresa?	X		
¿La empresa tiene implementados firewalls?	X		
¿Existen procedimientos y barreras que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo?	X		
¿Existe una política específica del sistema para el manejo de seguridad?		X	
¿Se asegura que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto?	X		
¿Existen políticas para el manejo de redes, sistemas operativos, aplicaciones, etc.?	X		
¿Existen sistemas alternativos secundarios de transmisión de información entre diferentes puntos?		X	

¿Existen políticas para el manejo de Internet?	X		
¿Los operadores pueden trabajar sin una supervisión minuciosa y no pueden modificar los programas ni los archivos que no correspondan?	X		
¿Existen políticas para el manejo de otras redes externas?	X		
¿La información transmitida es recibida por el destinatario al cual ha sido enviada y no a otro?	X		
¿Las funciones de seguridad están integradas en las funciones del personal?		X	
¿Se realiza un plan de seguridad física contra catástrofes como: inundaciones, incendios, cortes de energía?		X	

ANEXO # 9

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Elaborado por: Oscar René Gómez Hernández

Revisado por: Ernesto Scarlett Martínez Páiz

LISTA DE CHEQUEO PARA EL CASO DE LA SEGURIDAD FÍSICA EN INSTALACIONES DE CÓMPUTO

*(Recuérdese que se marca **SI** cuando el elemento está correctamente establecido para reflejar un fortaleza de control interno y **NO** en caso contrario)*

ELEMENTO A EVALUAR	SI	NO
¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del área de servidores para evitar daños al equipo?	X	
¿Está el área de servidores protegido de la luz solar directa?	X	
¿Está el centro de cómputo libre de ventanas hacia el exterior?		X
¿Tiene el área de servidores una iluminación mínima adecuada?		X
¿Se encuentran todos los elementos de iluminación a una altura adecuada?	X	
¿Cuenta el área de servidores con las luces de emergencia mínimas necesarias?		X
¿Se encuentran los interruptores de iluminación en un sitio adecuado?		X

¿Están separados los circuitos eléctricos de iluminación de los circuitos que alimentan los equipos?		X
¿Está limitada la existencia de artículos y materiales inflamables en el área de servidores?	X	
¿Se prohíbe a los operadores fumar dentro del área de servidores?	X	
¿Está instalada una alarma para detectar fuego (calor o humo) en forma automática?		X
¿La cantidad de estaciones manuales para comunicar la presencia de fuego es la adecuada?	X	
¿La cantidad y tipo de extintores automáticos en el área de servidores es la adecuada?		X
¿Si es que existen extintores automáticos son activados por detectores automáticos de fuego?		X
¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal corte la acción de los extintores por tratarse de falsas alarmas?		X
¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal pueda cortar la energía eléctrica?		X
¿En caso de que los extintores sean a base de gas, existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal pueda abandonar el local sin peligro de intoxicación?	X	
¿La cantidad de extintores manuales en el área de servidores es la adecuada?		X
¿El personal del área de servidores ha recibido capacitación del uso de extintores manuales?		X
¿Los extintores manuales o automáticos utilizados utilizan		

un agente que no dañe los equipos?		X
¿Se le da mantenimiento preventivo al sistema de extintores automáticos de manera periódica y programada?		X
¿Se verifica cada cierto tiempo que los extintores manuales estén cargados y funcionando correctamente?	X	
¿Existe un procedimiento establecido de acción en caso de una emergencia ocasionada por fuego?		X
¿Están los ductos de entrada de cableado al área de servidores debidamente sellados en su parte externa?	X	
¿Está el área de servidores construido con materiales anti-inflamables?		X
¿Los muebles del área de servidores fueron construidos con materiales anti-inflamables?		X
¿Son los cestos para basura de un material metálico que evite la propagación de fuego?		X
¿Está el área de servidores situado sobre el nivel del mar?		X
¿Está el área de servidores lejos de tuberías, desagües y canoas?	X	
¿Existe un mecanismo para detectar una fuga o derramamiento de agua?		X
¿Es el techo del área de servidores impermeable para evitar el paso de agua desde niveles superiores?		X
¿Están construidas las puertas del área de servidores de manera que sellen las entradas ante fugas externas, bloqueando el ingreso de agua por las mismas?		X
¿Contiene el área de servidores un drenaje en el piso en caso de ingreso de agua?		X

¿Tiene el local donde está instalado el área de servidores la protección antisísmica apropiada?		X
¿Están los equipos del área de servidores instalados con aditamentos especiales antisísmicos tales como anclajes al piso?		X
¿Existe una persona responsable de la seguridad a tiempo completo?		X
¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?	X	
¿Se controla el trabajo fuera de horario?		X
¿Existe vigilancia en el departamento de cómputo las 24 horas?		X
¿Existe un control de acceso con notificación en la entrada del departamento de cómputo?	X	
¿Se ha instruido a los encargados del centro de cómputo sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?		X
¿Existe una bitácora de las visitas e ingresos al área de servidores?		X
¿Tiene el local en donde se encuentra el área de servidores protección contra rayos?		X
¿Está el cableado eléctrico debidamente aterrizado según las necesidades de los equipos?	X	
¿Viajan los cables eléctricos por ductos separados que los del cableado de datos?	X	
¿Está el cableado eléctrico instalado sobre ductos de protección?	X	
¿Tiene la red eléctrica protección contra sobrecargas?	X	

¿Si se utilizan baterías de reserva, existe la ventilación adecuada necesaria?	X	
¿Existe una o varias UPS's que soporten la carga eléctrica del área de servidores?	X	
¿Existe una fuente de alimentación alterna para casos de falla de la alimentación normal?	X	
¿Se realizan mantenimientos periódicos a esta fuente de alimentación alterna?	X	
¿Está el cableado de datos debidamente canalizado e identificado?	X	
¿Se encuentran todas las canalizaciones protegidas de accesos ilícitos?	X	
¿Cuentan las puertas de área de servidores con cerraduras de seguridad adecuadas?	X	
¿Están las personas de limpieza capacitadas para realizar las funciones de aseo dentro del área de servidores?	X	
¿Cuenta el área de servidores con un proceso adecuado de desecho de papelería?		X

ANEXO # 10

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Elaborado por: Rocío Elizabeth Bolaines Portillo

Revisado por: Ernesto Scarlett Martínez Páiz

MATRIZ DE RIESGO INFORMATICO

Matriz de Análisis de Riesgo		Probabilidad de Amenazas					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos Físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir Contraseñas	No cifrar datos críticos
		3	4	3	2	2	2
Datos e Información							
RR.HH	4	12	16	12	8	8	8
Finanzas	1	3	4	3	2	2	2
Sistemas e Información							
Computadoras	4	12	16	12	8	8	8
Portátiles	2	6	8	6	4	4	4
Personal							
Coordinador	3	9	12	9	6	6	6
Pesonal Técnico	2	6	8	6	4	4	4

Bajo Riesgo = 1 – 6 (verde)

Medio Riesgo = 8 – 9 (amarillo)

Alto Riesgo = 12 – 16 (rojo)

ANEXO # 11

Grupo Profesional de Auditores, S. A. de C. V.

PROGRAMA DE SEGURIDAD FISICA

AREA: SEGURIDAD FÍSICA **REF. SF/1**

NOMBRE DE LA INSTITUCION: Teléfonos Fáciles S.A de C.V

AUDITOR DE CAMPO: Rocío Elizabeth Bolaines Portillo

SUPERVISOR: Ernesto Scarlett Martínez Páiz

EJERCICIO ECONOMICO: 2012

FECHA INICIO: 1 de Julio de 2012 **FECHA FINALIZACION:** 30 de Septiembre de 2012

INTRODUCCIÓN:

Este programa es una guía de los procedimientos básicos de auditoria de sistemas que deben ser realizados como pruebas de que la entidad cuenta con las instalaciones adecuadas para su funcionamiento y para asegurar el resguardo de los equipos y del personal con que cuenta**.**

OBJETIVOS:

1. Verificar y evaluar los controles físicos y ambientales establecidos en el centro de cómputo y áreas usuarias, con el fin de asegurar que se protejan tanto la seguridad física de las instalaciones donde esté ubicado el servidor, computadoras usuarias y personal de informática.

2. Verificar y evaluar los controles establecidos en el centro de cómputo y áreas usuarias, posibiliten controlar el acceso físico y la protección contra daños y fallas en los suministros de corriente, agua, aires acondicionados y extintores de fuego.

Referencia PT	PROCEDIMIENTOS	Elaborado por	Revisado por
	SEGURIDAD FISICA		
SF-1	1. Visitar las instalaciones de la empresa.	**R.E.B.P**	**E.S.M.P**
SF-2	2. Observe si las áreas usuarias del sistema tienen accesos restringidos exclusivamente para los responsables y/o colaboradores de las mismas y elaborar una cédula narrativa de ello.	**R.E.B.P**	**E.S.M.P**
SF-3	3. Elaborar una cédula de inventario de equipo del área de informática que contenga: • Referencia. • Identificación del producto. • Descripción (Nombre, Marca, Modelo, Serie, Color). • Fecha de adquisición. • Observaciones.	**R.E.B.P**	**E.S.M.P**
SF-4	4. Elaborar una cédula de inventario de equipo del área de auditoria interna que contenga: • Referencia. • Identificación del producto.	**R.E.B.P**	**E.S.M.P**

	• Descripción (Nombre, Marca, Modelo, Serie, Color). • Fecha de adquisición. • Observaciones.		
SF-5	5. Elaborar una cédula de inventario de equipo del área de contabilidad que contenga: • Referencia. • Identificación del producto. • Descripción (Nombre, Marca, Modelo, Serie, Color). • Fecha de adquisición. • Observaciones.	**R.E.B.P**	**E.S.M.P**
SF-6	6. Elaborar una cédula de inventario de equipo del área de logística que contenga: • Referencia. • Identificación del producto. • Descripción (Nombre, Marca, Modelo, Serie, Color). • Fecha de adquisición. • Observaciones.	**R.E.B.P**	**E.S.M.P**
SF-7	7. Elaborar una cédula de inventario de mobiliario que es utilizado en las diferentes áreas donde se encuentran los usuarios de los equipos informáticos. Esta cédula contiene:}	**R.E.B.P**	**E.S.M.P**

	• Referencia. • Código del mobiliario. • Descripción del mobiliario (Nombre, Marca, Serie, Color). • Área asignada. • Persona responsable del mobiliario. • Observaciones.		
SF-8	8. Elaborar una cédula narrativa de condiciones de mobiliario y equipo de la empresa que es utilizado para colocar el equipo informático.	**R.E.B.P**	**E.S.M.P**
SF-9	9. Hacer una narrativa de las condiciones físicas del local en que se encuentran la casa matriz y las sucursales elegidas como muestra.	**R.E.B.P**	**E.SM.P**
SF-10	10. Hacer una narrativa de las condiciones del local del punto de venta elegido como muestra.	**R.E.B.P**	**E.S.M.P**
SF-11	11. Verificar la existencia de rutas de evacuación de las instalaciones de la empresa.	**R.E.B.P**	**E.S.M.P**
SF-12	12. Elaborar una cedula narrativa de las rutas de evacuación que tiene la empresa en caso de emergencia.	**R.E.B.P**	**E.S.M.P**
SF-13	13. Verificar y elaborar una cédula narrativa de las medidas de seguridad que tiene la empresa contra posibles	**R.E.B.P**	**E.S.M.P**

	casos de incendios que pudiesen ocurrir en las instalaciones de la casa matriz. 14. Verificar si existen suministros de energía para las maquinas que se utilizan.		
SF-15	15. Elaborar una cedula analítica de suministros de energía que contengan: • Referencia. • Tipo de suministro. • Descripción general del suministro que contendrá, el nombre, color, marca, modelo, serie, color. • Fecha en que fue adquirido. • Tiempo de uso diario. • Lugar al que ha sido asignado. • Observaciones.	**R.E.B.P**	**E.S.M.P**
SF-16	16. Elaborar una cédula narrativa de mantenimiento de suministros de energía. 17. Solicitar el manual de uso de los suministros de energía con que cuenta la empresa.	**R.E.B.P**	**E.S.M.P**
SF-18	18. Elaborar cédula analítica para determinar el correcto uso de dichos suministros. 19. Verificar la existencia de extintores en las instalaciones de la empresa.	**R.E.B.P**	**E.S.M.P**
SF-20	20. Elaborar una cédula analítica de	**R.E.B.P**	**E.S.M.P**

	extintores que contenga: • Referencia. • Ubicación del extintor. • Descripción. • Peso. • Fecha que se compró. • Ultima fecha de carga. • Persona responsable. • Proveedor. • Observaciones.		
SF-22	21. Verificar la existencia de aires acondicionados en la empresa. 22. Elaborar una cédula analítica de aires acondicionados que contenga: • Referencia • Descripción • Ubicación • Fecha de adquisición • Tiempo que permanece encendido • Persona encargada de su uso • Observaciones.	**R.E.B.P**	**E.S.M.P**
SF-23	23. Elaborar una cédula narrativa de la temperatura de los aires acondicionado en las áreas en donde se encuentren los equipos informáticos.	**R.E.B.P**	**E.S.M.P**
SF-24	24. Elaborar cédula analítica de cableado del área donde se encuentra el equipo	**R.E.B.P**	**E.S.M.P**

SF-25	informático de la empresa. 25. Elaborar cédula analítica de mantenimiento de cableado de la empresa.	**R.E.B.P**	**E.S.M.P**

ANEXO # 12

Grupo Profesional de Auditores, S. A. de C. V.

PROGRAMA DE SEGURIDAD LOGICA
AREA: SEGURIDAD LOGICA

REF. SL/1

NOMBRE DE LA INSTITUCION: Teléfonos Fáciles S.A de C.V

AUDITOR DE CAMPO: Oscar René Gómez Hernández

SUPERVISOR: Ernesto Scarlett Martínez Páiz

EJERCICIO ECONOMICO: 2012

FECHA INICIO: 1 de Julio de 2012 **FECHA FINALIZACION:** 30 de Septiembre de 2012

OBJETIVOS:

- Identificar los documentos fuente, para el origen de datos ingresados al sistema.
- Evaluar si en los formularios del sistema, se requieren los datos en el orden lógico del contenido de los documentos fuentes.
- Verificar si en las pantallas de captura de datos, los campos están diseñados adecuadamente según el tipo de datos a ingresar por el usuario: caracteres, dígitos y fechas.
- Verificar si en las pantallas de captura de datos, el sistema valida valores y procesos, según corresponda.
- Verificar que los cálculos requeridos son realizados automáticamente por el sistema.

- Determinar la exactitud de los procesos realizados por el sistema.
- Evaluar los controles lógicos implementados en el sistema, para el registro de actividades realizadas por los usuarios en las interfaces del mismo.

REF. PT´S	PROCEDIMIENTOS	HECHO POR:	REV. POR:
	CLAVES DE ACCESO		
SLC-1	1. Evaluar el esquema de seguridad que se ha establecido para el acceso al sistema y a los datos que esta posee por ello se realizará cédula narrativa donde se especifiquen lo siguiente: a. Cuales son las políticas que se aplican a la Administración de la seguridad. b. Si existe un módulo determinado para la asignación de acceso a usuarios. c. Como se establecen los niveles de acceso a los usuarios. d. Cual es el nivel de protección existente sobre las tablas o bases de datos al sistema: • Verificar su alcance desde el sistema operativo (DOS o Windows) • Probar el acceso desde otros programas gestores de una base de datos (ACCES, VISUAL BASIC, FOX PRO o Excel) e. Si se tienen los archivos de ejecución del software y no el software de ejecución completo.	O.R.G.H	E.S.M.P
SLC-2	2. Verificar si el sistema cuenta con los siguientes controles de acceso de seguridad, para ello elaborar una cedula narrativa que contenga: a. Identificación del usuario (ID) b. Palabras clave de acceso (pasword) c. Mecanismos de autorización: Derecho a acceso a diversos recursos del sistema, debidamente	OR.G.H	E.S.M.P

	especificado por las reglas de autorización.		
SLC-3	3. Con una de las terminales donde corre el sistema, digitar clave al azar y verificar el número de intento permitido con pasword inválidos para sacarlo de la sesión. Elaborar narrativa.	O.R.G.H.	E.S.M.P
SLC-4	**4.** Solicitar el acceso a un usuario del sistema simultáneamente en diversas terminales para verificar el acceso al software y elaborar una cedula narrativa sobre este proceso.	O.R.G.H	E.S.M.P
SLC-5	**5.** Verificar si toman en cuenta algunas consideraciones por el administrador del sistema, para el establecimiento de palabras clave de acceso (password) a través de una cedula narrativa donde se evalúen: a. Generación del password: control que prevenga a los usuarios usar el mismo password cada ciclo. b. El ciclo de uso es por periodos menores a cada mes. c. Propiedad de password: son asignados a un solo usuario. d. Longitud y composición: son de al menos 6 caracteres alfa numéricos. e. Almacenamiento de password: El archivo maestro de password se almacena encriptado. f. Entradas de password: No son desplegables en pantallas cuando son digitados. g. Deben reingresarse al permanecer inactivos las terminales por más de 5 minutos. h. Son asignados por el propio usuario. i. Utilización asignados en diversos niveles: modulo dentro de la aplicación.	O.R.G.H	E.S.M.P
SLC-6	6. Verificar si existen instrucciones formales que orienten a los usuarios en la adecuada elección de password y evaluar si contemplan los siguientes elementos de no uso, elaborando cedula narrativa: a. Iníciales del nombre. b. Apodos. c. Nombres de conyugue o hijos. d. Fecha de cumpleaños.	O.R.G.H.	E.S.M.P

	e. Teléfonos. f. Direcciones. g. Letras o números consecutivos. h. Frases fáciles de adivinar. i. Palabras anteriormente utilizadas. **ORIGEN DE DATOS:**		
SLO-7	7. Elaborar cedula narrativa de origen de base de datos donde: Se identifique el origen de la base de datos: Documental, directo, automático, hibrido.	O.R.G.H.	E.S.M.P
SLO-8	8. Identificar los documentos que contienen los datos a ingresar en el sistema y elaborar un listado de estos, relacionándolos con el módulo específico del sistema donde se requieren.	O.R.G.H	E.S.M.P
	9. Si el origen de los datos es documental, verificar si se hace uso de documentos pre-impresos o formularios completados a mano en la secuencia de ingreso de datos al sistema.		
SLO-10	10. Si el ingreso de datos al sistema es por medio de documentos, a través de una cedula narrativa evaluar: a. Si están elaborados de acuerdo a la secuencia de ingreso al sistema. b. Se presentan títulos y encabezados descriptivos. c. Si están bien identificados y numerados. d. Si tienen espacio suficiente para correcciones y para firmas de responsable.	O.R.G.H	E.S.M.P
	ENTRADA DE DATOS:		
SLE-11	11. Determinar que validaciones existen en la pantalla de captura y verificar que el elemento de esta esté configurado correctamente, para lo cual se elaborará	O.R.G.H	E.S.M.P

	cedula narrativa de este proceso, donde se detallara lo siguiente: a. Evaluar los campos numéricos probando que no se puedan ingresar valores negativos donde no corresponda. b. Probar que los campos numéricos no acepten cantidades. c. Verificar que no se realicen cálculos manuales previamente a ser ingresados al sistema cuando dichos valores puedan operarse automáticamente. d. Realizar comprobaciones de valores numéricos operados dentro del sistema. e. Evaluar que los valores por cálculos automáticos en la aplicación no puedan ser modificadas manualmente por los usuarios. **CAMPOS TIPO MONEDA:** a. Evaluar los campos de tipo moneda, en los cuales existan límites de montos a ingresar respecto a otros valores también almacenados en el sistema. b. Verificar que no se puedan ingresar caracteres. **CAMPOS TIPO FECHA:** a. Revisar los campos con datos tipo fecha, donde se facilita su b. digitación, validando además los rangos de fecha permitidos por estos. c. Verificar la validación de fechas futuras donde amerite hacerse. d. Verificar que no se acepten fechas incongruentes con días, meses o años inválidos, a través de mascaras de entrada bien definidas. e. Verificar que no se puedan ingresar caracteres o dígitos. **CAMPOS CON FORMATO PREDEFINIDO.** a. Indagar y probar campos para los cuales existe un formato predefinido de ingreso de datos. b. Revisar mascaras de entrada para códigos o números		

	que tienen un formato establecido desde el origen de su emisión (ejemplo: NIT, NUP, ISSS, entre otros).		
SLE-12	12. Verificar que no se permita dejar campos vacios cuando estos sean de gran importancia para controles o cálculos en una misma pantalla o en otras del sistema.	O.R.G.H	E.S.M.P
SLE-13	13. Determinar el nivel de actualización o desfase en el ingreso de datos al sistema.	O.R.G.H	E.S.M.P
	PROCESO DE DATOS.		
SLP-14	14. Verificar los procesos que se realizan en el sistema fuera de las pantallas de captura (cierres, actualizaciones, o cargos de datos), a fin de determinara si se le da seguimiento al procedimiento establecido, realizar narrativa de este proceso y evaluar lo siguiente: a. Verificar los cálculos de mayor importancia con base a los datos con que fue alimentado. b. De ser necesario, solicitar se muestre el código fuente para procesos delicados que no satisfacen la confianza del auditor.	O.R.G.H	E.S.M.P
	SALIDA DE INFORMACION:		
SLS-15	15. Determinar su la información proporcionada por el sistema es suficiente para el usuario final o se ve en la necesidad de re-procesarla fuera del sistema, ello se especificará en una cédula narrativa.	O.R.G.H	E.S.M.P
SLS-16	16. Verificar que los reportes que se generan estén bien identificados, para ello elaborar cedula analítica que contenga: • Referencia • Tipo de reporte. • Área donde se emita.	O.R.G.H	E.S.M.P

	• Titulo coherente con la información que contiene si / no. • Encabezado adecuado. • Periodo cubierto. • Fecha de generación. • Hora de generación. • Nombre del programa que lo genera. • Nombre del usuario que lo emite. • Numeración de páginas. • Totales por reporte. 17. Verificar que los reportes generados y guardados no puedan ser editados por el usuario. **FIREWALL**		
SLF-18	18. Realizar inventario de firewall, para ello se elaborará una cédula analítica de Inventario, que contenga: • Referencia a los papeles de trabajo • Nombre del Firewall • Versión • Cantidad instalados • Ubicación • Año de instalación • Comentarios	O.R.G.H	E.S.M.P
SLF-19	19. Hacer una cédula narrativa del funcionamiento de los firewalls	O.R.G.H	E.S.M.P
	ROUTERS		
SLR-20	20. Hacer cédula de inventario de Routers que contenga: • Referencia de Papeles de Trabajo • Nombre del Router • Marca • Modelo • Serie • Ubicación • Comentarios	O.R.G.H .	E.S.M.P

SLA-21	**ANTIVIRUS** 21. Realizar inventario de antivirus, para ello elaborar cédula analítica de inventario de firewall, que contenga: • Referencia de papeles de trabajo • Nombre del antivirus • Proveedor • Periodicidad de actualización • Se tiene licencia • Equipos instalados • Comentarios	O.R.G.H	E.S.M.P

ANEXO # 13

Grupo Profesional de Auditores, S. A. de C. V.

PERFIL DE PERSONAL ASIGNADO

Una de las partes más importantes dentro de la planeación de la auditoria en informática es el personal que deberá participar y sus características.

NOMBRES/CARGO	GRADO ACADEMICO	EXPERIENCIA
Rocío Elizabeth Bolaines Portillo (Auxiliar de Auditoría)	Lic. Contaduría Pública.	Contabilidad, Asesorías, Consultoría, Auditoría Fiscal y Auditor de Sistemas.
Oscar René Gómez Hernández (Auxiliar de Auditoría)	Lic. Contaduría Pública y Técnico en Sistemas.	Contador, Auditor de Sistemas, Administrador de Redes, Programador.
Ernesto Scarlett Martínez Páiz (Supervisor de Auditoría)	Lic. Contaduría Pública y Técnico en Computación.	Contador, Auxiliar de Auditoría de Sistemas, Programador, Jefe de Informática.
Federico Paredes (Consultor)	Ing. en Sistemas	Profesional Externo. Persona Experta contratada para cumplir con NIA 620.

COMPETENCIAS	NIVEL ACADEMICO
Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervengan esté: • Debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo. • Características de conocimientos, práctica profesional y capacitación. • Con el suficiente nivel para poder coordinar el desarrollo de la auditoria, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.	• Ing. En Sistemas • Lic. En Computación • Técnico en informática. • Experiencia en el área de informática. • Experiencia en operación y análisis de sistemas. • Conocimientos de los sistemas más importantes. • Lic. En Contaduría Pública. En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes,

Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

ANEXO #14

CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES / SEMANAS	JULIO				AGOSTO				SEPTIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4
Presentación de Carta Oferta de Servicios para realizar Auditoria de Sistemas												
Presentación y firma de Carta Compromiso para realizar Auditoría.												
Recorrido de las instalaciones												
Evaluación de rutas de evacuación y seguridad física												
Entrevista preliminar												
Procedimientos de auditoria												
Evaluación de las condiciones del Centro de Cómputo												
Conteo físico de inventario de hardware												
Obtención de programas instalados en equipo de usuarios y seguridad lógica												
Otros procedimientos de obtención de evidencia												
Presentación de informe final												

ANEXO # 15

Grupo Profesional de Auditores, S. A. de C. V.

AUDITORES Y CONTADORES

TELÉFONOS FÁCILES S.A DE C.V

MEMORANDUM DE PLANEACION DE AUDITORIA DE SISTEMAS

AREA SEGURIDAD INFORMATICA

AÑO 2012

ÍNDICE DEL MEMORÁNDUM DE PLANEACIÓN

1. CONSIDERACIONES GENERALES

a) COMPROMISOS DE LA FIRMA

Realizar una auditoria especializada a la Seguridad Informática de forma adecuada, en base a la normativa técnica aplicable a los sistemas de información, permitiendo establecer una conclusión sobre el funcionamiento de la Seguridad Física y Lógica de los sistemas de información auditado.

b) OBJETIVOS DE LA AUDITORIA

GENERAL:

Emitir un informe sobre la Evaluación de la Seguridad Informática de los sistemas de información computarizados (SIC), para asegurar el correcto funcionamiento de las medidas de Seguridad Física implementadas y el cumplimiento, la integridad, confiabilidad, y confidencialidad de los sistemas, a través de las medidas de Seguridad Lógica.

ESPECIFICOS:

1. Verificar las medidas de Seguridad Física en la empresa.
2. Comprobar los controles establecidos de Seguridad Informática.
3. Comprobar la existencia de planes contingenciales que permitan seguir operando en casos de fallas o algún tipo de siniestros.
4. Verificar la existencia de controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.

5. Evaluar las condiciones del local en que se encuentra la empresa.
6. Verificar la ubicación de los servidores y las medidas de seguridad que tienen para ello.
7. Determinar el estado físico del mobiliario en el que se tienen los equipos informáticos.
8. Evaluar las condiciones ambientales bajo las que se encuentran los equipos informáticos.
9. Evaluar la idoneidad del recurso humano del área de informática.

c) ALCANCE

La evaluación a la Seguridad Informática a los sistemas de información computarizados, se realizará tomando en cuenta los siguientes parámetros:

1. La evaluación del espacio físico d la empresa.

2. La evaluación de los controles internos aplicados a los sistemas.

3. La verificación de rutas de evacuación en la empresa.

4. Evaluación de las medidas de seguridad física aplicables en la empresa en casos de siniestros como incendios, desastres naturales, robo, sabotaje, entre otras.

5. Verificación de condiciones de mobiliario y equipo de cómputo, área de servidor, cableado seguro, ergonometría, uso de extintores, aire acondicionado, suministros de energía, detectores de humo, de agua, etc.

6. La evaluación de las medidas de Seguridad Lógica, como controles de acceso, passwords, políticas de seguridad, administración de la seguridad, antivirus, firewall, routers, etc.

A través de las siguientes pruebas:

- ✓ Pruebas de control de usuario, que abarca el manual del control interno a los programas, módulos y aplicaciones; a fin de comprender la ruta crítica de la de los controles de acceso al sistemas, la aplicación de medidas de seguridad en los datos, el procesamiento de los mismos y relacionar con ello la información vinculada entre los diferentes módulos, además de entrevistas al personal de informática.

- ✓ Pruebas sustantivas, que comprenden el procesamiento electrónico de datos en los programas, módulos o aplicaciones que contiene el sistema de información; éstas tendrán como fin corroborar el cumplimiento de los siguientes aspectos:

. Identificar los errores en el procesamiento.

. Asegurar la calidad de los datos

. Comparación de datos físicos vrs. digitalizados a través de fuentes externas.

. Verificación de la comunicación a través de las diversas interfaces de red.

. Evaluación de las medidas de seguridad informática establecidas en la empresa, tanto la Seguridad Física como la Seguridad Lógica.

d) TIPO DEL INFORME A PRESENTAR

Se emitirá un informe final de auditoria el cual contendrá la conclusión final sobre la Evaluación de la Seguridad Física y Lógica de lo sistemas y las posibles sugerencias

de los hallazgos encontrados. La fecha tentativa ha ser entregado el informe es el 30 de Septiembre del presente año.

2. ENTENDIMIENTO DE LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

e) ESTUDIO Y EVALUACIÓN DE CONTROL INTERNO

Para la evaluación de la seguridad informática del os sistemas de información es necesario conocer los controles internos aplicables en los ambientes SIC, tanto los de Seguridad Física como los de Seguridad Lógica; a fin de unificar criterios y verificar el cumplimiento operativo de dichos controles.

Para el estudio y evaluación de control interno se utilizan procedimientos que verifican el cumplimiento de políticas relacionadas al control interno y dirigidas a los sistemas de la empresa a la que presta el servicio.

Inicialmente se correrán cuestionarios de evaluación de control interno y luego se verificaran los controles.

Entre los controles a verificar se encuentran:

- Controles sobre los Accesos de personas a la empresa
- Controles sobre la administración de la seguridad
- Controles sobre las políticas de seguridad existentes.
- Control sobre el funcionamiento de software de la empresa

3. NATURALEZA Y CONOCIMIENTO DEL NEGOCIO Y SU ENTORNO.

- **ANTECEDENTES DE LA EMPRESA**
- **ESTRUCTURA OPERATIVA Y ADMINISTRATIVA**
- **PUESTOS CLAVES**
- **MISIÓN VISIÓN Y VALORES DE LA EMPRESA**

- **PRINCIPALES POLÍTICAS DE INFORMÁTICA Y SEGURIDAD DE INFORMACIÓN**

1. Todos los empleados deberán seguir y revisar estas políticas, ya que pueden cambiar sin previo aviso, para ello pueden revisar en sus navegadores de Internet escribiendo en la barra de direcciones uno de los siguientes link`s http://192.168.102.12/ o por http://190.86.199.41/

2. Los jefes de cada departamento, deberán solicitar por correo electrónico del ingreso de un nuevo, para poder crear cuenta para acceso al dominio, credenciales de acceso a programas, carpetas compartidas y correo electrónico si este último es requerido, de igual forma se debe notificar cuando el empleado sea trasladado de departamento o se retire de la empresa, en el caso de vacaciones o ausencias prolongadas, se deberá identificar a los usuarios que tendrán acceso a los recursos del empleado ausente.

3. Se deberá mantener un ambiente limpio y despejado para la computador y periféricos asignados, sin obstruir principalmente entrada de aire para el correcto enfriamiento de los componentes de la computadora.

4. No quitar ni manchar el identificador numérico del equipo de cómputo.

5. La batería de la computadora (UPS) generalmente consta de dos tipos de conectores, con respaldo de batería y sin respaldo, se puede conectar los demás periféricos. Salvo solicitud por parte de líder se le dará acceso a otro empleado.

6. Al finalizar la jornada laboral se debe apagar la computadora de forma correcta, sin olvidar apagar también la batería (UPS).

4. PROGRAMACION DE LA AUDITORIA

- **DESARROLLO DEL PROGRAMA DE AUDITORIA.**

Un programa de auditoria es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoria planificados. El esquema típico de un programa de auditoria incluye lo siguiente:

1. **Tema de auditoria:** Donde se identifica el área a ser auditada.
2. **Objetivos de Auditoria:** Donde se indica el propósito del trabajo de auditoria a realizar.
3. **Planificación previa:** Donde se identifican los recursos y destrezas que se necesitan para realizar el trabajo; así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.
4. **Procedimientos de auditoria:**

- Recopilación de datos.
- Identificación de lista de personas a entrevistar.
- Identificación y selección del enfoque del trabajo
- Identificación y obtención de políticas, normas y directivas.

- Desarrollo de herramientas y metodología para probar y verificar los controles existentes.
- Procedimientos para evaluar los resultados de las pruebas y revisiones.
- Procedimientos de comunicación con la gerencia.
- Procedimientos de seguimiento.
- El programa de auditoria se convierte también en una guía para documentar los diversos pasos de auditoria y para señalar la ubicación del material de evidencia.

ANEXO #16

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Responsable: Ernesto Scarlett Martínez Páiz

Fecha de obtención de evidencia: 17 de Septiembre de 2012

PROCEDIMIENTOS DE AUDITORIA.

Observación, Revisión e Inspección.

<u>Área: Seguridad Física</u>: Suministros de Energía, Cableado, Espacio Físico.

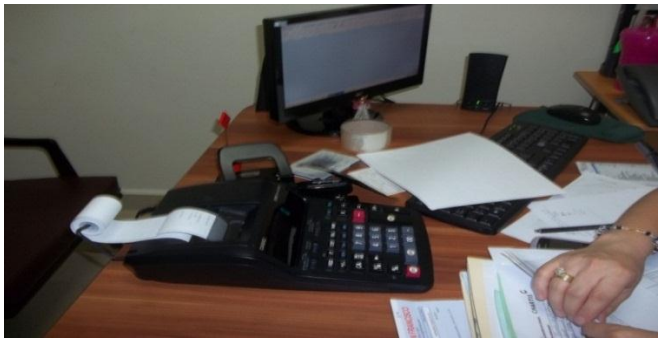
ANEXO #16

Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Responsable: Ernesto Scarlett Martínez Páiz **Fecha:** 17 de Septiembre de 2012

<u>Área: Seguridad Física</u>: Equipo de Cómputo, Aire Acondicionado, Extintor



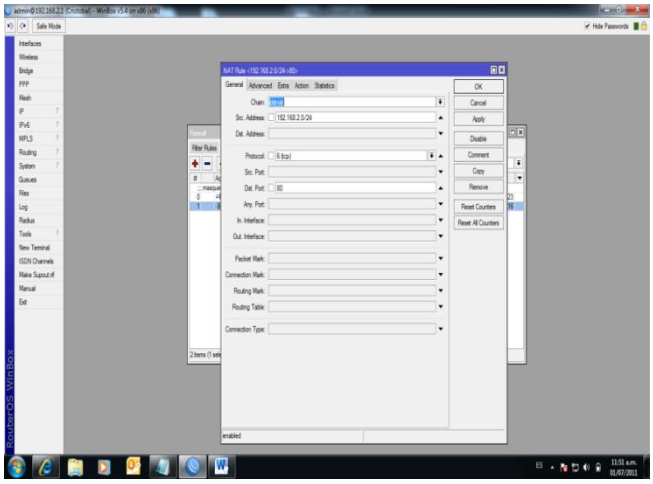
ANEXO #16

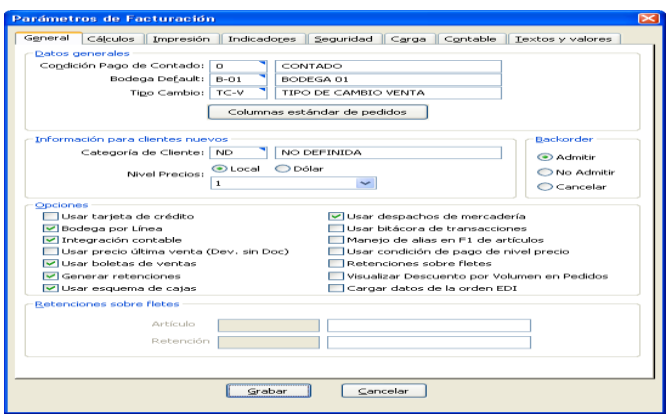
Grupo Profesional de Auditores, S. A. de C. V.

Empresa: Teléfonos Fáciles S.A de C.V

Responsable: Ernesto Scarlett Martínez Páiz **Fecha:** 17 de Septiembre de 2012

<u>Área: Seguridad Lógica:</u> Reloj Biométrico, Firewall, Captura de pantalla de programa.





ANEXO # 17

PAPELES DE TRABAJO.

AREA: SEGURIDAD FISICA.

CÉDULA DE INVENTARIO DE EQUIPO DE CÓMPUTO DEL ÁREA DE INFORMÁTICA

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

SF-2

Hoja N° 1 de 1

PREP: R.E.B.P

REV: E.S.M.P

Ejercicio: 2012; Cédula de Inventario de Equipo de Cómputo del area de Informática.

Area examinada: Seguridad Física

Fecha de inicio de Auditoria: Julio 2012

Fecha de Finalización: Septiembre 2012

Referencia	Identificación del Producto	Descripción					Fecha de adquisición	Persona responsable	Observaciones
		Nombre	Marca	Modelo	Serie	Color			
		Monitor	Hp		CNK6490D41	Gris metálico			
		Monitor	Samsung	E1920NX		Negro			
	37	CPU	SPWMX2			Gris metálico con negro			
	00041	CPU	52x max			Negro con parte gris met.			
		Teclado	Genius			Negro			
		Teclado	Genius			Negro			
		Batería	TRIPP-LITE			Negro			
		Batería	TRIPP-LITE			Negro			
		Batería	APC	Back up 550		Negro			
		Mini Laptop	Accer			Negro			

(1) *Datos según recuento físico*

ANEXO # 18

CÉDULA NARRATIVA DE CONDICIONES DE MOBILIARIO

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

SF-7

Hoja N° 1 de 1

PREP: R.E.B.P

REV: E.S.M.P

Ejercicio: 2012; Cédula Narrativa de Condiciones de Mobiliario
Area examinada: Seguridad Física
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

El mobiliario con que cuenta la empresa para colocar su equipo informático en las diferentes áreas se encuentra en muy buenas condiciones fisicas.

Datos según observación

ANEXO # 19

CÉDULA NARRATIVA DE ESPACIO FÍSICO DEL ÁREA DE LOCAL DE VENTA

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores. S. A. de C. V.

SF-8/1

Hoja N° 1 de 1
PREP: R.E.B.P
REV: E.S.M.P

Ejercicio: 2012, Cédula narrativa de espacio fisico del área de local de venta
Area examinada: Seguridad fisica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

En cuanto al espacio físico del área del local de venta a través de la visita que se llevó a cabo, se observa que se cuenta con el espacio físico adecuado, lo cual está en buenas condiciones para llevar a cabo las las actividades de la empresa.
se presentan unas fotografias que muestra el espacio físico adecuado.

Datos según observación

ANEXO # 20

CÉDULA NARRATIVA DE RUTAS DE EVACUACIÓN

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

SF-9

Hoja N° 1 de 1

PREP: R.E.B.P

REV:E.S.M.P

Ejercicio: 2012; Cédula Narrativa de Rutas de evacuación.

Area examinada: Seguridad Física

Fecha de inicio de Auditoria: Julio 2012

Fecha de Finalización: Septiembre 2012

Cuando se visito las instalaciones de la Casa Matriz de la empresa se verificó si existen rutas de evacuación en caso de ocurrir una emergencia como puede ser un movimiento telúrico, el señor Auditor Interno nos informó que no se cuenta con salidas emergentes ya que la única que existe es la entrada principal y dicha entrada es por medio de escaleras, además de ello los empleados no cuentan con instrucciones para salir al momento de encontrarse en dicha situación.

Datos según observación

ANEXO # 21

CÉDULA NARRATIVA DE ALARMAS

EMPRESA: TELEFONOS FACILES S.A DE C-V

Grupo Profesional de Auditores, S. A. de C. V.

SF-10

Hoja N° 1 de 1

PREP: R.E.B.P

REV: E.S.M.P

Ejercicio: 2012; Cédula Narrativa de alarmas.

Area examinada: Seguridad Física

Fecha de inicio de Auditoria: Julio 2012

Fecha de Finalización: Septiembre 2012

Con el objetivo de conocer la existencia de alarmas para detección de fuego y agua se procedió a preguntarle al Auditor Interno de la empresa a través de cuestionario de seguridad física si contaban con ello, el cual mencionó que solamente cuentan con alarma contra robo, y haciendo una pequeña prueba pudimos verificar que si es adecuada y que tiene buen funcionamiento.

Datos según observación

ANEXO # 22

CÉDULA DE SUMINISTROS DE ENERGÍA

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

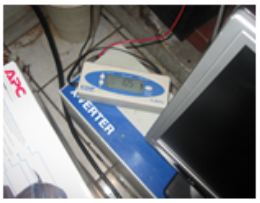
SF-12

Hoja N° 1 de 1

PREP: R.E.B.P.

REV: E.S.M.P.

Ejercicio: 2012; Cédula de Narrativa de Mantenimiento de suministros de energía
Area examinada: Seguridad Física
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012



Según comentó el Jefe del área de Informática el mantenimiento a los suministros de energía lo hace él, con excepción de las 4 baterias que tienen ,ya que no se pueden abrir debido a que estan selladas y se estima que la vida útil es de 1 año, debiendo ser reemplazadas cuando se cumpla ese tiempo.

Los Ups se les da mantenimiento superficial, es decir solo en la parte exterior y éste es realizado por el encargado del aseo en la empresa.

Datos según entrevista

ANEXO # 23

CÉDULA ANALÍTICA DE EXTINTORES

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

SF-13

Hoja N° 1 de 1

PREP: R.E.B.P.

REV: E.S.M.P.

Ejercicio: 2012; Cédula Analítica de extintores
Area examinada: Seguridad Física
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

Referencia	Ubicación del extintor	Descripción	Peso	Fecha que se compró	Ultima fecha de carga	Fecha de Vencimiento	Persona responsable	Proveedor	Observaciones
	Pasillo frente a las oficinas de tesorería en el segundo piso de las instalaciones de la empresa.	Marca Bauger YP-838732. Contenido P 2S ABC	12 libras	-	Marzo de 2012	Marzo de 2013	No hay nadie en especifico que sea responsable de dicho extintor.	Extinsal Extintores de ESA	La empresa solo cuenta con un extintor.

Datos obtenidos de Comprobantes de observación

ANEXO #24

CÉDULA NARRATIVA DE AIRE ACONDICIONADO

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

SF-15

Hoja N° 1 de 1

PREP: R.E.B.P.
REV: E.S.M.P.

Ejercicio: 2012; Cédula Narrativa de Aires acondicionado
Area examinada: Seguridad Física
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

El aire acondicionado Mini split Marca Carrier Alpha ubicado en el área de servidores se encuentra a temperatura de 26 centigrados, permanece encendido durante las 24 horas del día los 365 días del año. Según nos informó el Jefe de Informática dicho aire acondiconado ha sido reparado en una ocación con motivo de recargo de gas. Fué adquirido en diciembre de 2007. La central del aire acondicionado con que cuenta la empresa esta ubicado en oficinas de auditoria 1, segundo nivel de la empresa.

Datos obtenidos de Comprobantes de observación

ANEXO # 25

AREA: SEGURIDAD LOGICA

CÉDULA ANALÍTICA DE INVENTARIO DE PROGRAMAS

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Ejercicio: 2012; Cédula Analítica de Inventario de Programa
Area examinada: Seguridad Lógica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: sSeptiembre 2012

Hoja N° 1 de 1

PREP: O.R.G.H
REV: E.S.M.P

Referencia	Nombre del Programa	Pais de Creación	Versión	Lenguaje de Programación	Fecha de Instalación	Periodicidad de actualización	Cantidad de usuarios	Cantidad de módulos	Observaciones
SLS-1	SISTEMA EXACTUS ERP	Costa Rica SRL 2009	6.0 R2-SP2	VISUAL BASIC	NOVIEMBRE 2007	N/A	48	15 Modúlos	Los módulos instalados no pueden ser usados por todos los usuarios del sistema, para los puntos de ventas sólo se puede acceder a Facturación y Control de Inventario.

Datos según observación

ANEXO # 26

CÉDULA ANALÍTICA DE MÓDULOS DEL SISTEMA

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Hoja N° 1 de 1
PREP: O.R.G.H
REV: E.S.M.P

Ejercicio: 2012 Cédula analítica de Módulos del sistema

Area examinada: Seguridad Lógica

Fecha de inicio de Auditoria: Julio 2012

Fecha de Finalización: Septiembre 2012

Referencia	Nombre del módulo	Función Principal	Versión	Area donde se utilica	Documentos que se generan	A quien se dirige	Contraseña para ingresar al módulo SI/NO	Se tiene Manual de Usuario del Módulo	Privilegios de Usuario en el módulo					Observaciones
									Anular	Añadir	Consultar	Eliminar	Imprimir	
	Control Bancario	Procesamiento de Transferencias Bancarias	6.00.04	Contabilidad, Auditoria,Admón Gral	Reportes de Movimientos Bancarios	Comité Administrativo, Gerencia y Bancos	NO	SI		x	x		x	Los Jefes Líderes de cada
	Contabilidad General	Procesamiento de Información Financiera	6.00.12	Contabilidad, Auditoria	Estados Financieros, Registros Bancarios,Declaraciones	Comité Administrativo, Gerencia y Mins. De Hacienda	NO	SI		x	x	x	x	área son los autorizados
	Cuentas por Cobrar	Procesamiento de Clientes con Cuentas x Cobrar	6.00.02	Contabilidad, Auditoria	Reportes de Cuentas por Cobrar a clientes	Comité Administrativo, Clientes y Gerencia	NO	SI		x	x	x	x	para tener la mayoría de los
	Cuentas por Pagar	Procesamiento de Cuentas por Pagar	6.00.02	Contabilidad, Auditoria, Admón Gral.	Reportes y listado de Cuentas por pagar a proveedores	Comité Administrativo, Proveedores y gerencia	NO	SI		x	x	x	x	privilegios dentro del sistema,
	Recursos Humanos	Información de Recursos Humanos	6.00.03	Auditoria, Administración General	Listado de Recursos Humanos de la empresa	Comité Administrativo, Gerencia y Mins. De Trabajo	NO	SI		x	x	x	x	pero hay casos en los que
	Control de Nóminas	Procesamiento de Planillas	6.00.07	Contabilidad, Auditoria, Admón Gral.	Planillas de pagos de empleados.	Gerencia, AFP, ISSS; DGII, Ministerio de Hacienda	NO	SI	x	x	x	x	x	ni los Jefes tienen acceso
	Activos Fijos	Procesar información sobre Activos de la empresa	6.00.05	Contabilidad, Auditoria,Admón Gral	Inventarios mecanizados de Activos Fijos	Comité Administrativo, Gerencia	NO	SI		x	x	x	x	a realizar éstos roles.
SIS-2	Control de Inventario	Procesar la existencia de inventario y consultas a éste	6.00.09	Contabilidad, Auditoria, Compras, Ptos de Venta	Existencia en bodega, Requisiciones de Inventario	Comité Administrativo, Jefe de Logística	NO	SI			x			Sin embargo, el Jefe de Informática
	Facturación	Procesar ventas, emitir facturas, tickets, y trasladar a Conta.	6.00.08	Ptos de Venta, Contabilidad, Auditoria, Logística	Facturas, Tickets	Consumidores Finales, Clientes	NO	SI	x	x	x	x	x	es el único que tiene acceso
	Presupuesto Financiero	Crea información del presupuesto asignado por área	6.00.01	Logística, Admón Gral, Auditoria	Reportes de Presupuesto Financiero por área.	Comité Administrativo, Jefe de Logística	NO	SI		x	x		x	irrestricto a todos los privilegios
	Compras	Crear formularios e informes de compras	6.00.06	Contabilidad, Logística, Auditoria	Plan de Compras, Reportes de Compras mensuales, etc	Jefe de Logística, Comité Administrativo y Gerencia	NO	SI		x	x		x	ya que por ser él el que da soporte técnico
	Estadísticas de Ventas	Genera de forma gráfica resumenes de ventas y montos.	6.00.01	Logística, Admón Gral, Auditoria	Reporte de Estadística de Venta por Sucursal y Consolidado	Jefe de Logística, Comité Administrativo y Gerencia	NO	SI			x		x	a los programas y módulos, puede
	Pronósticos de Ventas	Crea información relacionada con ventas	6.00.01	Logística, Admón Gral, Auditoria	Reporte de Proyecciones de ventas por sucursales y montos	Jefe de Logística, Comité Administrativo y Gerencia	NO	SI		x	x	x	x	acceder sin previa autorización
	Caja Chica	Procesa informes de caja chica	6.00.00	Contabilidad, Auditoria	Reportes de transacciones de Caja Chica y asignación de ésta	Jefe de Contabilidad, Auditor Interno	NO	SI	x	x	x	x	x	o supervisión.
	Control de Vacación	Crear informes sobre Control de vacaciones	6.00.03	Auditoria, Administración General	Reporte de Control de Vacación por cada empleado.	Jefe de Contabilidad, Auditor Interno	NO	SI		x	x		x	

Datos según comprobación del sistema

ANEXO # 27

CÉDULA ANALÍTICA DE APLICACIONES DE LOS MÓDULOS

EMPRESA: TELEFONOS FACILES S.A DE C.V

Ejercicio: 2012; Cédula analitica de aplicaciones de los módulos
Area examinada: Seguridad Lógica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

Hoja N° 1 de 1
PREP: O.R.G.H
REV: E.S.M.P

Referencia	Nombre de la Aplicación	A que módulo pertenece	Función principal	Proceso de Ejecución			Periodicidad de la Actualización	Privilegios de Usuario					Comentarios
				Rápido	Normal	Lento		Anular	Añadir	Consultar	Eliminar	Imprimir	
	Cálculo de Impuesto	Contabilidad Gral	Cálculo de ISR de los empleados, ISSS y AFP		x		Cada 6 meses			x		x	Sólo se pudo acceder
	Descuentos sobre mercadería	Facturación	Calcular descuentos por cliente frecuente	x			Cada 6 meses			x	x	x	a las aplicaciones que se
SLS-3	Planillas	Control de Nóminas	Elaboracón de Nóminas de empleados		x		Cada 6 meses		x	x	x	x	detallan aquí, las demás
	Estados Financieros	Contabilidad Gral	Elaboración de Estados Financieros de la empresa		x		Cada 6 meses	x	x	x	x	x	aplicaciones no pudieron
	Bodega	Control de Inventario	Consultas de existencia en bodega	x			Cada 6 meses			x		x	ser evaluadas de manera especifica

(S)

Datos según observación

(S) *Datos según corroboración del sistema*

ANEXO # 28

SUB-CÉDULA ANALÍTICA DE LOS MÓDULOS

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Ejercicio: 2012;Sub-Cédula analitica de aplicaciones de los módulos
Area examinada: Seguridad Lógica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

Hoja N° 1 de 1

PREP: O.R.G.H
REV: E.S.M.P

Referencia	Nombre de la Aplicación	Proceso mecanizado	Proceso manual	Proceso de Ejecución			Diferencias	Comentarios
				Rápido	Normal	Lento		
SLS-4	Cálculo de Impuesto (AFP)	$12.98	$12.98	x			$0.00	Se constató que la aplicación de Cálculo de Impuesto en la que se hacen cálculos de AFP, ISSS e ISR, funciona de forma correcta. Sin embargo, sólo se accedió e comprobar el funcionamiento de 2 procesos dentro de la aplicación.
	Cálculo de Impuesto (ISSS)	$6.23	$6.23				$0.00	

(S)

Datos según observación

(S) *Datos según corroboración del sistema*

ANEXO # 29

CÉDULA NARRATIVA DE ADMINISTRACIÓN DE SEGURIDAD

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Hoja N° 1 de 1

Ejercicio: 2012 Cèdula Narrativa de Administración de Seguridad
Area examinada: Seguridad Logica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

PREP:O.R.G.H
REV: E.S.M.P

Referencia:
SLC-1

A través de entrevistas y cuestionarios al Area de Informática se evaluó el esquema de seguridad que se ha establecido para el acceso al sistema y a los datos que se poseen y se determinó que existen políticas para la Administración de la Seguridad , por ejemplo la Asignación de Claves de Acceso al Sistema, dichas claves son asignadas por el Jefe de Informática que también es el Administrador de Red.

Se preguntó si hay un módulo determinado para la asignación de claves de acceso y él Administrador de Red nos comunicó que efectivamente se tiene uno del cual solamente es él el encargado del acceso de dicho módulo.

Los niveles de acceso a los usuarios son establecidos dependiendo del área en la que se encuentren , pero de manera general todos los usuarios deben tener claves de acceso para el equipo y para el sistema en el que trabajen.

El nivel de protección existente sobre las bases de datos de la empresa están bien definidos, ya que no se tuvo acceso a ésta área por protección a la información almacenada en dichas bases y así mantener íntegra y confidencial la información almacenada.

El sistema operativo que se tiene es Windows Server, y el Lenguaje de Programación es Visual Basic.

Se tienen instalados los software ejecurables de los programas y no los software completos.

Datos obtenidos de Comprobantes de observación

ANEXO #30

CÉDULA NARRATIVA DE PASSWORD

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Hoja N° 1 de 1

Ejercicio: 2012 Cèdula Narrativa de Passsword
Area examinada: Seguridad Logica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

PREP: O.R.G.H
REV: E.S.M.P

Referencia:
SLC-3

Se vericó mediante procesos de observación y entrevista al Jefe de Informática que se tienen controles de acceso de seguridad que están conformados por :

Identificación de Usuario (ID)

Las claves de acceso (password)

Mecanismos de Atorización

Estos tres elementos forman parte de los controles que con previa autorización son implementados a cada uno de los usuarios del sistema, además de las especificaciones que se dan sobre los privilegios o roles que desarrolla cada usuario dentro del sistema.

Estas especificaciones las realiza el Jefe de Informática y él es el responsable de la asignación de Identificación de Usuario así como la contraseña respectiva, que posteriormente él usuario la cambia a su conveniencia y cómo se detalla en otras cédulas los intentos válidos para el ingreso de la contraseña son únicamente cinco, si no se digita de manera correcta en ésta cantidad de intentos, el sistema se bloquea y es necesario pedir el desbloqueo al Jefe de Informática que también es el Administrador de red, que da mantenimiento y soporte técnico al sistema.

Datos obtenidos de Comprobantes de observación

ANEXO # 31

CÉDULA ANALÍTICA DE INVENTARIO DE ROUTERS

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Ejercicio: 2012; Cédula Analítica de Inventario de Routers
Area examinada: Seguridad Lógica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización:Septiembre 2012

Hoja N° 1 de 1

PREP:O.R.G.H
REV: E.S.M.P

Referencia	Nombre de Routers	Marca	Modelo	Serie	Ubicación	Comentarios
SLR-20	Router de Servicios Integrados	Cisco	1800	1841	Servidor principal Casa matriz	En la empresa solamente se tiene un Routers, que se encuentra en la Casa matriz, en todas las terminales de las demás sucursales y puntos de venta se encuentran intercomunicadas con switchs

ANEXO # 32

CÉDULA NARRATIVA DE FUNCIONAMIENTO DE FIREWALL

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

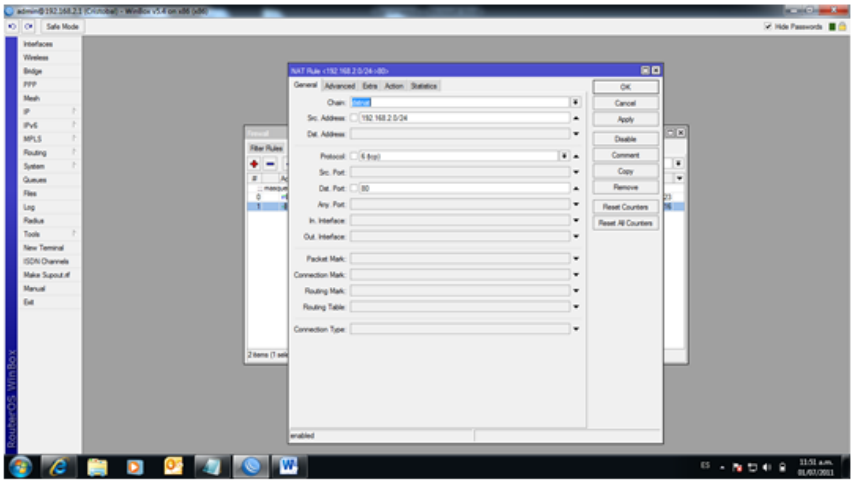
Referencia:
SLF-19

Hoja N° 1 de 1
PREP: O.R.G.H
REV: E.S.M.P

Ejercicio: 2012 Cédula Narrativa de Funcionamiento de Firewall
Area examinada: Seguridad Logica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

Para verificar el funcionamiento de los Firewalls instalados en los diferentes servidores de la empresa se pudo verificar el funcionamiento que éstos tienen para proteger la red y la información que se tiene dentro , en entrevista al Jefe de Informática, se dijo que la red ha tenido 5 intentos de sabotaje pero oportunamente el Firewall ha bloqueado los URL.
Los Firewall sirven para bloquear el acceso a la red de usuarios no autorizados, y que maliciosamemente quieren acceder a las Bases de Datos existentes en la red.

La imagen que se muestra , es una pantalla capturada del Firewall usado por la empresa.



ANEXO # 33

CÉDULA ANALÍTICA DE INVENTARIO DE ANTIVIRUS

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Ejercicio: 2012; Cédula Analítica de Inventario de Antivirus
Area examinada: Seguridad Lógica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización:Septiembre 2012

Hoja N° 1 de 1

PREP: O.R.G.H
REV: E.S.M.P

Referencia	Nombre de Antivirus	Proveedor	Periodicidad de la actualización	Licencia	Equipos instalados	Comentarios
SLA-21	Windows Security Essentials	Microsoft Corporation	Cada año	Si	48	El antivirus que poseen se actualiza automáticamente en cada sesión en internet, pero la actualización de todo el software de antivirus se actualiza cada año.

ANEXO # 34

CÉDULA NARRATIVA DE FORMULARIOS O MANUALES DE FUNCIONAMIENTO

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

Referencia:
D-1

Hoja N° 1 de 1

PREP: O.R.G.H
REV: E.S.M.P

Ejercicio: 2012 Cédula narrativa de Formularios
Area examinada: Seguridad Logica
Fecha de inicio de Auditoria: Julio 2012
Fecha de Finalización: Septiembre 2012

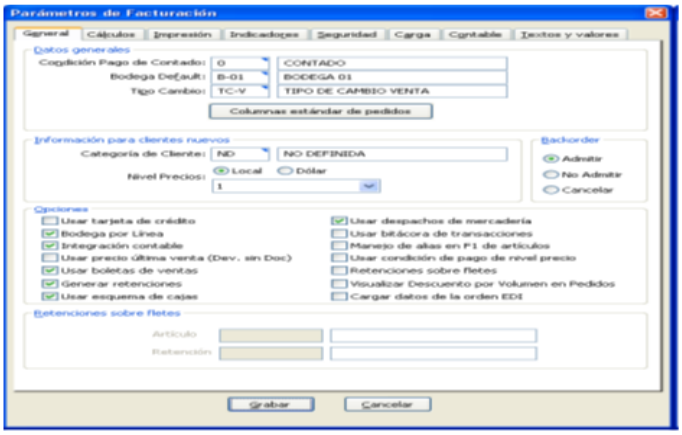
En ésta área no pudo ser examinada debido a que no se conto con el tiempo suficiente para hacer un estudio pormenorizado y completo a cerca de todos los documentos o manuales usados.

En el desarrollo de los procedimientos se pretendia:
Verificar que los empleados sepan de la existencia de dichos manuales.
Hacer cedula narrativa de los diferentes tipos manuales, tomando como muestra el manual de usuario del sistema.

Elaborar una cédula analítica de documentos donde , se evaluaría:

Nombre del manual, Fecha de elaboración, Elaborado por,Revisado por, Se ha modificado desde su creación , Se entrega copia a usuario,Donde se resguarda, Capacitaciones sobre uso del manual.
Mediante muestreo verificaríamos si utilizan el manual de usuarios.

Solamente pudimos evaluar el Manual de Instalación del Módulo de Facturación, en el cual indica como realizar accciones dentro de dicho módulo, como corregir, como adaptarlo, como darle mantenimiento, etc.
Así como el funcionamiento de los parámetros que hay en facturación:



El manual de funcionamiento del Módulo de instalación, muestra todas las pantallas sobre los parámetros con los que cuenta el módulo, así como su funcionamiento.

ANEXO # 35

Grupo Profesional de Auditores, S. A. de C. V.

ÍNDICE DE REFERENCIA A LOS PROGRAMAS

Ejercicio: 2012; Índice de Programas de Auditoria de Sistemas

Empresa: Teléfonos Fáciles, S.A. DE C.V.

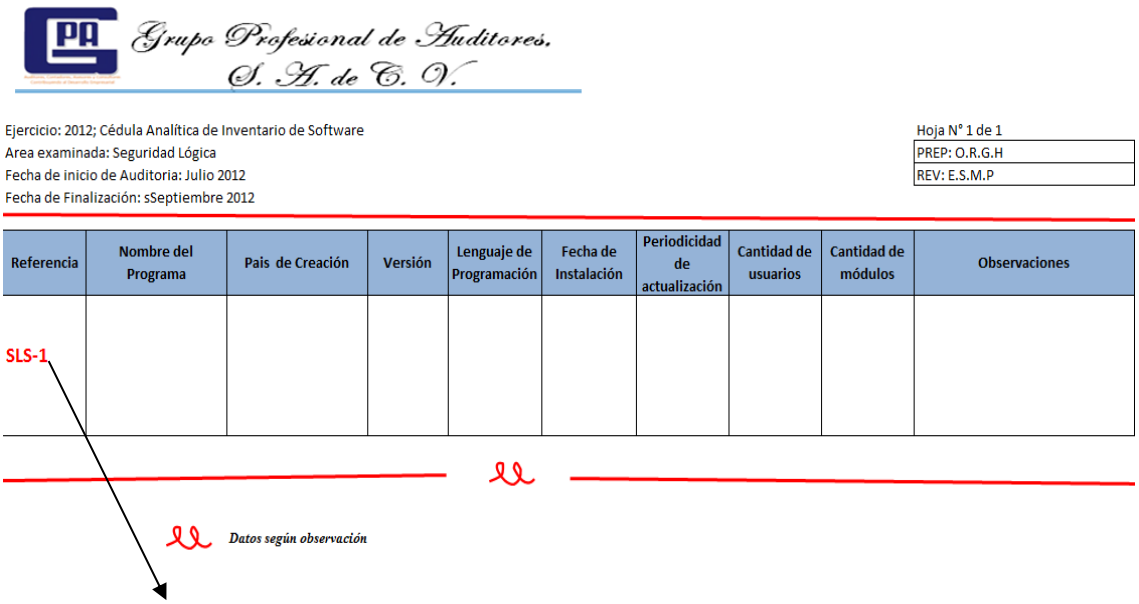
Fecha Inicio de Revisión: Julio 2012

Fecha de Finalización de Revisión: Septiembre 2012

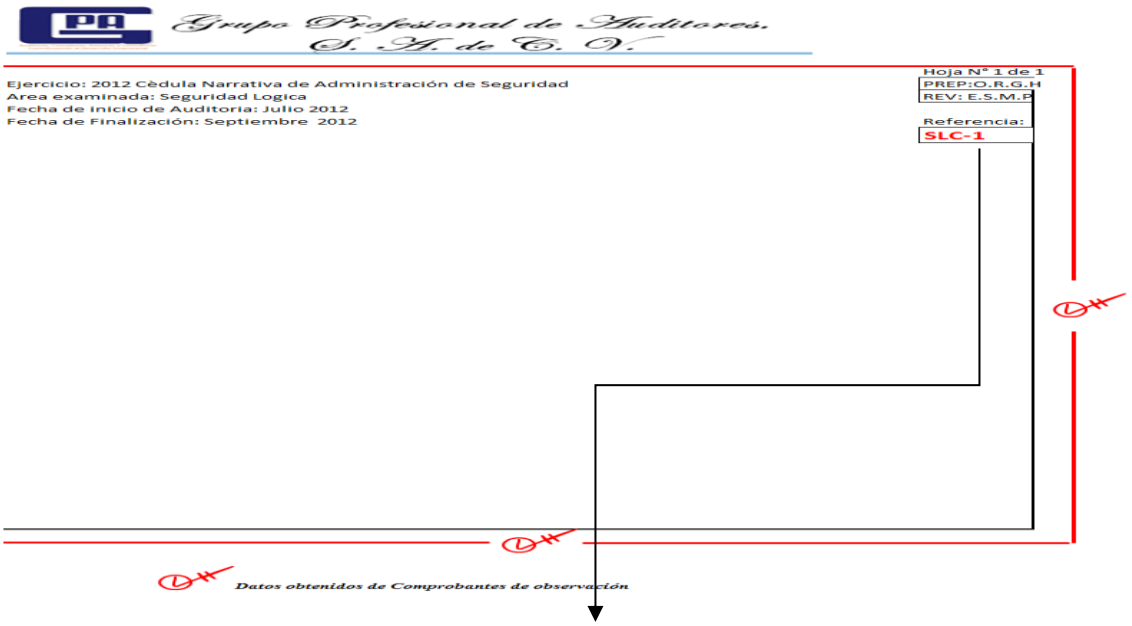
ANEXO # 36

REFERENCIACIÓN DE PAPELES DE TRABAJO

EMPRESA: TELEFONOS FACILES S.A DE C.V



Papel de trabajo al cual se hace la referencia



Papel del trabajo del cual viene la referencia

ANEXO #37

CÉDULA DE MARCAS DE AUDITORÍA DE SISTEMAS

EMPRESA: TELEFONOS FACILES S.A DE C.V

Grupo Profesional de Auditores, S. A. de C. V.

MS

Ejercicio: *2012; Cedula de Marcas de Auditoría de Sistemas*
Empresa: *Teléfonos Fáciles S.A de C.V*
Fecha Inicio de Revisión: *Julio 2012*
Fecha de Finalización de Revisión: *Septiembre 2012*

Hoja No 1 de 1

PREP: R.E.B.P
REV: E.S.M.P

Datos obtenidos de Comprobantes de observación

Datos según cuestionario de Control Interno

Cotejado con manuales

Datos según entrevista

Según confirmaciones

Datos según observación

S ***Datos según corroboración del sistema***

I ***Datos según recuento físico***

ANEXO # 38

Grupo Profesional de Auditores, S. A. de C. V.

ARCHIVO ADMINISTRATIVO

FIRMA DE AUDITORIA: GRUPO PROFESIONAL DE AUDITORES S.A DE C.V

DIRECCION: Calle Luis XVI, Pol. A-2, #7, Ciudad Real, San Miguel **TELEFONO:** 2261-0001

NOMBRE DEL CLIENTE: TELÉFONOS FÁCILES, S. A. DE C. V.

DIRECCION: Barrio El Calvario, #6, San Miguel. **TELEFONO:** 2661-0505

PERIODO AUDITADO: Julio- Septiembre 2012

CONTENIDO **ÍNDICE**

Personal que llevará a cabo la Auditoría de Sistemas:

Rocío Elizabeth Bolaines Portillo
(Auxiliar de Auditoría 1)

Oscar René Gómez Hernández
(Auxiliar de Auditoría 2)

Ernesto Scarlett Martínez Páiz
(Supervisor de Auditoría)

A A

ANEXO # 39

Grupo Profesional de Auditores, S. A. de C. V.

ARCHIVO PERMANENTE

NOMBRE DEL CLIENTE: Teléfonos Fáciles, S. A. de C. V.

DIRECCION: Barrio El Calvario, #6, San Miguel. **TELEFONO:** 2661-0505

PERIODO AUDITADO: Julio- Septiembre 2012

NOMBRE, TITULO Y CARGO DEL PERSONAL DEL CLIENTE CON QUIEN COMUNICARSE: Ing. Carlos Alberto Huezo, Jefe de Informática y Administrador de Red.

Lic. Héctor Suárez, Auditor Interno.

SISTEMA DE AUDITORIA APLICADO: Estándar

CONTENIDO	ÍNDICE		
Escritura de Constitución	☐	**Licencias de Antivirus**	☐
NIT de la Empresa	☐	**Contratos de Internet**	☐
Mision y Vision de la empresa	☐	**Contratos de Mantenimiento**	☐
NRC de la Empresa	☐	**Políticas de Seguridad**	☐
Estructura Organizativa	☐	**Políticas de Programación**	☐
Antecedentes de la Empresa	☐	**Diagrama de Redes**	☐
Antecedentes del Centro de Cómputo.	☐	**Plan de Contingencia**	☐
		Leyes Aplicables	☐
Organigrama del Centro de Cómputo.	☐	**Principales formularios automatizados**	☐
Manuales del Sistema	☐		
Manuales de Usuario	☐		
Copias de licencias de Programas	☐		

A P

ANEXO # 40

Grupo Profesional de Auditores, S. A. de C. V.

ARCHIVO CORRIENTE

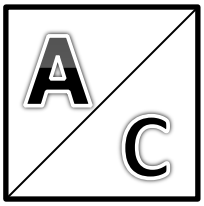
NOMBRE DE LA EMPRESA: TELÉFONOS FÁCILES S.A DE C.V

PERIODO AUDITADO: JULIO-SEPTIEMBRE DE 2012

NOMBRE DEL AUDITOR: GRUPO PROFESIONAL DE AUDITORES S.A DE C.V

AREA: AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDO	ÍNDICE
Carta a la Gerencia	☐
Informe de Auditoría	☐
Cédula de hallazgos	☐
Cédula de Marcas	☐
Areas Críticas	☐
Entrevistas	☐
Cuestionarios de Seguridad Física	☐
Cuestionario de Seguridad Lógica	☐
Lista de Chequeo	☐
Matriz de Riesgo	☐
Programas de Auditoría	☐
Papeles de Trabajo de Seguridad Física	☐
Papeles de Trabajo de Seguridad Lógica	☐
Diagramas de Red	☐
Evaluación del Plan de Contingencia	☐
Fotografías	☐



ANEXO # 41

Grupo Profesional de Auditores, S. A. de C. V.

INFORME FINAL DE AUDITORIA DE SEGURIDAD INFORMATICA DE LA EMPRESA: "TELEFONOS FACILES S.A. DE C.V."

Preparado por:

*"**GRUPO PROFESIONAL DE AUDITORES S.A. DE C.V."***

Dirigido a:

"TELEFONOS FACILES S.A. DE C.V."

Fecha de emisión

30 DE SEPTIEMBRE DE 2012

I. INTRODUCCIÓN

En cumplimiento a nuestro contrato de servicios para el año 2012 con la empresa "TELEFONOS FACILES S.A. DE C.V.", se realizó auditoria a la Seguridad Informática en la cual se evaluó el la Seguridad Física y la Seguridad Lógica de la empresa, en cuanto a los sistemas informáticos, instalaciones, equipos, entre otros; dicha auditoria fue realizada durante el período de __JULIO_____ a _SEPTIEMBRE_____ de 2012.

II. OBJETIVOS

- **GENERAL**

Emitir un informe sobre la Evaluación de la Seguridad Informática de los sistemas de información computarizados (SIC), para asegurar el correcto funcionamiento de las medidas de Seguridad Física implementadas y el cumplimiento, la integridad, confiabilidad, y confidencialidad de los sistemas, a través de las medidas de Seguridad Lógica.

- **ESPECIFICOS**

1. Verificar las medidas de Seguridad Física en la empresa.
2. Comprobar los controles establecidos de Seguridad Informática.
3. Comprobar la existencia de planes contingenciales que permitan seguir operando en casos de fallas o algún tipo de siniestros.
4. Verificar la existencia de controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.
5. Evaluar las condiciones del local en que se encuentra la empresa.

6. Verificar la ubicación de los servidores y las medidas de seguridad que tienen para ello.
7. Determinar el estado físico del mobiliario en el que se tienen los equipos informáticos.
8. Evaluar las condiciones ambientales bajo las que se encuentran los equipos informáticos.
9. Evaluar la idoneidad del recurso humano del área de informática.

III. ALCANCE DE AUDITORIA.

1. SEGURIDAD FÍSICA

- Se realizaron los inventarios correspondientes de los equipos y del mobiliario que utiliza la empresa.

- Se evaluó los controles de seguridad física con los que cuenta la empresa, como lo es rutas de evacuación para el personal en caso de ser necesario salir de las instalaciones; las áreas que están restringidas en la empresa.

- Se observó las condiciones físicas del local en donde se encuentra ubicada la empresa, al mismo tiempo las condiciones del mobiliario en el que se tiene el equipo informático.

- Se verificó la temperatura del aire acondicionado que se tiene en el área de servidores.

- Se evaluó las condiciones físicas del local de un punto de venta elegido como muestra.

2. **SEGURIDAD LÓGICA**

- Se realizaron inventarios de los programas y módulos instalados en el sistema.

- Se evaluaron los controles de seguridad lógica de la empresa, en los cuales se verificó las claves de acceso, origen de datos, entrada de datos, procesamiento de datos y salida de información.

- Se evaluó la creación de las contraseñas del sistema, los diferentes usuarios y la seguridad en cuanto a la protección de éstas.

- Verificación del programa **EXACTUS** y módulos dentro del sistema y las aplicaciones que se pueden realizar dentro de éste.

- Se realizó el inventario de Firewall existentes en los diferentes servidores de la empresa.

- Se verificó el funcionamiento de los firewall, y la efectividad de éstos para bloquear las amenazas a la red.

- Se evaluó la existencia de Back Ups en la empresa, su almacenamiento y la respectiva restauración de éstos.

IV. RESULTADOS

Producto de la aplicación de procedimientos de auditoria en las áreas de seguridad física, y seguridad lógica obtuvimos el resultado siguiente:

AREA: SEGURIDAD FÍSICA

HALLAZGO DE AUDITORIA № 1

NO TIENEN ALARMAS PARA DETECCIÓN DE FUEGO Y AGUA

CONDICIÓN:

Con el objetivo de conocer la existencia de alarmas para detección de fuego y agua se procedió a preguntarle al Auditor Interno de la empresa a través de cuestionario de seguridad física si contaban con ello, el cual mencionó que solamente cuentan con alarma contra robo.

CAUSA:

- Falta de gestión por parte del Comité Administrativo para la adquisición de alarmas para detección de fuego y agua.

EFECTOS:

- Filtro de agua
- Inundaciones
- Destrucción de Activos
- No percatarse de algún incendio para ser erradicado a tiempo.
- No detectar la humedad que pueda afectar a los equipos informáticos de la empresa.

RECOMENDACIÓN:

- Al Comité Administrativo se le recomienda que gestione a la Gerencia de la empresa la adquisición e instalación de alarmas para detección de fuego y humedad en las áreas claves de la empresa como por ejemplo en el área de servidores.

HALLAZGO DE AUDITORIA № 2
FALTA DE SIMULACROS Y RUTAS DE EVACUACIÓN

CONDICIÓN:

Para verificar las rutas de evacuación que existe en la empresa en caso de ocurrir una emergencia como puede ser un movimiento telúrico, se nos informó que no se cuenta con salidas emergentes ya que la única que existe es la entrada principal y dicha entrada es por medio de escaleras, además de ello los empleados no cuentan con instrucciones para salir al momento de encontrarse en dicha situación.

CAUSA:

- Falta de instrucción a los empleados.
- Falta de simulacros.
- No existe un comité de prevención de accidentes y desastres que oriente sobre la importancia de crear rutas de evacuación en la empresa.

EFECTOS:

- Al momento de ocurrir un movimiento telúrico puede ocasionarse disturbios al momento de evacuación, lo que puede conllevar a caídas y golpes entre los empleados de la empresa.

RECOMENDACIONES:

- A la gerencia de la empresa se le recomienda que:
  - Se cree un comité de prevención de accidentes y desastres.
  - Se instruya al personal de la empresa en caso que sea necesario abandonar las instalaciones por una emergencia.
  - Se realicen simulacros de evacuación de las instalaciones de la empresa por lo menos una vez al año.

HALLAZGO DE AUDITORIA № 3
UN SOLO EXTINTOR EN LA EMPRESA

CONDICIÓN:

Para verificar el área donde se encuentran los Extintores de la empresa se realizó la inspección correspondiente y se pudo determinar que la empresa solo cuenta con un extintor para todas las áreas. Dicho extintor está ubicado en el segundo piso de la empresa, en un pasillo entre el área de tesorería y pagaduría lo que ocasiona que en caso de una emergencia no todos los departamentos tendrían acceso a dicho extintor.

CAUSA:

- Existencia de un solo extintor.
- Falta de un comité de prevención que indique la importancia de tener extintores en la empresa.

EFECTOS:

- Que no se pueda cubrir con un solo extintor el origen de un incendio en la empresa.
- Que al ocurrir un siniestro en cualquier otro departamento el extintor no esté al alcance de la persona que lo necesite.

RECOMENDACIONES:

- Se recomienda al Comité Administrativo que realicen capacitaciones dirigidas a los empleados en cuánto al uso del extintor.
- Se recomienda al Comité Administrativo que se adquieran más extintores, por lo menos que haya uno por cada departamento.

- A la Gerencia que se apruebe la realización de simulacros para hacer uso del extintor.

HALLAZGO DE AUDITORIA № 4

MALA UBICACIÓN DE CAJA TERMICA DE ENERGIA

CONDICIÓN:

Se visitó uno de los puntos de venta de la empresa, el cual fue tomado como muestra, se realizó la inspección correspondiente y se determinó que la caja térmica de energía está ubicada en un lugar no adecuado ya que se encuentra al libre acceso de cualquier persona que ingrese a la tienda debido a que está a una altura de un metro y medio de donde están las sillas de atención al cliente.

CAUSA:

- No se tiene un lugar adecuado donde se ubique la caja térmica de energía.
- El edificio es arrendado

EFECTOS:

- Daños por manipulación de la caja térmica por alguna persona.
- Ocurrencia de apagones de energía que pueda causar daños al equipo, o pérdida de información que se esté generando en ese momento.

RECOMENDACIONES:

- Se le recomienda al Comité Administrativo, evalué la reubicación de la caja térmica de energía.

- A la Gerencia, que la caja térmica de energía se pueda instalar en un lugar donde solo personal autorizado de la empresa tenga acceso a ella.

AREA: SEGURIDAD LÓGICA

HALLAZGO DE AUDITORIA № 5
EXCESO DE PRIVILEGIOS DEL JEFE DE INFORMATICA

CONDICIÓN:

A través de entrevista y cuestionarios realizados al Jefe de Informática y al Auditor Interno se pudo constatar que el Jefe de Informática tiene demasiados privilegios dentro del sistema EXACTUS, ya que él es el único que tiene acceso a realizar todos los roles, es decir, Agregar, Anular, Modificar, Consultar y Eliminar información inclusive en Módulos de Control Bancario.

CAUSA:

- Exceso de Confianza por parte de la Gerencia.
- Perfil del Jefe de Informática.

EFECTOS:

- En caso de inconformidad por parte del Jefe de Informática con la empresa, él puede realizar alguna acción que afecte o distorsione la información del sistema.

RECOMENDACIONES:

- A la Gerencia, que supervise los procesos y privilegios realizados por el Jefe de Informática.
- A la Gerencia, que realice un Contrato de Confidencialidad con el Jefe de Informática, para protegerse de cualquier acción malintencionada que éste pueda realizar.

HALLAZGO DE AUDITORIA № 6
INEXISTENCIA DE PLAN DE CONTINGENCIA

CONDICIÓN:

A fin de evaluar la salvaguarda de los sistemas dentro de la empresa, se procedió a verificar la existencia de un Plan de Contingencia que permita operar en forma normal en casos de cualquier irregularidad y se determinó que tal Plan no existe.

CAUSA:

- No existe una Política donde se estipule la creación de un Plan de Contingencia.

- Falta de gestión del Comité Administrativo para incluir en su Plan de Trabajo la creación de un Plan de Contingencias.

EFECTOS:

- Mala imagen de la empresa con los Clientes

- La no continuidad de la empresa.

RECOMENDACIONES:

- Al Comité Administrativo, que elabore un borrador de Plan de Contingencia para ser revisado y aprobado.
- Al Comité Administrativo que se incluya dentro de las políticas la creación de un Plan de Contingencia.
- A la Gerencia, que se implemente el Plan de Contingencias

HALLAZGO DE AUDITORIA № 7
DEPENDENCIA DE LA ADMINISTRACION A LOS PROCESOS REALIZADOS POR EL JEFE DE INFORMATICA

CONDICIÓN:

A través de entrevistas y cuestionarios aplicados al personal de la empresa, se determinó que la mayoría de procesos relacionados con el óptimo funcionamiento de los sistemas de información, dependen del jefe de informática.

CAUSAS:

- No existe una política de segregación de funciones.
- Se centralizan las funciones solo en el jefe de informática.
- No existe oportunidades de especialización para los otros dos empleados que forman parte del área de informática.

EFECTOS:

- Incapacidad para la resolución de problemas en el funcionamiento de los sistemas de información.
- Atrasos en los procesos debido al no tratamiento oportuno de los problemas.
- Inconformidad de los usuarios de los sistemas con respecto a los tiempos de respuesta en la resolución de problemas relacionados con el sistema.

RECOMENDACIONES:

- El Gerente General debe proponer la apertura de nuevos puestos para el área de informática, de forma que se tengan alternativas para la resolución de todos los problemas inherentes a los sistemas de información.
- La gerencia debe proponer, aprobar y aplicar una política para una mayor segregación de las funciones propias del área de informática.

- El jefe de informática debe capacitar a los otros dos miembros del área a fin de que tengan los conocimientos para resolver los problemas que actualmente él está tratando.

HALLAZGO DE AUDITORIA № 8
ILIMITADO TIEMPO DE PERMANENCIA EN EL SISTEMA

CONDICIÓN:

Para efectos de evaluar y verificar el adecuado funcionamiento del Sistema EXACTUS, se evaluaron los periodos de permanencia del usuario dentro del sistema y se determinó que los periodos de acceso son ilimitados, aun en lapsos de tiempo no utilizado.

CAUSA:

- No existen políticas de restricción para bloqueos del sistema en periodos de tiempo en los que no es utilizado.

EFECTOS:

- Probabilidades de rastreo y manipulación de la información por parte de otros usuarios debido al fácil acceso.

RECOMENDACIONES:

- Al Comité administrativo, que se le den indicaciones al Jefe de Informática sobre la implementación de tiempos de permanencia máximos dentro del sistema; ya que así no se verá expuesta la información que se está procesando a otros usuarios.

HALLAZGO N° 9
FALTA DE ACTUALIZACIÓN DE CONTRASEÑA.

CONDICIÓN:
Al verificar el sistema EXACTUS se pudo observar que las contraseñas de los usuarios no son renovadas, es decir, no son actualizadas periódicamente en el programa y el equipo.

CAUSA:

- Falta de políticas que regule la actualización de contraseña.

- Falta de supervisión por parte del jefe de cada uno de los departamentos que existen en la empresa donde correspondan los usuarios.

EFECTOS:

- Vulnerabilidad de la información.

RECOMENDACIONES:

- Al Comité Administrativo, crear una política de actualización de contraseña en periodos cortos, para que la información este bien protegida.

- Al Jefe de Informática que programe dentro del sistema una aplicación de recordatorio para actualizar periódicamente la contraseña.

HALLAZGO DE AUDITORIA № 10

EL SISTEMA OPERATIVO PARA LA RED POSEE PROBLEMAS DE SOPORTE POR EL PROVEEDOR MICROSOFT.

CONDICIÓN:

La versión del Software utilizado para operar el sistema son las versiones Windows Server Unit 7 2003, Windows XP 2003, los cuales el proveedor ya no podrá dar Soporte técnico, ya que ésta versión ya no será producida por la compañía Microsoft.

CAUSAS:

- Desactualización en las versiones de los sistemas operativos.
- El proveedor no posee el soporte de la versión de Windows 2003.
- Falta de políticas en cuanto al uso de Dispositivos de Almacenamiento de los usuarios del sistema, que pueden ser potenciales amenaza para filtrar un virus al sistema.
- Exceso de confianza por el Firewall Mikrotik versión 5.4, (corta fuego) instalado al servidor de la RED para detectar las amenazas de ataque al sistema Operativo.

EFECTOS:

- Ataques o hacker al sistema por virus informáticos

- Se tienen que utilizar más medios de Almacenamiento de respaldo debido a que se deben de formatear con frecuencia las Maquinas.

- Pérdida de Información por posibles fugas, o ataques filtrados a la RED.

- Mayor vulnerabilidad en el sistema, debido a que las versiones antiguas son más frágiles para que se puedan ocasionar daños por defraudadores de sistemas.

RECOMENDACIONES:

Al Jefe de informática:

- Mantener un monitoreo constantemente para verificar los problemas ocasionados en la Red, para evitar robos o filtraciones en la Información.

- Instalar en las maquinas los mejores antivirus para detectar y eliminar las posibles amenazas de virus en la RED.

- Mantener constantemente en actualización los Firewalls, para evitar sabotajes al sistema.

- Al Comité Administrativo, que se presupueste la adquisición de nuevos programas de las versiones más recientes para estar en contacto con el proveedor para el soporte técnico de éstos.

F._____

Licda. Teresa Barahona

Representante Legal

"GRUPO PROFESIONAL DE AUDITORES S.A DE C.V"

ANEXO # 42

CARTA A LA GERENCIA

San Miguel, 30 de Septiembre de 2012.

"Teléfonos Fáciles S.A de C.V"

Comité Administrativo

PRESENTE.

Respetables señores:

Por este medio hacemos de su conocimiento, deficiencias menores que fueron detectadas en la evaluación de la Seguridad Física y Lógica dentro de la Auditoria de Sistemas, las cuales por su naturaleza, frecuencia y materialidad no se reportaran como hallazgo en el informe final de esta.

A continuación detallamos las deficiencias detectadas y sus respectivas recomendaciones:

A) SEGURIDAD FISICA.

- Al visitar las instalaciones de la empresa se pudo observar que no está prohibido el ingreso de alimentos y bebidas al personal de la empresa al lugar en donde se encuentra el equipo informático que utilizan para realizar su trabajo.

  Recomendación: La gerencia de la empresa debe establecer políticas que prohíban el ingreso de alimentos y bebidas al lugar donde se encuentra

ubicado el equipo informático, ya que esto puede generar daños en menor y mayor grado.

- Se determino a través de cuestionario y entrevista, que los empleados de la empresa no saben como utilizar los extintores de fuego, debido a que no se les han impartido capacitaciones para su utilización en situaciones de emergencia.

  Recomendación: El comité administrativo debe gestionar que el cuerpo de bomberos de San Miguel imparta una capacitación sobre la utilización de extintores en situaciones de emergencia.

- En recorrido por las instalaciones de la empresa, se pudo constatar de que no cuentan con plantas generadoras de energía, ocasionando lo anterior altas posibilidades de interrupción de labores en aquellas situaciones de cortes prolongados de la energía eléctrica.

  Recomendación: El comité administrativo debe gestionar la adquisición de plantas generadoras de energía para que sean ubicadas en las instalaciones de la empresa.

- A través de un recorrido por las instalaciones de la empresa, se pudo comprobar que no hay señalización de las rutas de evacuación que permita la salida rápida, ordenada y segura del personal en escenarios como incendios, terremotos, etc.

  Recomendación: El comité administrativo debe seleccionar a un grupo determinado de personas para que conformen un subcomité de salvaguarda y

seguridad social en cuyas atribuciones estará la identificación y rotulación de las rutas de evacuación de la empresa.

- A través de observación al sistema de cableado, se encontró que los cables no están polarizados en su totalidad.

  Recomendación: La gerencia debe gestionar una revisión general al sistema actual de cableado a fin de solucionar aquellos problemas que podrían ocasionar cortocircuitos e incendios.

B) SEGURIDAD LOGICA.

- Al realizar entrevista al Jefe de Informática se pudo constatar que el mantenimiento de la RED interna se realiza cada 4 meses y cuando se reportan problemas de falla, que demanden el mantenimiento correctivo.

  Recomendación: Al Jefe informático programar con mayor frecuencia monitoreo a la Red, para dar el mantenimiento preventivo y correctivo para un buen funcionamiento y seguridad de la Red Informática.

- Al realizar entrevista al informático para detectar problemas en la Red, se determinó que los problemas que ocasionan con mayor frecuencia la caída de la RED son: la descarga de programas con gran capacidad, él envió de correo en cadena de notas por los usuarios en Fechas de Felicitaciones o de Divulgación de Información, y fallas en el servidor del proveedor externo (CLARO).

  Recomendación: Al Jefe de Informática establecer políticas de seguridad y supervisar a los usuarios de la Red, para que no se den este tipo de aplicaciones de la Red en masa que ocasionan disturbios en el ancho de

banda, y consecuentemente caídas en la Red, así gestionar el pronto restablecimiento en cuanto a la Red externa.

- Al realizar entrevista al informático para el establecimiento y asignación de claves de acceso al sistema (Password), se detectó que las contraseñas se cambian en el momento en que se ha creado la cuenta de un nuevo usuario, y en casos de extravió u olvido de las mismas, manteniendo estas contraseñas sin tiempo definido, siendo habilitadas para los usuario, aun cuando no se encuentre en la empresa, porque solo se reasignan al nuevo usuario.

  Recomendación: Al Jefe de Informática establecer las Políticas de seguridad a las claves de acceso que designen al encargado de Informática cambiar las Password, en periodos cortos de tiempo, o por lo menos una vez al mes, para así evitar que otros personas por disgustos con la empresa puedan tener acceso al sistema y sabotear la Información, ya que con el cambio de contraseñas de estaría evitando que usuarios (pasados), que ya están fuera de la empresa puedan, apropiarse a través de esta deficiencia y poder infiltrarse al sistema.

Para desvanecer las debilidades señaladas anteriormente, será necesario que presente la evidencia suficiente para demostrar que han cumplido con las recomendaciones; todo en pro de mejorar la eficiencia, eficacia, transparencia y seguridad que se debe tener en cuanto al manejo de la información que se genere internamente a través de los sistemas.

Atentamente

F._____

Licda. Teresa Barahona
Representante Legal
"GRUPO PROFESIONAL DE AUDITORES S.A DE C.V"

ANEXO # 43

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA ORIENTAL

DEPARTAMENTO CIENCIAS ECONÓMICAS

SECCIÓN DE CONTADURÍA PÚBLICA.

Respetables Gerentes, Auditores Internos e Informáticos solicitamos su colaboración en el llenado del presente cuestionario, el cual se utilizará con fines académicos en la elaboración del trabajo de graduación denominado "Propuesta de una guía de evaluación de Seguridad Informática a las Empresas Distribuidoras de Telefonía Móvil de la ciudad de San Miguel"

Objetivo: Conocer la existencia de Seguridad Informática en las Empresas Distribuidoras de Telefonía Celular de la Ciudad de San Miguel y la importancia de contar con una guía que facilite la Evaluación de dicha Seguridad.

Indicación: Marque con una "X" el cargo que desempeña, y de igual forma en la respuesta o respuestas que considere correctas.

Gerente ☐ ☐ **Auditor** ☐ **Informático**

1. ¿Cuenta con Seguridad Informática en su Empresa?
   SI ☐ NO ☐

2. Si su respuesta es afirmativa, ¿Tiene un Manual por escrito de dicha Seguridad?
   SI ☐ NO ☐

3. El Servicio Informático de la Empresa es proporcionado por:
   Centro de Cómputo ☐ Proveedor Externo ☐

4. Los Programas utilizados en el Sistema, son creados:
   Externamente ☐ Internamente ☐

5. Cuenta con el siguiente Personal Informático en la Empresa:
   Lic. En Computación ☐ Ing. En Sistemas ☐ Técnico ☐ Otros ☐

6. ¿Conoce si existen medidas de Seguridad Física en su empresa?
   SI ☐ NO ☐

7. ¿Conoce las medidas de Seguridad Lógica?
   SI ☐ NO ☐

8. ¿Existen las siguientes condiciones en el Centro de Cómputo?
   Aire acondicionado ☐ Cableado ☐ Extintores ☐ Suministros de ☐ Energía

   Sensores de Agua ☐ Detectores de Humo ☐

9. ¿El edificio de la Empresa, está protegido contra los siguientes siniestros?
   Robo ☐ Incendios ☐ Desastres naturales ☐

10. ¿Tiene conocimientos sobre los Riesgos Informáticos?
    SI ☐ NO ☐

11. ¿Han sufrido pérdidas ocasionas por los siguientes factores?
    Fraude Informático ☐ Sabotaje ☐ Fallas ☐ Virus ☐ Otros ☐

12. ¿Qué tipo de comunicación utilizan?
    Internet ☐ Intranet ☐ Correo Electrónico ☐ Correo Institucional ☐

13. ¿Las Licencias de los Programas están legalizadas?
    SI ☐ NO ☐

14. ¿Las claves de acceso al sistema tienen periodicidad limitada?
    SI ☐ NO ☐

15. ¿Con qué periodicidad se les cae el Sistema?
    Diario ☐ Semanal ☐ Quincenal ☐ Mensual ☐ Nunca ☐

16. ¿Cada cuánto tiempo se realizan los respaldos o back ups?
    Diario ☐ Semanal ☐ Quincenal ☐ Mensual ☐

17. ¿Cuenta con un Plan de Contingencia?
    SI ☐ NO ☐

18. ¿Se le ha efectuado Auditoría de Sistemas a la Empresa?
    SI ☐ NO ☐

19. Si la respuesta anterior es afirmativa. ¿Conoce el proceso de Auditoría de Sistemas para la evaluación de la Seguridad Física y Lógica?
    SI ☐ NO ☐

20. ¿Le gustaría contar con una guía para evaluar la Seguridad Física y Seguridad Lógica?
    SI ☐ ☐ NO

ANEXO # 44

GLOSARIO

ANTIVIRUS:

En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos.

AUDITORIA DE SISTEMAS:

Es 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.

AUDITORIA DE SEGURIDAD FISICA:

Es el análisis de la adecuación de las instalaciones, salvaguarda ante un posible fuego o inundaciones, acceso físico al hardware, pólizas de seguro, etc.

Se evalúan las protecciones físicas de datos, programas instalaciones, equipos redes y soportes, y por supuesto habrá que considerar a las personas, que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector.

AUDITORIA DE SEGURIDAD INFORMATICA:

Analiza los procesos relacionados únicamente con la seguridad, ésta puede ser física, lógica y locativa pero siempre orientada a la protección de la información.

AUDITORIA DE SEGURIDAD LOGICA:

La auditoría de la seguridad lógica pretende la salvaguarda en dos aspectos: la acreditación de los usuarios y el secreto de archivos y transacciones.

Es necesario verificar que cada usuario solo pude acceder a los recursos que se le autorice el propietario, aunque sea de forma genérica, según su función, y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución, traslado a los sistemas lo que representaríamos en una matriz de accesos.

AUTENTICIDAD:

La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

BACK UP:

El **Backup** de archivos permite tener disponible e íntegra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

BASE DE DATOS:

Una base de datos o banco de datos (en ocasiones abreviada con la sigla *BD* o con la abreviatura *b. d.*) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

BIOMETRIA INFORMATICA:

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

CONFIDENCIALIDAD:

Es la que garantiza que la información está accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.

CRIPTOGRAFIA:

La criptografía es la ciencia que se ocupa del cifrado de mensajes en clave y del desarrollo de sistemas de encriptación. De ella se desprende el análisis criptográfico, encargado del descifrado de mensajes en clave.

DELITOS INFORMATICOS:

Toda acción (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.

DISPONIBILIDAD:

El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos y garantiza el correcto funcionamiento de los sistemas de información.

EVALUACION DE SEGURIDAD:

Es el proceso en la auditoría de sistemas que pretende verificar el cumplimiento de los siguientes aspectos: control de datos, políticas de respaldo, políticas y procedimientos, políticas de revisión de bitácoras, control de las licencias de software, control de medios de almacenamiento masivo, control del mantenimiento y evaluación de la configuración del sistema de cómputo. Además de elementos como protección física, aire acondicionado, suministros de energía, detectores de agua y humo, cableado polarizado, extintores, rutas de acceso, manuales, mantenimiento, alarmas contra robos, contra incendios, inundaciones, etc.

EVIDENCIA COMPETENTE DE AUDITORIA:

Es aquella información de calidad en relación a su relevancia y confiabilidad y suficiente en términos de cantidad, al tener en cuenta los factores como: posibilidad de información errónea, importancia y costo de la evidencia.

EVIDENCIA DE AUDITORIA:

La evidencia de auditoría es la información que obtiene el auditor para extraer conclusiones en las cuales sustenta su opinión.

FIREWALL:

Un firewall es un programa o hardware diseñado para bloquear las conexiones no deseadas a través de una red (por ejemplo Internet) mientras que permite las conexiones autorizadas.

FRAUDE INFORMATICO:

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. Los fraudes Informáticos también llamados PHISHING, es un plan que se utiliza para engañar a los consumidores y hacerles que revelen información personal y financiera por Internet.

HALLAZGO DE AUDITORIA:

Los hallazgos de la auditoría: son resultados de la evaluación de la evidencia de auditoría recopilada frente a los criterios de auditoría.

INFORME DE AUDITORIA:

Es el resultado de la información, estudios, investigación y análisis efectuados por los auditores durante la realización de una auditoría, que de forma normalizada expresa

por escrito su opinión sobre el área o actividad auditada en relación con los objetivos fijados, señalan las debilidades de control interno, si las ha habido, y formula recomendaciones pertinentes para eliminar las causas de tales deficiencias y establecer las medidas correctoras adecuadas.

INTEGRIDAD:

Garantizar que los datos sean los que se supone que son, es decir la corrección y completitud de la información

MANUAL DE SEGURIDAD INFORMATICA:

Es un documento en el que se plasman las medidas que buscan establecer los estándares de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos. Es una forma de suministrar un conjunto de normas internas para guiar la acción de las personas en la realización de sus trabajos.

MARCAS DE AUDITORIA:

Las marcas de auditoria son aquellos símbolos convencionales que el auditor adopta y utiliza para identificar, clasificar y dejar constancia de las pruebas y técnicas que se aplicaron en el desarrollo de una auditoria. Son los símbolos que posteriormente permiten comprender y analizar con mayor facilidad una auditoria.

MUESTREO DE AUDITORIA

La aplicación de procedimientos de auditoría en menos de 100% de las partidas existentes dentro de una población que es relevante para la auditoría, de tal modo que todas las partidas integrantes del universo, y sujetas a muestreo, tengan la oportunidad de ser seleccionadas, con objeto de proporcionarle al auditor bases razonables para obtener conclusiones sobre la población entera.

NORMA DE SEGURIDAD:

Define qué hay que proteger y en qué condiciones, pero para situaciones más concretas. Sirven para establecer unos requisitos que se sustentan en la política y que regulan determinados aspectos de seguridad.

PAPELES DE TRABAJO:

Son el conjunto de cédulas y documentación fehaciente que contienen los datos e información obtenidos por el auditor en su examen, así como la descripción de las pruebas realizadas y los resultados de las mismas sobre los cuales sustenta la opinión que emite al suscribir su informe.

POLITICA DE SEGURIDAD INFORMATICA:

Definen qué quiere la organización a muy alto nivel, de forma muy genérica, quedando como una declaración de intenciones sobre la seguridad de la Organización.

PLAN CONTIGENCIAL:

Un plan de contingencia es una estrategia planificada con una serie de procedimientos que faciliten u orienten a tener una solución alternativa que permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

PLAN DE SEGURIDAD INFORMATICA:

Consiste en la creación de una serie de políticas, procedimientos y métodos para llevar a cabo e implementar la Seguridad Informática.

Está comprendido por: Ámbito de aplicación con detalle de recursos protegidos, Estructura de los ficheros y descripción de los sistemas, Procedimientos de notificación, Gestión y respuesta ante las incidencias y, Actualización y adecuación legal.

PROCEDIMIENTOS DE AUDITORIA:

Los procedimientos de auditoría, son el conjunto de técnicas de investigación aplicables a una partida o a un grupo de hechos y circunstancias relativas a los estados financieros sujetos a examen, mediante los cuales, el contador público obtiene las bases para fundamentar su opinión.

PROCEDIMIENTOS DE EVALUACIÓN DEL RIESGO:

Procedimientos de auditoría desarrollados para obtener un entendimiento de la entidad y su entorno, incluyendo el control interno, con objeto de identificar y evaluar los riesgos de error material debido a fraude o error, de acuerdo con el marco de información financiera aplicable.

PROCEDIMIENTO DE SEGURIDAD:

Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución.

REDES:

Una red es un sistema de transmisión de datos que permite el intercambio de información entre ordenadores.

REFERENCIAS DE LA AUDITORIA:

Es un índice alfanumérico que siempre figura en rojo y se coloca en la esquina superior derecha.

RESPONSABLE DE LA SEGURIDAD:

El responsable de seguridad informática es el encargado de mantener como bien dice la palabra, la seguridad en el área de la informática, enfocada específicamente a la protección de la infraestructura computacional y todo lo relacionado con esta

(incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

RIESGO INFORMATICO:

Se define como: "La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generando se así perdidas o daños.

SEGURIDAD EN DATOS:

La seguridad es un aspecto muy importante en el manejo de información en el mundo de hoy. Las comunicaciones por correo electrónico y los archivos guardados en el disco duro deben estar protegidos en una forma que garantice que en el evento de que caigan en manos de terceros, la información contenida no se encuentre comprometida. El cifrado de mensajes y de archivos es la forma más segura de prevenir la pérdida de información.

SEGURIDAD DE REDES:

La seguridad de redes es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos.

SEGURIDAD FISICA:

La Seguridad Física consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

SEGURIDAD LOGICA:

La Seguridad Lógica: consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

SEGURIDAD LÓGICA Y CONFIDENCIAL:

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada apersonas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

SUFICIENCIA (DE LA EVIDENCIA DE AUDITORÍA): medida cuantitativa de la evidencia de auditoría. La cantidad de evidencia de auditoría necesaria depende de la valoración del auditor del riesgo de incorrección material así como de la calidad de dicha evidencia de auditoría.

TAAC:

Las TAAC's son un conjunto de técnicas y herramientas utilizados en el desarrollo de las auditorias informáticas con el fin de mejorar la eficiencia, alcance y confiabilidad de los análisis efectuados por el auditor, a los sistemas y los datos de la entidad auditada.

TELEFONIA CELULAR:

Es a aquel sistema de comunicación que se da a partir del uso de elementos pequeños o "células" que se conocen como celulares. La telefonía celular es uno de los avances más importantes y difundidos en el mundo en los últimos años y su llegada a millones de personas tiene que ver con la facilidad y la comodidad que otorga a sus clientes para comunicarse desde cualquier lugar y a cualquier hora.

USUARIO:

En informática, un usuario es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona.

VIRUS:

Un virus informático es un código que tiene la habilidad de infectar ordenadores sanos y replicarse desde los mismos, por la similitud en el comportamiento se los llamó virus.