UNIVERSIDAD MICHOACANA DE SAN NICOLAS DE HIDALGO

FACULTAD DE CONTADURIA Y CIENCIAS ADMINISTRATIVAS

"PROPUESTA METODOLOGICA PARA MEDIR LA SEGURIDAD INFORMATICA EN LA RED DE INFORMACION EN UN CENTRO DE COMPUTO".

TESIS PROFESIONAL

QUE PARA OBTENER EL TITULO DE

LICENCIADA EN INFORMATICA ADMINISTRATIVA

PRESENTA:

GABRIELA ANAHI EGUIA OLMEDO

ASESORA DE TESIS:

DRA. MA. HILDA RODALES TRUJILLO

Morelia, Michoacán, Agosto **2012**

INDICE

INTRODUCCION 5
PLANTEAMIENTO DEL PROBLEMA 7
OBJETIVO GENERAL 7
OBJETIVOS ESPECIFICOS 8
JUSTIFICACION 8
1. MARCO TEORICO 9
1.1 ADMINISTRACIÓN DE CENTROS DE CÓMPUTO 9
1.2 FUNDAMENTOS DE LAS REDES DE COMPUTADORAS 10
1.3 ESTANDARIZACION Y CERTIFICACION DE LA SEGURIDAD INFORMATICA 17
1.3.1 Puertos y servicios de una red IP 19
1.4 SEGURIDAD INFORMATICA 21
1.5 ESTANDARES DE SEGURIDAD 22
1.6 ANALISIS DE GESTION DE RIESGO EN UN SISTEMA INFORMATICO 22
1.6.1 Recursos de análisis y gestión de riesgos 24
1.6.2 Amenazas y vulnerabilidades 25
1.7 IMPACTOS Y RIESGOS 26
1.8 DEFENSAS SALVAGUARDAS O MEDIDAS DE SEGURIDAD 28
1.8.1 Controles de seguridad 28
1.9 EVALUACION DE RIESGOS 31
1.10 AUDITORIA INFORMATICA 32
1.11 METODOLOGIAS DE CONTROL INTERNO, SEGURIDAD Y AUDITORIA INFORMATICA 38
1.11.1 Las metodologías de auditoría informática 40
1.12 PRINCIPALES AREAS DE LA AUDITORIA INFORMATICA 41
1.13 CLASIFICACION DE AUDITORIAS EN LA SEGURIDAD DE DATOS 43
1.14 APLICACIONES EN APOYO A LA SEGURIDAD INFORMATICA 44
1.15 INSTRUMENTOS Y METODOLOGIAS DE EVALUACION 45
1.16 ENTREVISTA 46

1.16.1 Tipos de preguntas 47
1.17 SONDEOS 50
1.18 CHECKLIST O CUESTIONARIOS 52
1.18.1 Tipos de indicadores: 57
1.19 ESCALAMIENTO TIPO LIKERT 58
1.20 DISEÑO Y APLICACION DE CUESTIONARIOS 60
1.20.1 Aplicación de cuestionarios 61
2. APORTACION AL TEMA 62
2.1 DEFINICION DEL OBJETIVO Y VARIANTES EN LA SEGURIDAD DE UN CENTRO DE CÓMPUTO 62
2.1.1 Fundamentos de seguridad 64
2.2 ESTRUCTURA DEL INSTRUMENTO DE MEDICION 65
2.3 METODOLOGIA DE ANALISIS DE RIESGOS 66
2.4. DISEÑO DE LA FORMA COMO INSTRUMENTO DE EVALUACION 67
2.5 DISEÑO DE FORMATO DE CUESTIONARIO PARA LA AUDITORIA DE SEGURIDAD 68
2.6 REPORTE DE LA EVALUACIÓN DE LOS USUARIOS DEL CENTRO DE CÓMPUTO 70
2.7 ELABORACION DE CUESTIONARIOS BASADO EN LOS FUNDAMENTOS DE SEGURIDAD EN CENTROS DE CÓMPUTO 71
2.7.1 Cuestionarios sobre la seguridad física 71
2.7.1.1 Formato para medir la seguridad física: Ubicación. 71
2.7.1.2 Formato para medir la seguridad Física: Estructura. 73
2.7.1.3 Formato para medir la seguridad lógica: Amenazas. 74
2.7.1.4 Formato para medir la seguridad física: Control y acceso. 76
2.7.1.5 Formato para medir la seguridad física: Protección. 78
2.7.2 Cuestionarios sobre la seguridad Lógica 80
2.7.2.1 Formato para medir la seguridad lógica: Usuarios. 80
2.7.2.2 Formato para medir la seguridad lógica: Sistemas. 82
2.7.2.3 Formato para medir la seguridad lógica: Discos. 83
2.7.2.4 Formato para medir la seguridad lógica: Aplicación. 85
2.7.2.5 Formato para medir la seguridad lógica: Bases de datos. 87
2.8 FORMATO TIPO CARTA DE AUDITORÍA 89
2.9 ELEMENTOS A EVALUAR EN CENTROS DE COMPUTOS REALES 91

2.10 EVALUACION DE ELEMENTOS PARA LA AUDITORIA DE SEGURIDAD EN UN CENTRO DE CÓMPUTO 92
2.11 APLICACIÓN DEL INSTRUMENTO DE EVALUACION (CUESTIONARIOS) 93
CONCLUSION 101
RECOMENDACIONES 102
PERSPECTIVAS 103
BIBLIOGRAFIA 104

INTRODUCCION

Una entidad, oficina o departamento que se encarga del procesamiento de datos e información de forma sistematizada, es llamada centro de cómputo, esté permite que se lleve el procesamiento con la utilización de computadoras que están equipadas con el hardware y el software necesarios para cumplir con dicha tarea. Por lo general, las computadoras se encuentran interconectadas en red y cuentan con conexión a Internet, las cuales estas controladas por el proceso administrativo, este proceso se da en varias etapas: Planeación, organización, dirección y control.

El control es el proceso de determinar lo que se está llevando a cabo, a fin de establecer las medidas correctivas necesarias y así evitar desviaciones en la ejecución de los planes. Aplicado por la auditoría informática que es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial y mantiene la integridad de los datos.

La auditoria consiste en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen con los objetivos o estrategias, estableciendo cambios que se deberían realizar para la consecución de los mismos. La auditoría se aplica mediante metodologías, que son necesarias para desarrollar cualquier proyecto, ésta identifica el nivel de "exposición" por la falta de controles mientras el análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones en base al costo beneficio de la misma. Una metodología es el plan de investigación que permite cumplir ciertos objetivos en el marco de una ciencia. Todas las metodologías en seguridad van encaminadas a establecer y mejorar las contramedidas que garanticen que la productividad de que las amenazas se materialicen en hechos sea lo más baja posible o al menos quede reducida de una forma razonable en costo beneficio.

Las metodologías de auditoría informática son de tipo cualitativo/subjetivo. Se puede decir que son subjetivas por excelencia. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen en gran profesionalidad y formación continua. De la misma forma se describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar. La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. Si bien las metodologías de auditoría son subjetivas y están basadas en profesionales de gran nivel.

En el presente trabajo de investigación se propone un instrumento de apoyo en la metodología que propone (Peso, 2001) en la auditoria informática para llevar a cabo la seguridad informática a fin de medirla en las redes de información de un centro de computo como medida de control.

Este trabajo es una investigación de tipo cualitativo/ inductivo, por lo tanto es una investigación flexible y el punto de partida son conceptos esenciales a la investigación y se divide en tres partes principales.

En la primera parte de la investigación se llevó a cabo el marco metodológico que dará fundamento a la aportación propia en el desarrollo metodológico de una auditoria informática específicamente por lo que respecta al marco teórico, la segunda parte de este trabajo está integrado por las referencias teóricas y contextuales, que es donde se muestra la información bibliográfica y documental referente a la estructura y componentes de sus elementos de lo que refiere a la red de ordenadores, los recursos que serán evaluados en el centro de computo, así como el análisis de riesgos en la seguridad informática, los tipos de amenazas informáticas, así mismo se hace una amplia investigación sobre las metodologías existentes para la elaboración de cuestionarios como instrumento de medición en el proceso de auditoría informática y su aplicación a los centros de computo. También contiene algunas citas de algunas obras que apoyan el trabajo que incluyen información de los factores, elementos y características del medio que se relacionan con el problema.

La tercera parte de este trabajo se diseña la metodología recomendada por (Kendall, Analisis y diseño de sistemas, 2005) para la elaboración y diseño de cuestionarios que servirán de apoyo a la auditoria informática, se aplica este instrumento a la empresa con la finalidad de probar su viabilidad y emitir algunas recomendaciones. También se encuentran la cuantificación de resultados, en donde se habla de la forma en que se aplicará el instrumento de evaluación para el centro de cómputo y el análisis de la aplicación que abarca la interacción de los sujetos aplicando este instrumento. Este proyecto espero y sirva de apoyo o sea una alternativa que los ayude a tratar un problema, pero sobre todo que sirva de apoyo para que reflexionen sobre la importancia de conocer y mejorar los recursos tecnológicos que se deben tener en los centros de cómputo para evitar cualquier tipo de ataque informático.

Finalmente, se dan a conocer las conclusiones a que se arribó con el desarrollo del presente trabajo de investigación, la bibliografía que sirvió de base para el marco teórico, así como algunos anexos que sirvieron de apoyo en el desarrollo de esta portación.

PLANTEAMIENTO DEL PROBLEMA

Prácticamente el centro de computo cuenta con un gran número de problemas que afectan la red de información. Esto debido a la falta de revisión en el área de seguridad. Analizando, aplicando e investigando, me di cuenta cuáles son esos inconvenientes que han hecho deficiente el proceso de transmitir los datos de información con seguridad. Lo cual hace que se obtenga un resultado más afondo y seguro si aplicamos y realizamos una auditoría de seguridad.

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto se puede hacer robo de información o alterar el funcionamiento de la red. Tomando en cuenta de que se pueden presentar varios aspectos que no permitan que un centro de cómputo sea seguro como es el caso de sabotaje, incendio, inundación, perdida de respaldos o por personas que se dedican a entrar en la red de información de varias empresas. Sin embargo el hecho de que la red no sea conectada a un entorno no nos garantiza la seguridad de la misma.

En el centro de cómputo existe la posibilidad de que se dé el caso, que se encuentren algunos tipos de amenazas. Para ello se diseñará un instrumento de evaluación, que diagnosticará que se está omitiendo o que faltaría para prevenir, evitar o eliminar daños en el sistema de información.

Con base a lo anterior considero fundamental abordar esta problemática diseñando un instrumento de evaluación por medio de la realización de cuestionarios y formatos que ayudaran para la realización de una auditoría capaz de mejorar la seguridad en la red de información en cualquier centro de cómputo.

OBJETIVO GENERAL

Diseñar un instrumento de medición para auditar la seguridad física y lógica en un centro de cómputo en donde además se obtenga información suficiente para ofrecer alternativas de seguridad y se identifiquen los problemas de seguridad en la red de información del centro de cómputo.

OBJETIVOS ESPECIFICOS

- Analizar e Investigar los diferentes aspectos que involucran el buen funcionamiento del centro de cómputo, su evaluación y control.
- Investigar aspectos generales y específicos relacionados con la seguridad física y lógica de un centro de cómputo.
- Analizar, comparar y seleccionar la metodología más adecuada para el diseño de instrumentos de medición.
- Ponderar el impacto que representa el diseño de un instrumento de medición en el desarrollo metodológico de la Auditoría Informática.

JUSTIFICACION

Debido a que la información es parte fundamental en toda sociedad la importancia de tenerla segura y en resguardo es aún mayor, nuestra información corre el riesgo de que se presenten problemas de inseguridad, pues debemos entender que es necesario comenzar a preocuparnos por los motivos que ocasionan o afectan la perdida de la información existente, frente a los retos que representan las condiciones cambiantes de su entorno social y tecnológico, el centro de computo replantea nuevos cambios en la estructura de respaldo de la información ya que se divide en varias áreas de la ciencia, la tecnología, las humanidades y las disciplinas estableciendo mecanismos de planeación estratégica y prospectiva, apoyados en la asesoría de la información y la pérdida que esta puede afectar, hace que nuestro proyecto sea importante realizarlo ya que se tiene en cuenta el cambio en nuevas áreas de tecnología y se podrá obtener un conocimiento entre las amenazas existentes dentro de la red del centro de computo. Y así dar una solución y obtener como beneficio la seguridad de la información encontrada en la red así como proteger, recuperar y resguardar a esta mediante robo, perdida o daño. La seguridad informática no es un bien medible, en cambio; sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

Es por eso la importancia de aplicar instrumentos de medición que nos ayuden a proporcionar un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático en la red de datos de información acerca del centro de cómputo, así como evaluar los riesgos que enfrenta. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se

estima el impacto potencial y los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios ya que son el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

1. MARCO TEORICO

1.1 ADMINISTRACIÓN DE CENTROS DE CÓMPUTO

Para (Meza) un centro de cómputo representa una entidad dentro de la organización, la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna. Su función primordial es primordial la labor administrativa para hacerla más segura, fluida y así simplificarla. El centro de cómputo es responsable de centralizar, custodiar y procesar la mayoría de los datos con los que opera la compañía. Prácticamente todas las actividades de los demás departamentos se basan en la información que les proporciona dicho centro. La toma de decisiones depende de gran medida de la capacidad de respuesta del proceso de datos. Por lo anterior casi no se escatima la inversión para proveerlo del equipo técnico necesario.
Un centro de cómputo significa la culminación de la sistematización de la empresa. El análisis y diseño de sistemas de información implica un alto grado de eficiencia administrativa dentro de la organización, de lo contrario difícilmente se podrían llevar a la práctica los diseños. En otras palabras el centro de cómputo debe predicar la buena administración.
Áreas de un centro de cómputo

El centro de cómputo está compuesto por las siguientes áreas:

- Área directiva
- Área técnica
- Área operativa
- Área administrativa

Características generales

Debido a la naturaleza de un centro de cómputo, la complejidad de los problemas que lo aquejan es diversa. Estos problemas son ocasionados por personas (ya sean trabajadores de la organización o usuarios), problemas en las maquinas y problemas en los programas, ya

sean paquetes utilizados o los programas que se construyen para los usuarios, además de los problemas relacionados con la construcción que alberga las computadoras.

Clasificación:

Los problemas comunes dentro de un centro de cómputo se clasifican en:

- Problemas de hardware
- Problemas de software
- Problemas de recurso humanos
- Problemas de instalaciones física

El administrador de un centro de cómputo

Cuando se designa a una persona para un cargo administrativo de cualquier nivel, se espera en su desempeño en las funciones propias de su puesto este en congruencia con sus antecedentes laborales en l.as funciones operativas que venía desempeñando previamente, y por tanto, se espera que esta persona adquiera de manera mágica las siguientes características:

- Habilidad para asumir riesgos
- Profesionalismo
- Decisiones oportunas y adecuadas
- Designación de subordinados
- Definición de objetivos y políticas
- Control
- Cualidades

1.2 FUNDAMENTOS DE LAS REDES DE COMPUTADORAS

(Vieites, 2006) Define un computadora como máquina electrónica que recibe y procesa datos para convertirlos en información útil, por lo cual una red de computadoras está constituida por un conjunto de computadoras que se conectan entre sí para poder cambiar información y compartir una serie de servicios.
También señala que las redes de computadoras se han popularizado desde mediados de los años ochentas, propiciadas por la introducción de la computadora personal (PC personal computer) en las oficinas. La implantación de estos equipos de trabajo personales en las empresas plantea dos nuevos tipos de demandas:

- Por una parte, la necesidad de compartir información en forma ágil y sencilla entre los usuarios de estos equipos.
- Por otra parte, la posibilidad de compartir recursos escasos entre varios de estos equipos: impresoras, discos duros, dispositivos de hardware y conexiones a otras redes como internet.

Se pueden distinguir tres tipos de redes de computadoras, dependiendo de su alcance geográfico y de sus características de funcionamiento.

- Redes de área local
- Redes de red amplia
- Red de área metropolitana

El principal problema que ha tenido que afrontar la industria informática para desarrollar las redes de computadoras ha sido el conseguir la interconexión de distintos tipos de equipos y sistemas informáticos, en principio totalmente incompatibles entre sí. Para ello, (Vieites, 2006) define una serie de estándares y protocolos que permiten alcanzar la interoperabilidad entre los distintos sistemas.

Los estándares facilitan el desarrollo de sistemas y servicios compatibles entre los distintos fabricantes del mercado. Existen diferentes organismos nacionales e internacionales encargados de la aprobación de los distintos estándares que afectan a la industria de la informática y las telecomunicaciones.

Algunos de los principales organismos responsables de la estandarización en el ámbito de la informática y las telecomunicaciones son el Institute of Electrica and Electronic Engineers (IEEE), la International Telecommunications Union (ITU), American National Standards Institute (ANSÍ), European Telecommunications Standards Institute (ETSI), Committee for Telegraphy and Telephony (CCITT) o la International Standards Organization (ISO).

A su vez, el organismo internacional ISO ha definido el modelo de Interconexión de Sistemas Abiertos (OSI), para facilitar la interconexión de equipos y redes de distintos fabricantes.

En el ámbito de Internet varios organismos se encargan de definir los estándares para dar soporte a los protocolos y servicios de la Red.

Para poder establecer la comunicación entre los ordenadores que forman parte de una red, se utilizan “protocolo de comunicaciones”, que constituyen una serie de normas y procedimientos definidos para poder resolver los problemas asociados al intercambio de información:

- Trasmisión fiable de los datos: que los datos lleguen libres de errores y sin pérdidas a su destino
- Encaminamiento a través de la red: que los datos se entreguen a la computadora destinatario atravesando otras maquinas conectadas a la red.

- Gestión del dialogo entre maquinas: establecer un orden entre la comunicación de las aplicaciones que se ejecutan en las computadoras de la red.

Para resolver todas estas cuestiones se ha definido un modelo en "capas" o niveles: el modelo OSI del organismo de estandarización ISO, es una torre de protocolos para facilitar la interconexión de equipos de redes y de distintos fabricantes. Cada capa ofrece una serie de servicios a la inmediatamente superior y se apoya en los servicios proporcionados en las capas inferiores.

- Nivel físico: se ocupa de las cuestiones relacionadas con la conexión eléctrica, el cableado, la definición de los tipos de señales y esquemas de codificación de empleados.
- Nivel de enlace: su misión es garantizar la transmisión fiable entre maquinas que se encuentran directamente conectadas, se ocupa del control de acceso al medio en medios compartidos, como en el caso de un bus en una red local.
- Nivel de red: se encarga del encaminamiento a través de la red, consigue que los datos se entreguen al equipo destinatario atravesando varios ordenadores y equipos de interconexión.
- Nivel de trasporte: es el responsable de garantizar que la trasmisión extremo a extremo a través de la red sea fiable, se responsabiliza del control de flujo para evitar que equipos rápidos lleguen a saturar las transmisiones a otros más lentos.
- Nivel de sesión: se encarga de la gestión de dialogo entre las máquinas que intervienen entre la comunicación a través de la red.
- Nivel de presentación: tiene como función de llevar a cabo la codificación de los datos.
- Nivel de aplicación: es específico de la aplicación que proporciona el servicio final a los usurarios y define como deben de actuar los ordenadores que intervienen en la comunicación para poder facilitar dicho servicio.

ELEMENTOS UTILIZADOS EN LAS REDES DE COMPUTADORAS

(Vieites, 2006) Comenta que para construir una red de computadoras, se emplean una serie de equipos hardware y herramientas software, cuya función es ofrecer los servicios necesarios para la transmisión de datos entre los ordenadores y otros dispositivos que se conectan en la red.

En primer lugar es necesario instalar en cada computadora o terminal una tarjeta de red, encargada del envió y recepción de datos a través del medio de transmisión. Asimismo se requiere la instalación del cableado utilizado para construir el medio de transmisión compartido por todos los ordenadores y terminales: par trenzado, UTP, cable coaxial o fibra óptica.

Se distinguen dos tipos de cable de par trenzado: par trenzado no apantallado y par trenzado apantallado. Por otra parte los dispositivos de interconexión facilitan la interconexión de redes LAN, WLAN y WAN de distintas características: bridges, routers, gateways, etc.

DISPOSITIVOS DE INTERCONEXION

Repetidores

Son dispositivos que generan la señal y la transmiten a un nuevo segmento de la red de área local (LAN) sin interpretar la información y sin tomar ninguna decisión sobre su origen y destino.

Puentes (Bridges)

Se encargan de almacenar y reexpedir tramas de datos de redes tipo LAN, facilitando la interconexión de redes LAN que utilicen distintas técnicas de control de acceso al medio.
Los puentes se encargan de regenerar la señal para transmitirla a la otra red local solo cuando sea necesario, es decir, cuando los datos vayan destinados a un equipo que se encuentra en esa otra red, realizando una adaptación a la técnica de control de acceso al medio empleada en esta segunda red.

Concentradores (hubs switches)

Se emplean en el cableado estructurado de edificios y oficinas, cuya finalidad es evitar el despliegue de una red en topología en estrella, en la que todos los cables utilizados se conectan a los puertos de uno de estos dispositivos.
Se distinguen dos tipos de concentradores:

- Concentradores elementales, denominados hubs, que simplemente retrasmiten la señal que reciben por uno de sus puertos a todos los demás puertos.
- Concentradores inteligentes, denominados switches, que utilizan una matriz interna de conmutación para retransmitir los datos que reciben por uno de sus puertos directamente por el puerto en que se encuentra el equipo al que van dirigidos, sin utilizar el resto de los puertos.

Encaminadores (routers)

Facilitan la interconexión de distintas redes de ordenadores, ocupándose del encaminamiento de los paquetes de datos a partir de la interpretación de las direcciones de origen y de destino. También se encargan del control de la congestión, midiendo la cantidad de tráfico que deben cursar en cada instante.

Pasarelas

Son dispositivos capaces de realizar una conversión de protocolos entre dos redes totalmente distintas. Trabaja en los niveles altos de modelo OSI (Vieites, 2006).

TIPOS DE REDES

Redes de área local LAN

Para (Vieites, 2006) una red de área local (del ingles: LAN Local Area Network) ocupa una red geográfica, generalmente limitada a un edificio o una planta dentro de un edificio. Se trata de una red de carácter privado, gestionada por una única organización y que posee una alta fiabilidad y seguridad, ofreciendo elevadas tasas de transferencias de decenas o cientos de Mbps alcanzando incluso lo gbps.

Hay varios tipos de redes de área local, en función del tipo de cable utilizado, la disposición o topología del cable, la velocidad de datos a la que operan. Los protocolos de comunicaciones y el método de control de acceso al medio compartido.

- Topología lineal: red en la que los equipos se conectan directamente a un único cable, que actúa como un bus de datos terminado por dos resistencias

Figura 1: Topología lineal (Vieites, 2006)

- Topología en anillo: en esta topología el cable se cierra sobre si mismo formando un anillo.

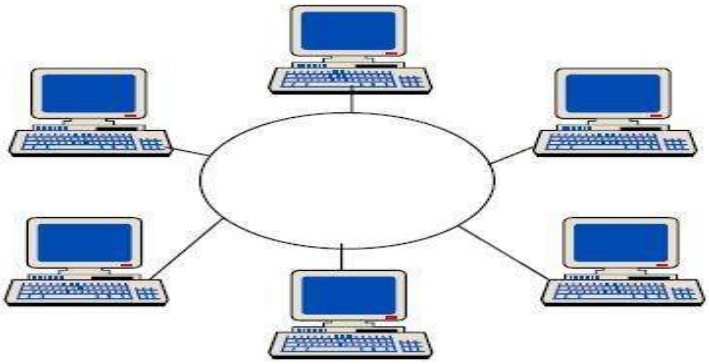


Figura 2: Topología de anillo (Vieites, 2006)

Topología en estrella: en esta configuración todos los cables parten de una posición central hacia los equipos que constituyen la red. A cada equipo llega un único cable independiente,

de tal modo que una rotura en dicho cable solo deja aislado al equipo que depende de él, posibilitando que el resto de la red siga trabajando con normalidad.

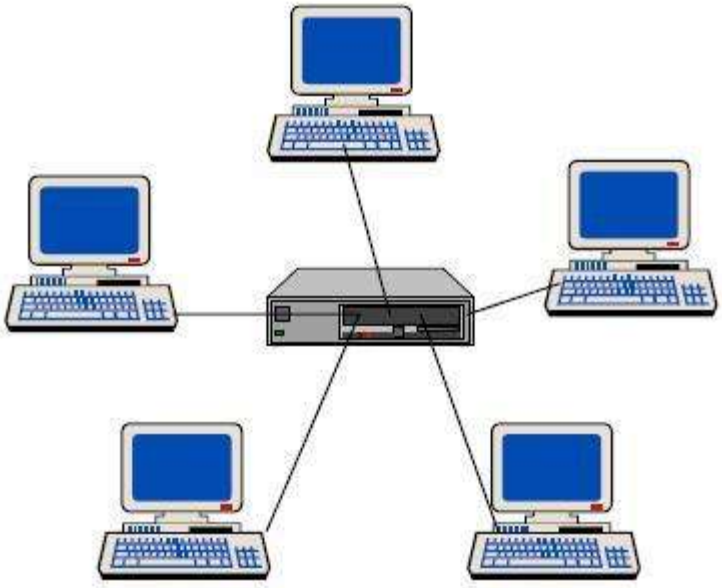


Figura 3: Topología de estrella (Vieites, 2006)

En la norma IEEE 802.3 se distinguen distintos tipos de redes Ethernet, en función del tipo de cable empleado, de la velocidad de transmisión y de la longitud máxima de la red:

- 10Base-5: 10 Mbps con cable coaxial y longitud máxima de 500 metros.
- 10Base-2: 10 Mbps con cable coaxial RG-58 y longitud máxima de 185 metros.
- lOBase-T: 10 Mbps con cable par trenzado UTP y longitud máxima de 100 metros.
- lBase-5: 1 Mbps con cable par trenzado UTP y longitud máxima de 500 metros.
- lOBase-F: 10 Mbps con cable de fibra óptica y longitud máxima de 4.000 metros.
- lOOBase-TX: 100 Mbps con cable par trenzado UTP categoría 5 de ocho hilos (del ingles: Fast Ethernet).

Por otra parte, TokenRing es un tipo de red local desarrollado por IBM, que cuenta con una cierta implantación en el sector de la banca, si bien hoy en día ha perdido cuota de mercado a favor de la tecnología Ethernet. Sus características se definen en la norma IEEE 802.5, utilizando un mecanismo de paso de testigo en anillo para el control de acceso al medio.

Redes inalámbricas (WLAN)

(Vieites, 2006) Define una red inalámbrica como un tipo especial de red de área local en la que los equipos se pueden conectar a través de ondas electromagnéticas o de puertos que utilizan infrarrojos, evitando de esto modo la necesidad de cablear los edificios.
Las redes inalámbricas presentan dos importantes ventajas: la movilidad de los equipos dentro de la zona de cobertura, así como la facilidad en el despliegue y puesta en marcha de la red, ya que no se requiere el tendido de cables por el interior del edificio.
Por lo tanto, las redes inalámbricas más extendidas (modo infraestructura) emplean tarjetas de red conectadas a pequeñas antenas que realizan las funciones de un transmisor/receptor de radiofrecuencia y que se conectan a un "punto de acceso" de la red, dispositivo consistente en un hub o un switch que cuenta con un equipo transmisor/receptor de radiofrecuencia.
Debido a la notable reducción del costo de los equipos necesarios, a la adopción de una serie de estándares que facilitan la interoperabilidad (normas Wi-Fi) y a la mayor oferta de productos disponibles en el mercado, este tipo de redes, también conocidas como Wireless LAN (WLAN), están experimentando un notable desarrollo en estos últimos años, siendo previsible que se produzca una fuerte expansión de los servicios inalámbricos en el corto y en el medio plazo.

Redes de área amplia (WAN)

Se caracterizan por su amplia extensión geográfica, de varias decenas incluso miles de kilómetros. Suelen ofrecer una menor fiabilidad y calidad de servicio que las redes locales, con menores tasas de transferencia para los usuarios finales.
(Vieites, 2006), comenta que una red WAN puede tener un carácter privado, si pertenece a una organización que la utiliza exclusiva, o bien un carácter público, cuando pertenece a uno o varios operadores de telecomunicaciones que la utilizan para proporcionar una serie de servicios a sus clientes. Etas redes persiguen ofrecer servicios de transmisión de todo tipo de información: ficheros de ordenador, correo electrónico, voz, imágenes, etc.

El protocolo TCP/IP

El principal problema que se ha tenido que afrontar durante el desarrollo de Internet ha sido el conseguir la interconexión de distintos tipos de redes y sistemas informáticos, totalmente incompatibles entre sí. Para ello, se ha definido un conjunto de protocolos de comunicaciones que permiten alcanzar la interoperabilidad entre los distintos sistemas, constituyendo una especie de "lenguaje común" a todos los equipos conectados a la Red.

El protocolo TCP/IP, desarrollado a principios de los años ochenta por la Universidad de Berkeley (California) e implantado en Internet desde 1983, es el que se encarga de garantizar la comunicación fiable entre equipos. Asimismo, para cada uno de los servicios proporcionados por Internet se ha desarrollado un protocolo específico: HTTP para el World Wide Web, HTTPS para el World Wide Web seguro, SMTP para el correo electrónico, NNTP para el acceso a grupos de noticias (news), etc.

TCP/IP define, por tanto, un conjunto de normas que rigen la transmisión de datos entre los ordenadores conectados a Internet. Se divide en dos protocolos principales, que constituyen la base de todos los restantes:

- El protocolo IP (del ingles: Internet Protocol), cuyo cometido principal es el encaminamiento de los paquetes de datos por la red, seleccionando la ruta que debe seguir cada uno para alcanzar su destino, sin preocuparse de si éstos se entregan ordenados o si alguno se pueda llegar a perder en la red.
- El protocolo TCP (del ingles: Transfer Control Protocol), que se encarga de llevar a cabo la fragmentación de la información en paquetes y de garantizar la transmisión fiable de datos entre el transmisor y receptor: reagrupamiento de los paquetes, detección de errores y gestión de retransmisiones, control del flujo de datos, etc.

1.3 ESTANDARIZACION Y CERTIFICACION DE LA SEGURIDAD INFORMATICA

Direccionamiento de los equipos

Cada tarjeta de red (NIC) instalada en un equipo informático, ya sea éste un ordenador, impresora u otro dispositivo periférico, tiene asignada una dirección física. Esta dirección también es conocida como dirección MAC (del ingles: Médium Access Control), tiene una longitud de 48 bits (6 bytes) y es asignada por el propio fabricante y grabada en el hardware de la tarjeta. De este modo, cada tarjeta de red puede ser identificada de forma única en cualquier red a la que se encuentre conectada.

Cada equipo conectado a Internet tiene asignado un número que permite su identificación y que se conoce como "dirección IP". Se trata de una dirección lógica o dirección de red, constituida por una secuencia de 4 bytes (32 bits), asignada de forma estática o dinámica al dispositivo mediante software.

Las direcciones IP pueden ser fijas (cuando son asignadas de forma estática al equipo en cuestión) o dinámicas, siendo asignadas en este último caso mediante un servidor DHCP (del ingles: Dynamic Host Configuration Protocol), de tal modo que cada equipo podría utilizar una dirección distinta en cada sesión de trabajo dentro de la red. La asignación dinámica facilita la configuración y gestión de los equipos en redes grandes, posibilitando compartir un número reducido de direcciones IP disponibles entre un número mayor de equipos. Sin embargo, debemos tener en cuenta la limitación de que no se podrían conectar todos los equipos de forma simultánea a la red, ya que el número de conexiones estaría restringido por el número de direcciones IP disponibles, puesto que no pueden existir dos equipos compartiendo la misma dirección en una red.

(Royer, 2004), distingue dos partes de una dirección IP: el número que identifica a la subred (red conectada a Internet) y el número que identifica al ordenador dentro de la subred (cada ordenador conectado a la red se denomina "host", siguiendo la terminología de Internet). Este esquema de direccionamiento se ha definido para poder acomodar tanto a redes grandes, compuestas por un gran número de equipos, como a redes pequeñas, de una forma bastante flexible.
De este modo, se han creado cinco clases de direcciones IP, utilizando para su distinción el prefijo de subred de la dirección IP:

DIRECCIONES IP		
Dirección	**Subred**	**Capacidad**
Clase A: (0…127)	8 bits dedicando 24 para identificar cada máquina dentro de ls subred	128 redes
Clase B: (128…223)	24 bits dedicando 8 bits para identificar cada máquina dentro de la subred.	16.384 redes
Clase C: (192…223)	24 bits dedicando 8 bits para identificar cada máquina dentro de la subred.	2.097.152 redes

También las direcciones IP pueden ser públicas o privadas. Las primeras son las que se pueden utilizar directamente por los equipos conectados a Internet, por lo que tienen que ser asignadas por los organismos que gestionan los recursos de Internet (en este caso la

ICANN, Internet Corporation for the Assignment of names and Numbers) a las empresas y organismos que las solicitan.
Las direcciones IP privadas sólo se pueden utilizar en el interior de una red privada. Este tipo de direcciones han sido propuestas para que las organizaciones puedan trabajar internamente con un número mayor de direcciones de las que tienen oficialmente asignadas para conectarse a Internet (direcciones públicas).

Rango direcciones	1 0.xxx.xxx.xxx	172.016.xxx.xxx	192.168.xxx.xxx
Máscara subred	255.0.0.0	255.255.0.0	255.255.255.0

Tabla 1: Rangos de direcciones IP privadas (Royer, 2004).

Se ha definido el protocolo NAT (del ingles: Network Address Translation) para realizar una traducción de direcciones privadas a direcciones IP públicas, facilitando de este modo que varios equipos internos de la red de una organización (cada uno con su propia dirección IP privada) puedan conectarse a Internet compartiendo una misma dirección IP pública, aprovechando al máximo el espacio de direcciones públicas disponible en la actualidad.
No obstante, está prevista la ampliación del tamaño actual de las direcciones IP de 4 bytes a 16 bytes con la nueva versión del protocolo IP, denominada IPv6, para incrementar de forma drástica el número total de direcciones disponibles, solucionando así el problema de escasez de direcciones planteado por el espectacular crecimiento de la Red en los últimos años, muy por encima de las previsiones más optimistas.

1.3.1 Puertos y servicios de una red IP

(Lamere, 1987) define un puerto como una entidad empleada para poder ofrecer distintos servicios y establecer comunicaciones simultáneas desde una misma máquina. De este modo, cada servicio de Internet se ofrece en un determinado puerto, es decir, el servidor o equipo en cuestión se encuentra escuchando en ese puerto a la espera de las peticiones de los clientes que se deseen conectar a él.
Se emplea un número de 16 bits para identificar a cada puerto, por lo que existen un total de 65.535 puertos disponibles. Los primeros números, desde el puerto O hasta el 1.023, se conocen como "puertos bien conocidos" (Well Knawn París) y se reservan a determinados servicios. Los puertos desde el número 1.024 hasta el 49.151 son puertos registrados y asignados de forma dinámica: son utilizados, por ejemplo, por el equipo cliente que establece una conexión con un equipo servidor. Por último, los puertos desde el número 49.152 hasta el 65.535 se consideran puertos privados, reservados para otros usos.

En la siguiente tabla se presenta una relación de los puertos utilizados por algunos de los servicios más conocidos de Internet:

Puerto	Servicio	Protocolo	Descripción
20	FTP-Datos	TCP/UDP	Transferencia ficheros
21	FTP	TCP	Control de la transferencia de ficheros
23	TELNET	TCP/UDP	Conexión remota
25	SMTP	TCP/UDP	Envío de mensajes de correo
53	DNS	TCP/UDP	Servicio de nombres de dominio
80	HTTP	TCP/UDP	World Wide Web
110	POP3	TCP/UDP	Acceso a buzones de correo
194	IRC	TCP/UDP	Chat
443	HTTPS	TCP	HTTP seguro vía SSL

Tabla 2: Lista de puertos y servicios de Internet (Lamere, 1987).

Una red IP puede ofrecer multitud de servicios a sus usuarios, utilizando para ello dos protocolos de transporte distintos: el protocolo TCP y el protocolo UDP (User Datagram Protocole).

Los servicios basados en el protocolo TCP son servicios orientados a conexión, es decir, requieren de un establecimiento previo de una conexión entre los equipos antes de poder proceder al intercambio de datos. Así mismo, el protocolo TCP establece un control del flujo de datos, limitando el número de paquetes enviados que se encuentran pendientes de confirmación.

Se trata, en definitiva, de un servicio de transmisión de datos robusto y fiable, que se encarga de garantizar que todos los paquetes de datos transmitidos son recibidos correctamente por su destinatario y en el orden adecuado, detectando y corrigiendo posibles pérdidas o daños en estos paquetes de datos.

Por su parte, los servicios basados en el protocolo UDP son servicios no orientados a conexión. En este tipo de servicios no existen confirmaciones ni se numeran los paquetes de datos, por lo que éstos se podrían perder en la red o llegar desordenados al equipo.

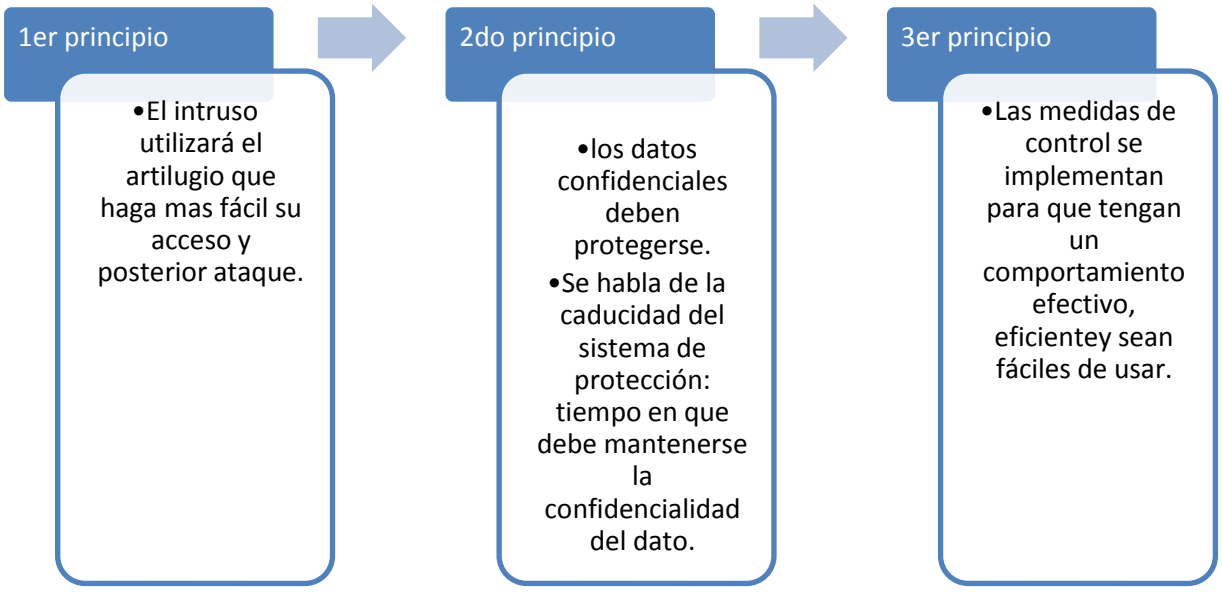
El protocolo UDP se emplea sobre todo en aplicaciones de tiempo real ("streaming" de audio y vídeo, telefonía IP, etc.), así como en algunas aplicaciones sencillas y servicios de Internet que no requieran de un intercambio continuo de datos entre el cliente y el servidor (como SNMP, TFTP, NFS, etc.).

1.4 SEGURIDAD INFORMATICA

(Miret, 2006)Definen la seguridad es la "cualidad de seguro". La seguridad no es un producto, sino un proceso.
Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:
Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico.
La seguridad informática no es un bien medible, en cambio; sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.
A finales del siglo XX e inicios del XII tanto las empresas, organismos e incluso particulares comienzan a tomar verdadera conciencia de su importancia. Hoy en día, tener un sistema que cumpla con los estándares de gestión de la seguridad es sinónimo de calidad de servicio.

Principios de la seguridad informática

(Miret, 2006) Definen los siguientes principios de seguridad:



1.5 ESTANDARES DE SEGURIDAD

(Vieites, 2006), considera que en el caso de los estándares de seguridad existen al menos tres razones que justifican su desarrollo e implantación:

- Suministrar normas de seguridad a los fabricantes de productos. Los estándares permiten establecer una serie de orientaciones para el desarrollo de nuevos productos.
- Definir métricas de evaluación, de certificación y de acreditación. Aplicadas tanto procesos como a técnicas de gestión y al desarrollo de comercialización de productos y servicios.
- Trasmitir la comunicación necesaria a los usuarios y consumidores. Los usuarios pueden comparar sus requerimientos específicos de seguridad frente a lo establecido en distintos estándares para poder determinar cuál es nivel de seguridad que necesitan, y en consecuencia, que características o atributos deberían exigir a los productos o servicios que vayan adquirir.

Para (Vieites, 2006), la evaluación consiste en el análisis de la capacidad de un determinado producto para proteger la información de acuerdo a unos criterios establecidos.
La certificación es el proceso que permite determinar la capacidad de un determinado producto para proteger la información de acurdo a unos criterios establecidos.
Mediante el proceso de certificación se puede confirmar de forma independiente la validez de los resultados y conclusiones de la evaluación previa, y si estas evaluaciones se han llevado a cabo de acuerdo con el procedimiento establecido. Este principio se distingue en cuatro tipos de certificaciones:

- Certificación de la seguridad de las tecnologías de la información.
- Certificación de la seguridad cristológica
- Certificación de la seguridad física
- Certificación de la seguridad de emanaciones radioeléctricas.

1.6 ANALISIS DE GESTION DE RIESGO EN UN SISTEMA INFORMATICO

Para (Vieites, 2006), un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que debe realizar con rigor y objetividad para

que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de información y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo.
En el proceso propiamente dicho de la gestión de riesgos se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema no el posible impacto en la organización, así como permitir la recuperación del sistema o la transferencia del problema a un tercero.

Figura 4: análisis de gestión de riesgos en una organización (Vieites, 2006).

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).
El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo:

$$WR_i = R_i * I_i$$

Otros factores que debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

Luego, con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + \ldots + WR_n * I_n)}{I_1 + I_2 + \ldots + I_n}$$

Los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

- Estimación del riesgo de pérdida del recurso (R i)
- Estimación de la importancia del recurso (I i)

1.6.1 Recursos de análisis y gestión de riesgos

Para (Vieites, 2006), los recursos son los activos para proteger el sistema informático de la organización.

Presenta los principales recursos que se deberían tener en consideración a la hora de analizar y gestionar los riesgos.

- Recursos hardware: servidores y estaciones de trabajo, ordenadores portátiles, impresoras, escáneres y otros periféricos.
- Recursos software: sistemas operativos, herramientas ofimáticas, software de gestión, herramientas de programación, aplicaciones desarrolladas a medida, etc.
- Elementos de comunicaciones: dispositivos de conectividad, armarios con paneles de conexión, cableado, puntos de acceso a la red, líneas de comunicación con el exterior, etc.
- Información que se almacena, procesa y distribuye a través del sistema.
- Locales y oficinas donde se ubican los recursos físicos y desde los que acceden al sistema los usuarios finales.
- Personas que utilizan o se benefician directa o indirectamente del funcionamiento del sistema.
- Imagen y reputación de la organización.

Cada recurso o activo de la organización se podría caracterizar por un código, su descripción, su costo o precio de adquisición, su costo de reposición, su nivel de criticidad o importancia para el mantenimiento de las actividades de la organización, el nivel requerido de integridad y de confidencialidad, etc.

1.6.2 Amenazas y vulnerabilidades

(Vieites, 2006), Considera una amenaza como cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.
Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Algunas amenazas de seguridad son:

- Amenazas naturales: inundaciones, incendio, tormenta, fallo eléctrico, explosión, etc.
- Amenazas de agentes externos: virus informáticos, ataque de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red robos, estafas, etc.
- Amenaza de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc.

También podremos definir una clasificación alternativa, teniendo en cuenta el grado de intencionalidad de la amenaza:

- Accidentes: averías del hardware y fallos del software, incendio, inundación, etc.
- Errores: errores de actualización, de explotación, de ejecución de determinados procedimientos, etc.
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc.

Para (Royer, 2004) las amenazas que pesan sobre la empresa son de naturaleza múltiple y se encuentran en constante evolución.
El dominio cubierto por la seguridad, es muy amplio y la define como la protección contra todos los daños sufridos y causados por la herramienta informática y originada por el acto voluntario y de mala fe de un individuo.

Antes de implementar una política de seguridad, es indispensable preguntarse qué nivel de seguridad necesitamos. En efecto, la implementación de medidas de seguridad implica a menudo consecuencias ligadas a:

- Restricciones para los usuarios, que deberán autenticarse antes de acceder a algunos recursos.
- La carga financiera que representa la adquisición de los programas de protección.
- El tiempo de trabajo necesario para implementar estas soluciones.
- Una mayor complejidad de la infraestructura.

Estas amenazas se clasifican en tres tipos de amenazas las cuales son:

- **Amenaza natural**
- **Amenaza accidental**
- **Amenaza deliberada**

Las categorías generales de amenazas o ataques son las siguientes:

- Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- Intercepción: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

Para (Vieites, 2006), una vulnerabilidad es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarles daño y producirles pérdidas en la organización.

Vulnerabilidad: Es el acontecimiento que se puede dar entre la amenaza y el activo, es decir que la vulnerabilidad es la condición que nace de la amenaza y va directo al activo.
Riesgo: Es la probabilidad que se concrete una amenaza dado a que la vulnerabilidad existe y el riesgo es alto (probabilidad que se roben información) (alta probabilidad que aumente el caudal e inunde mi casa).

1.7 IMPACTOS Y RIESGOS

Para (Vieites, 2006), el impacto es la medición y valoración del daño que podría producir a la organización un incidente de seguridad.

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles. En este sentido podría resultar de gran ayuda la realización de entrevistas en profundidad con los responsables de cada departamento, función o proceso de negocio, tratando de determinar cuál es el impacto real de la revelación, alteración o perdida de la información para la organización, y no solo del elemento TIC (Tecnología de la Información y Comunicación) que la soporta.

Para (E., 2006), utilizar una computadora es peligroso. Sin embargo, millones de personas alrededor del mundo trabajan con una computadora, hacen sus compras desde una computadora y hasta consiguen pareja a través de ella. Lo primero que hay que decir es que el uso diario de computadoras no representa un peligro en sí mismo. Si es cierto que existen, y ya de ahí la preocupación, muchísimos riesgos de los cuales los usuarios deben cuidarse para no encontrarse desamparado mediante un ataque inesperado. Estos riesgos pueden ser minimizados con ayuda de programas especialmente diseñados para combatir los ataques.

(Vieites, 2006), considera un riesgo como la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

El nivel de riesgo depende, por lo tanto, del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que estas puedan tener en el funcionamiento de la organización.

La organización debería evaluar el nivel de riesgo atendiendo a la frecuencia de materialización de las amenazas y al nivel de impacto causado en el negocio.

Se muestra un ejemplo de algunos riesgos e impactos que pueden llegar afectar a las organizaciones si no se toman medidas preventivas para evitarlos.

RIESGOS	IMPACTOS
Riesgo de acceso o seguridad	Pérdida de rentabilidad del negocio
Riesgo de disponibilidad	Pérdidas financieras
Riesgo de infraestructura	Falta de capacidad para alcanzar los objetivos de negocio
Riesgo de integridad	Pérdida de reputación
Riesgo de proyectos de TI	Desventaja competitiva
Riesgo de inversión o costo	Problemas con los reguladores

Tabla 3: Impactos y Riesgos (Vieites, 2006).

1.8 DEFENSAS SALVAGUARDAS O MEDIDAS DE SEGURIDAD

Para (Vieites, 2006) una defensa, salvaguardas o medidas de seguridad es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto de la organización.

Una medida de seguridad activa es cualquier medida utilizada para anular o reducir el riesgo de una amenaza. Las medidas activas podrían, a su vez, clasificarse en medidas de prevención y medidas de detección.

Una medida de seguridad pasiva es cualquier medida empleada para reducir el impacto cuando se produzca un incidente de seguridad. Por ello a las medidas pasivas también se les conoce como medidas de corrección.

Algunos ejemplos de medidas preventivas son: la autenticación de usuarios, el control de acceso a los recursos, la encriptación de datos sensibles, la formación de los usuarios, etc. Entre las medidas detectivas se encuentran los sistemas de detección de intrusos o las herramientas y procedimientos para el análisis de los "logs". Por último, como medidas correctivas se podrían considerar las copias de seguridad, el plan de respuesta a incidentes y de continuidad del negocio, etc.

Se pueden distinguir entre defensas físicas y defensas lógicas. Las primeras se refieren a medidas que implican el control de acceso físico a los recurso y de las condiciones ambientales en que tienen que ser utilizados. Mientras que las segundas se encuentran relacionadas con la protección conseguida mediante distinta herramientas y técnicas informáticas: autenticación de usuarios, control de acceso a los ficheros, encriptación de los datos sensibles, etc.

1.8.1 Controles de seguridad

(Francisco, 2009) La seguridad computacional a menudo se divide en tres categorías maestras distintas, comúnmente llamadas controles:

- Físico
- Técnico
- Administrativo

Estas tres amplias categorías definen los objetivos principales de una implementación de seguridad apropiada. Dentro de estos controles hay subcategorías que detallan aún más los controles y como estos se implementan.

Controles físicos

El control físico es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. Ejemplos de los controles físicos son:

- Cámaras de circuito cerrado
- Sistemas de alarmas térmicos o de movimiento
- Guardias de seguridad
- Identificación con fotos
- Puertas de acero con seguros especiales
- Biométrica (incluye huellas digitales, voz, rostro, iris, escritura a mano y otros métodos automatizados utilizados para reconocer individuos)

Controles técnicos

Los controles técnicos utilizan la tecnología como una base para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red. Los controles técnicos son mucho más extensos en su ámbito e incluyen tecnologías tales como:

- Encriptación
- Tarjetas inteligentes
- Autenticación a nivel de la red
- Listas de control de acceso (ACLs)
- Software de auditoría de integridad de archivos

Controles administrativos

Los controles administrativos definen los factores humanos de la seguridad. Incluye todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso a qué recursos e información usando medios tales como:

- Entrenamiento y conocimiento
- Planes de recuperación y preparación para desastres
- Estrategias de selección de personal y separación
- Registro y contabilidad de personal

Sniffer

Según (Francisco, 2009), un sniffer es un programa que captura todos los datos que pasan a través de una tarjeta de red y se basa en un defecto del protocolo Ethernet. En este protocolo los ordenadores de la red, aceptan el paquete o no, según vaya dirigido a ellos o no. Lo que hace el sniffer es poner la tarjeta en modo promiscuo (promiscuous mode). El modo promiscuo significa que la tarjeta capturara todos los paquetes Ethernet, aunque no vayan dirigidos a ella.

También se encarga de monitorizar y analizar el tráfico en una red de computadoras, detectando los cuellos de botella y problemas que existan. Ya que puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red.

Gran cantidad de tráfico confidencial viaja en claro, sin ningún tipo de cifrado, por las redes de la mayoría de las empresas. Ese es el entorno ideal para un sniffer, que puede acceder de forma transparente a esa información, y permitir que alguien abuse de su conocimiento. Por eso es muy importante realizar búsquedas periódicas de sniffers dentro de las redes de cualquier empresa, no sólo por el daño que puedan causar, sino también porque encontrarlos es señal de que se ha producido y explotado una grave brecha y hay que tomar medidas inmediatas.

Existen diferentes pruebas que se realizan cuyo objetivo tratan de conseguir es que la máquina que tiene la tarjeta de red en modo promiscuo se traicione a sí misma, revelando que ha tenido acceso a información que no iba dirigida a ella y que, por tanto, tiene un sniffer. Éste es un objetivo ambicioso y complejo que puede resultar imposible.

Cortafuegos

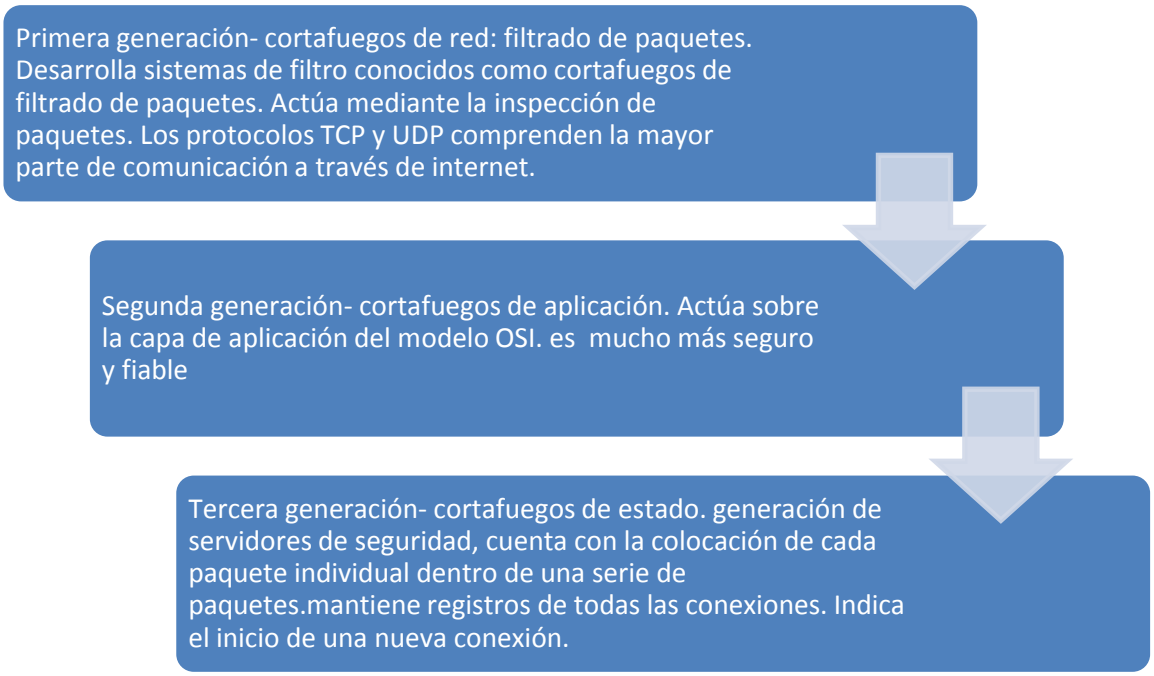
(Falcon, 2006) Comenta que un cortafuego es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. También es frecuente conectar al cortafuegos a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un Firewall funciona definiendo una serie de autorizaciones para la comunicación, tanto de entrada como de salida, mediante Reglas. Estas reglas se pueden hacer teniendo en cuenta los puertos de comunicación, los programas o las IP de conexión. Estas reglas pueden ser tanto restrictivas como permisivas, es decir, pueden ser reglas que denieguen o autoricen

las comunicaciones (de entrada, de salida o ambas) a un determinado puerto, un determinado programa o una determinada IP.

Generaciones de cortafuegos



1.9 EVALUACION DE RIESGOS

Se trata de identificar los riesgos, cuantificar su probabilidad e impacto, y analizar medidas que los eliminen lo que generalmente no es posible o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

Es necesario revisar si se han considerado las amenazas, o bien evaluarlas si es el objetivo, y de todo tipo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a : personas, datos, programas, redes, instalaciones, u otros activos, y llegar suponer un peor servicio a usuarios internos y externos estos normalmente clientes, imagen degradada u otros difícilmente cuantificables, e incluso perdida irreversible de datos y hasta el fin de la actividad de la entidad en los casos graves.

La protección no ha de basarse solo en dispositivos y medios físicos, sino en formación e información adecuada al personal.

El factor humano es el principal a considerar, salvo en algunas situaciones de protección física muy automatizados, ya que es muy crítico; si las personas no quieren colaborar de poco sirven los medios y dispositivos aunque sean caros y sofisticados.
Una vez identificados y medidos los riesgos, lo mejor sería poder eliminarlos, pero como se indica, normalmente lo más se consigue es disminuir la probabilidad de que algo se produzca o bien su impacto: con sistemas de detección de extinción, mediante revisiones periódicas, copiando archivos críticos, exigiendo una contraseña u otros controles según los casos.

1.10 AUDITORIA INFORMATICA

Auditoria. Concepto
La palabra de auditoría proviene del latín auditorius, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír. La Informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. A finales del siglo XX, los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los sistemas de la información de la empresa. El concepto de auditoría es mucho más que esto.

Para (Peso, 2001) la auditoría consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar con las condiciones que le han sido prescritas. Es una función que se acomete a posterior, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

(Gómez, 2007), comenta que el concepto de auditoría es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc. La Informática hoy, está dentro de la gestión integral de la empresa, y por eso, las normas y estándares propiamente informáticos deben estar, sometidos a los generales de la misma.

Para (Elinos, 2011) La Auditoría Informática es aquella que tiene como objetivo principal la evaluación de los controles internos en el área de PED (Procesamiento Electrónico de Datos) que tiene como objetivos evaluar los controles de la función informática, analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente.

Los objetivos de la auditoría son para mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que sustenta. El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de ésta, también ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas.

En la auditoría extrema se trata de saber si la entidad a través de funciones como administración de la seguridad, auditoría interna otras si las anteriores no existieran a evaluado de forma adecuada los riesgos, si los informes han llegado a los destinatarios correspondientes y si están tomando las medidas pertinentes. En este caso se debe considerar la metodología que se sigue para evaluar los riesgos más que las herramientas.
Al hablar de la seguridad siempre se habla en sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información, y algunos controles van más dirigidos a tratar de garantizar algunas de estas características.
La confidencialidad: se cumple cuando solo las personas autorizadas pueden conocer los datos o la información correspondiente.
La integridad: consiste en que solo los usuarios autorizados pueden variar los datos. Deben quedar pistas para control posterior y para auditoría.
La disponibilidad: se alcanza si las personas autorizadas pueden acceder a tiempo a la información a las que estén autorizadas.
Deben existir además autenticidad: que los datos o información sean atenticos, introducidos o comunicados por usuarios auténticos y con las autorizaciones necesarias.

Fases de la auditoría de la seguridad

- Concreción de los objetos y delimitación del alcance y profundidad de la auditoría, así como del periodo cubierto en su caso, por ejemplo revisión de accesos del último trimestre; si no se especifica, los auditores deberán citar en el informe el periodo revisado, porque podría aparecer alguna anomalía anterior.
- Análisis de posibles fuentes y recopilación de información: en el caso de los internos este proceso puede no existir.
- Determinación del plan de trabajo y de los recursos y plazos en caso necesario, así como de comunicación a la entidad.
- Adaptación de cuestionarios y consideración de herramientas o perfiles de especialistas necesarios, sobre todo en la auditoría externa.
- Realización de entrevistas y pruebas.
- Análisis de resultados y valoración de riesgos.
- Presentación y discusión del informe provisional.
- Informe definitivo.

- Anexo al informe
- Carpeta de evidencias
- Seguimiento de las modificaciones acordadas

Estructura del informe definitivo:

El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

Definición de objetivos y alcance de la auditoría.

Enumeración de temas considerados:

- Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.

Cuerpo expositivo:

- Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
- Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- Puntos débiles y amenazas.
- Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
- Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes.

La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.

- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

- El hecho debe poder ser sometido a cambios.
- Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
- No deben existir alternativas viables que superen al cambio propuesto.
- La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:
Hecho encontrado.

- Ha de ser relevante para el auditor y para el cliente.
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

Consecuencias del hecho

- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

Repercusión del hecho

- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

Conclusión del hecho

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

Recomendación del auditor informático

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe definitivo:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.
Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.
La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

Procedimientos
(Rivas, 1988) Refiere que el elemento esencial de la auditoría se fundamenta y justifica por medio de unos procedimientos específicos a proporcionar una seguridad razonable de lo

que se afirma. Cada clase o tipo de auditoría posee sus propios procedimientos para alcanzar el fin previsto aun cuando puedan en muchos casos coincidir. Se pretende garantizar que se toman en consideración todos los aspectos, áreas, elementos, operaciones, circunstancias, etc. que sean significativas.
Para ello se establecen procedimientos que son:

- El trabajo se planificará apropiadamente y se supervisará adecuadamente.
- Se estudiará y evaluará el sistema de control interno.
- Se obtendrá evidencia suficiente y adecuada.

Se establece que la evidencia obtenida deberá recogerse en los papeles de trabajo de auditor como justificación y soporte del trabajo efectuado y la opinión expresada.
Estas tres normas se deducen de la situación real actual de los riesgos que ha de afrontar el auditor.

Los controles establecidos por la entidad auditada pudieran permitir que se produjerán irregularidades, potencialmente significativas, casuales o voluntarias.
Al no someterse a revisión todas y cada una de la operaciones, cabe la posibilidad que se escape a la atención al auditor alguna de aquellas irregularidades.

Variación del objeto

Es innegable que con mayor o menor profundidad la gestión de las entidades ha experimentado un cambio sustancial y hoy, salvo casos dignos del Guinnes, se utiliza la TI (Tecnología de la Información) en todo proceso.
Se ha introducido un nuevo elemento cualitativo en el objeto de la auditoría, el uso de la informática como factor consustancial a la gestión, con la introducción de la Tecnología de la Información (TI) en los sistemas, muy probablemente basada en las ventajas que aporta la información con respecto al trabajo manual, entre las que según (Martin, 2006), se podrían distinguir.

VENTAJAS DE LA INFORMACION		
INFORMACION	HUMANO	COMPUTADOR
Costo de explotación	Alto	Bajo
Costo de operación	Alto	Bajo
Rendimiento continuado	Disminuye	Constante
Consistencia	Poca	Excelente
Capacidad de calculo	Buena	Pobre
Reacción ante lo inesperado	Buena	Pobre

Sentido común	Excelente	Pobre
Lenguaje	Bueno	Pobre

Tabla 4: Variación del objeto (Martin, 2006).

La propia TI incide en los procedimientos que el auditor ha de aplicar proporciona paralelamente medios de ejecutarlos de forma eficiente y directa. Las CAATS (Técnicas de auditoría asistidas por computador) ponen a disposición del auditor una amplia variedad de herramientas que no solo visualizan los nuevos procedimientos si no que mejoran sensiblemente su aplicación y amplían la gama disponible.
La introducción de las TI en los sistemas de información afecta a los auditores de una forma dual:

- Cambia el soporte del objeto de su actividad
- Posibilita la utilización de medios informatizados (CAATs) para la realización de sus procedimientos.

Consultoría. Concepto

Para (Peso, 2001), consiste en "dar asesoramiento o consejo sobre lo que ha de hacer o como llevar adecuadamente una determinada actividad para obtener los fines deseados".

Los elementos de la consultoría podrían resumirse en:

ELEMENTOS DE CONSULTORIA	
Contenido	Dar asesoramiento o consejo
Condición	De carácter especializado
Justificación	En base a un examen o análisis
Objeto	Establecerlos específicamente
Finalidad	Establecer la manera de llevarla a cabo adecuadamente

Tabla 5: Elementos de consultoría (Peso, 2001).

La auditoría verifica a posterior si estas condiciones, una vez realizada esta función o actividad, se cumplen y los resultados pretendidos se obtienen realmente.
Tipos o clases de auditorías:

CLASES DE AUDITORIAS			
CLASE	**CONTENIDO**	**OBJETIVO**	**FINALIDAD**
Financiera	Asesoramiento	Planes de cuentas y procedimientos administrativos	Diseño e implementación
Informática	Asesoramiento	Aplicaciones y planes de contingencia	Desarrollo, diseño e implementación

Tabla 6: Clases de auditoría

La auditoría informática debe realizarse dentro del marco de la auditoría general. El cometido de la auditoría informática se puede dividir en:

- Un estudio del sistema y un análisis de los controles organizativos y operativos del departamento de informática.
- Una investigación y análisis de los sistemas de aplicación que se estén desarrollando o que ya estén implantados.
- La realización de auditorías de datos reales y de resultados de los sistemas que se estén utilizando.
- La realización de auditorías de eficiencia y eficacia.

(Ramos M. Á., 2008)define la auditoría informática como la revisión de la propia informática y de su entorno y desglosa sin carácter exhaustivo que las actividades a que da lugar esta definición puedan ser:

- Análisis de riesgos.
- Planes de contingencia.
- Desarrollo de aplicaciones.
- Asesoramiento en paquetes de seguridad.
- Revisión de controles y cumplimiento de los mismos, así como de las normas legales aplicables.
- Evaluación de la gestión de los recursos informáticos

1.11 METODOLOGIAS DE CONTROL INTERNO, SEGURIDAD Y AUDITORIA INFORMATICA

Introducciones a las metodologías

(Peso, 2001), Comentan que cualquier proceso científico debe estar sujetos a una disciplina de proceso definida con anterioridad se llamara metodología.

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de "acierto/error".

Una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo.

La proliferación de metodologías en el mundo de la auditoría y el control informático se pueden observar en los primeros años de la década de los ochenta paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas. Una de ellas es la seguridad de los sistemas de información.

Aunque de forma simplista se trata de identificar la seguridad informática a la seguridad lógica de los sistemas, nada esta mas lejos de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos para la informática.

Si definimos la seguridad de información como la doctrina que trata de los riesgos informáticos o creados por la informática entonces la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

El nivel de seguridad en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger la información de la entidad y sus medios de proceso.

La informática crea unos riesgos de los que hay que proteger y preservar a la entidad con un entramado de contramedida, y la calidad y la eficacia de las mismas es el objeto a evaluar para poder identificar así sus puntos débiles y mejorarlos.

Los factores de una contramedida son:

- La normativa debe definirse de forma clara y precisa todo lo que debe existir y ser cumplido, tanto desde el punto de vista conceptual, como practico, desde lo general a lo particular. Debe inspirarse en estándares, políticas, marco jurídico, políticas y normas de empresa, experiencia y práctica profesional.
- la organización la integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa.
- Las metodologías son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.
- Los objetivos de control son los objetivos a cumplir en el control de procesos.
- Los procedimientos de control son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución

de uno o varios objetivos de control y, por tanto, deben estar documentados y aprobados por la dirección.

- Dentro de la tecnología de seguridad están todos los elementos, ya sean hardware o software, que ayudan a controlar un riesgo informático. Dentro de este concepto están los cifradores, autentificadores, equipos "tolerantes del fallo", las herramientas de control etc.
- Las herramientas de control son elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objeto de control.
- Llamaremos plan de seguridad a una estrategia planificada de acciones y productos que lleven a un sistema de información y sus centros de proceso de una situación inicial determinada a una situación mejorada.

1.11.1 Las metodologías de auditoría informática

(Peso, 2001), Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: las auditorias de controles generales como producto estándar de auditores profesionales, que son una homologación de las mismas a nivel internacional, y las metodologías de los auditores internos.
El objetivo de las auditorias de controles generales es dar una opinión sobre la finalidad de los datos del computador para la auditoría.
La auditoría debe demostrar con pruebas todas sus afirmaciones, y por ello siempre debe contener al apartado de pruebas, llegando al extremo de que hay auditorias que se basan solo en pruebas como la auditoría de integridad.
La metodología de auditor interno debe ser diseñada y desarrollada por el propio auditor, y esta será la significación de su grado de experiencia y habilidad.
Entre las dos metodologías de evaluación de sistemas de análisis de riesgos y auditoría existen similitudes y grandes diferencias. Ambas tienen papeles de trabajo obtenidos del trabajo de campo tras el plan de entrevistas, pero los cuestionarios son totalmente distintos.
El auditor interno debe de crear sus metodologías necesarias para auditar los distintos aspectos o áreas que defina en el plan auditor.

El plan auditor

(Peso, 2001) Comenta que el auditor elabora un documento en el que se debe escribir todo sobre su función y el trabajo que realiza en la entidad.

Las partes de un plan auditor deben ser al menos las siguientes:

- Funciones. Ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la informática y de control interno informático,

y este debe ser auditado también. Deben escribirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.

- Procedimientos. Para las distintas tareas de las auditorias. Entre ellos están el procedimiento de apertura, el de entrega de discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción del informe final, etc.
- Tipos de auditoría que realiza, metodologías y cuestionarios de las mismas. Existen dos tipos de auditorías según su alcance: la full o completa de una área, la Corrective Action Review (CAR) que es la comprobación de acciones correctivas de auditorías anteriores.
- Sistema de evaluación y los distintos aspectos que evalúa. Independiente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc. Así como realizar una evaluación global de resumen para toda la auditoría.
- Nivel de exposición. Significa la suma de factores como impacto, peso del área, situación de control en el área. Se puede incluso rebajar el nivel de un área auditada porque está muy bien y no merece la pena revisarla tanto a menudo.

    - Lista de distribución de informes.
    - Seguimiento de las acciones correctoras.
    - Plan quincenal.
    - Plan de trabajo anual

Las metodologías de auditoría informática son del tipo cualitativo/subjetivo. Están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas que exigen una gran profesionalidad y forma continuada.

1.12 PRINCIPALES AREAS DE LA AUDITORIA INFORMATICA

Para (Peso, 2001) La función de auditoría informática se aplica en diferentes entornos o áreas, cada una de las cuales tiene sus propios objetivos y estándares de aplicación, estas áreas son:

- La Auditoría física
- Auditoría de la Ofimática
- Auditoría de la Dirección
- Auditoría de la Explotación

- Auditoría del Desarrollo.
- Auditoría del Mantenimiento.
- Auditoría de Bases de datos.
- La auditoría de Técnica de Sistemas.
- Auditoría de la calidad.
- Auditoría de la Seguridad.
- Auditoría de Redes.
- Auditoría de Aplicaciones.

Estas áreas deben estar sometidas a un exigente control interno, además del disparo de los costos, podrá producirse la insatisfacción del usuario. Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Auditoría de la seguridad

Áreas que puede cubrir la auditoría de la seguridad

- Lo que hemos denominado controles directivos, es decir los fundamentos de la seguridad: políticas, planes, funciones, existencia y funcionamiento de algún comité relacionado, objetivos de control, presupuesto, así como existen sistemas y métodos de evaluación periódica de riesgos.
- El desarrollo de las políticas: procedimientos, posibles estándares, normas y guías, sin ser suficiente que existan estas últimas.
- Amenazas físicas externas: inundaciones, incendios, explosiones, costo de líneas o de suministros, terremotos, terrorismo, huelgas.
- Control de acceso adecuado, tanto físicos como los denominados lógicos, para que cada usuario pueda acceder a los recursos a que este autorizado y realizar solo las funciones permitidas: lectura, variación, ejecución, borrado, copia, y quedando las pistas necesarias para control y auditoría, tanto en determinados casos.
- Protección de los datos: lo que fije la LOPD (Ley Orgánica de Protección de Datos) en cuanto los datos de carácter personal bajo tratamiento autorizado, y otros controles en cuanto a los datos en general, según clasificación que exista, la designación de propietarios y los riesgos a que estén sometidos.
- Comunicaciones y redes: topología y tipos de comunicaciones, posible uso de cifrado, protección antivirus, estar en sistemas aislados aunque el impacto será menor que en una red.
- El entorno de producción, entendido como tal explotación mas técnica de sistemas, y con especial énfasis en el cumplimiento de contratos en lo que se refiera a protecciones, tanto respecto a terceros cuando se trata de una entidad que presta

servicios, como el servicio recibido de otros, y de forma especial en el caso de la subcontratación total u outsourcing.

- La continuidad de las operaciones.

1.13 CLASIFICACION DE AUDITORIAS EN LA SEGURIDAD DE DATOS

AUDITORIA DE LA SEGURIDAD FÍSICA

Para (Kendall, Analisis y diseño de sistemas, 2005) Se evaluaran las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y habrá que considerar a las persona; 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.

Las amenazas pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidente de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores, negligencias, huelgas, epidemias o intoxicaciones.

Desde la perspectiva de las protecciones físicas algunos aspectos a considerar son:

- Ubicación del centro de procesos
- Estructura, diseño, construcción y distribución de edificios.
- Amenazas de fuego, riesgos por agua, problemas por el suministro eléctrico.
- Controles tanto preventivos como de detección relacionada con los puntos anteriores.
- Además del acceso, en determinados edificios o áreas debe controlarse el contenido de carteras, paquetes, bolsos o cajas, ya que podrían contener explosivos, así como de lo que se quiere sacar del edificio.
- Protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte, además de otras protecciones no físicas, todo bajo un sistema de inventario.

AUDITORIA DE LA SEGURIDAD LÓGICA

Es necesario verificar que cada usuario solo pueda acceder a los recursos a los que autorice el propietario, aunque sea de forma genérica, según su función y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución, traslados a los sistemas lo que representaríamos en una matriz de accesos en la que figuran los sujetos: grupos de usuarios o sistemas, los objetos que pueden ser accedidos con mayor o menor granularidad: un disco, una aplicación, una base de datos, una librería de programas, un tipo

de transacción, un programa, las posibilidades que se le otorgan lectura, modificación, borrado y ejecución.
En cuanto a la 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.
Aspectos a evaluar respecto a las contraseñas:

- Asignación de contraseñas
- Longitud
- Vigencia
- Control para no asignar "x" ultimas.
- Números de intentos permitidos al usuario.
- Contraseñas cifradas.
- Protección o cambio de contraseñas.
- Controles existentes para evitar y detectar caballos de troya.
- La no cesión, y el uso individual y responsable de cada usuario.

1.14 APLICACIONES EN APOYO A LA SEGURIDAD INFORMATICA

Los motivos por los que puede ser necesaria una auditoría informática mediante un software en una empresa pueden ser de lo más común, desde un simple control rutinario como parte del cumplimiento del control, pasando por una actividad programada como política de la organización o por un peritaje en busca de anormalidades en la empresa.

Algunos tipos de software utilizados para la realización de auditorías informáticas pueden ser:

- Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.
- El software MEYCOR COBIT (CSA) ha sido desarrollado por DATASEC y constituye una herramienta con características únicas a nivel mundial, ya que en su versión actual, se encuentran incorporados estándares mundiales como el marco COBIT 4.1 Esto constituye un elemento diferenciador, MEYCOR COBIT (CSA) no

sólo sirve para realizar un diagnóstico de la situación actual y generación de recomendaciones, sino que permite realizar evaluaciones periódicas, las cuales pueden ser comparadas entre sí para medir los avances alcanzados de un período a otro. En la última versión de MEYCOR-AUDIT COBIT (CSA). La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado.

- Statistical Package for the Social Sciences (SPSS) es un programa estadístico informático muy usado en las ciencias sociales y las empresas de investigación de mercado. En la actualidad, la sigla se usa tanto para designar el programa estadístico como la empresa que lo produce. Como programa estadístico es muy popular su uso debido a la capacidad de trabajar con bases de datos de gran tamaño. Además, de permitir la recodificación de las variables y registros según las necesidades del usuario. El programa consiste en un módulo base y módulos anexos que se han ido actualizando constantemente con nuevos procedimientos estadísticos. Cada uno de estos módulos se compra por separado. Actualmente, compite no sólo con softwares licenciados como lo son SAS, MATLAB, Statistica, Stata, sino también con software de código abierto y libre, de los cuales el más destacado es el Lenguaje R. Recientemente ha sido desarrollado un paquete libre llamado PSPP, con una interfaz llamada PSPPire que ha sido compilada para diversos sistemas operativos como Linux, además de versiones para Windows y OS X. Este último paquete pretende ser un clon de código abierto que emule todas las posibilidades del SPSS.

1.15 INSTRUMENTOS Y METODOLOGIAS DE EVALUACION

Las metodologías son necesarias para desarrollar cualquier proyecto que se proponga de manera ordenada y eficaz.

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.

Se menciona algunos tipos de instrumentos de metodologías de evaluación como son los siguientes:

- Entrevista
- Sondeos

- Checklist o cuestionarios

Un instrumento de la metodología de evaluación muy importante en la auditoría de seguridad son los cuestionarios ya que a través de este instrumento de investigación. Se utiliza, en el desarrollo de una auditoría ya que es una técnica ampliamente aplicada en la investigación del auditor de carácter cualitativa, para poder obtener resultados acerca de la información de una empresa. No obstante lo anterior, su construcción, aplicación y tabulación poseen un alto grado científico y objetivo. Elaborar un Cuestionario válido no es una cuestión fácil; implica controlar una serie de variables.

1.16 ENTREVISTA

Kendall y Kendall (2005), menciona los cinco pasos para preparar una entrevista los cuales son; Leer los antecedentes, leer y entender tanto como sea posible los antecedentes de los entrevistados y su organización. Con frecuencia este material se puede obtener del sitio web corporativo, de un informe actual o anual, de un boletín corporativo o de cualquier publicación que explique el estado de la organización. Otra ventaja de su organización es investigar su organización es maximizar el tiempo que invierta en las entrevistas; sin esta preparación podría perder tiempo haciendo preguntas generales sobre los antecedentes.
Establecer objetivos de la entrevista, utilice los antecedentes que haya recopilado así como su propia experiencia para establecer los objetivos de la entrevista. Debe de haber de cuatro a seis áreas clave referentes al procesamiento de información y el comportamiento relacionado con la toma de decisiones acerca de las cuales tendrá usted que hacer preguntas. Estar áreas incluye fuentes de información, formatos de información, frecuencia de la toma de decisiones, cualidades de la información y estilo de la toma de decisiones.
Decidir a quién entrevistar, cuando tenga a quien decidir entrevistar, incluya a gente clave de todos los niveles que vayan a ser afectadas por el sistema de alguna manera.
Preparar al entrevistado, prepare a la persona que va ser entrevistada hablándole por anticipado o enviándole un mensaje de correo electrónico y dándole tiempo para pensar en la entrevista. Debido a que con la entrevista se pretende satisfacer muchos objetivos normalmente esta se debe realizar en persona y no por correo electrónico. Las entrevistas se deben llevar a cabo en 45 minutos o en una hora a lo mucho.
Decidir el tiempo de preguntas y la estructura, escriba preguntas que abarquen las áreas clave de la toma de decisiones que haya descubierto al terminar los objetivos de la entrevista. Las técnicas apropiadas para preguntar son el corazón de la entrevista. Las preguntas tienen formas básicas que usted debe de conocer, los dos tipos de preguntas son

las abiertas y cerradas. Es posible estructurar su entrevista de tres modos distintos: una estructura de pirámide, una estructura de embudo o una estructura de diamante.

1.16.1 Tipos de preguntas

La diferencia más importante entre las preguntas que se utilizan para la mayoría de las entrevistas y aquellas usadas en los cuestionarios es que las entrevistas permiten la interacción entre las preguntas y sus significados. En una entrevista el analista tiene la oportunidad de refinar una pregunta, definir un término confuso, cambiar el curso de las preguntas, responder a una mirada desconcertada y controlar generalmente el contexto.
En un cuestionario sólo se pueden aprovechar algunas de estas oportunidades. Por lo tanto, para el analista, las preguntas deben tener suficiente claridad, el flujo del cuestionario debe ser convincente, las preguntas de los encuestados deben anticiparse y la aplicación del cuestionario debe planearse en detalle.
Los tipos básicos de preguntas que se utilizan en los cuestionarios son las abiertas y las cerradas, al igual que en las entrevistas. Debido a las limitaciones propias de los cuestionarios, se justifica una explicación adicional de los tipos de preguntas de éstos.
Las preguntas abiertas son particularmente adecuadas para situaciones en que usted desea descubrir las opiniones de miembros de la organización sobre algún aspecto del sistema, ya sea un producto o un proceso. Estas preguntas incluyen aquellas como ¿Qué piensa de poner a todos los gerentes en una intranet? Y explique por favor como toma una decisión de programación de producción. Considere el término abiertas. En realidad abierta describe las opciones del entrevistado para responder. Están abiertas. La respuesta puede ser de dos palabras o dos párrafos, dependiendo que tan extensa sea.
Las ventajas de utilizar las preguntas abiertas son muchas e incluyen las siguientes:

- Hacen que el entrevistado se sienta a gusto.
- Permiten al entrevistador entender el vocabulario del entrevistado, el cual refleja una pregunta cerrada limita la respuesta disponible para el entrevistado. Le dan una pregunta y cinco respuestas, pero no le permiten anotar su propia respuesta y aún así se espera que conteste la pregunta correctamente.

Un tipo especial de pregunta cerrada es la pregunta bipolar. Este tipo de pregunta limita aún más las opciones del entrevistado pues sólo le permite una opción en cada polo, como sí o no, verdadero o falso, de acuerdo o desacuerdo.

Las ventajas de utilizar preguntas cerradas de cualquiera de los dos tipos incluyen lo siguiente:

- Ahorrar tiempo.
- Comparar las entrevistas fácilmente.
- Ir al grano.
- Mantener el control durante la entrevista.
- Cubrir terreno rápidamente.
- Conseguir datos relevantes.

Sin embargo, las desventajas de utilizar preguntas cerradas son considerables. Dichas desventajas
Incluyen lo siguiente:

- Aburren al entrevistado.
- No permiten obtener gran cantidad de detalles debido a que el entrevistador proporciona el marco de referencia para el entrevistado.
- Olvidar las ideas principales por la razón anterior.
- No ayudan a forjar una relación cercana entre el entrevistador y el entrevistado.

Así, en su calidad de entrevistador, usted debe pensar cuidadosamente los tipos de pregunta que utilizará.
Las preguntas abiertas y cerradas tienen ventajas y desventajas, Observe que al elegir un tipo de pregunta sobre el otro realmente involucra un intercambio; aunque una pregunta abierta ofrece amplitud y profundidad para la contestación, las respuestas a las preguntas abiertas son difíciles de analizar.

- Abierta
- Baja Confiabilidad de los datos
- Uso eficiente del tiempo
- Cerrada
- Alta

También existen las preguntas abiertas (no estructuradas).En este tipo de preguntas abiertas es el usuario encuestado quien responde con sus propias palabras a la pregunta formulada. Son esenciales para conocer el marco de referencia del encuestado y para redactar después las alternativas a ofrecer en las preguntas cerradas. Por ello resultan oportunas y adecuadas en el caso de estudios exploratorios o preencuestas (encuestas piloto o sondeos previos)

Atributos de las preguntas

- Abierta y cerrada.

- Baja Precisión de los datos
- Mucha Amplitud y profundidad
- Mucha Habilidad requerida del entrevistador
- Difícil Facilidad de análisis
- Educación, valores, actitudes y creencias
- Proporcionan gran cantidad de detalles
- Revelan nuevas líneas de preguntas que pudieron haber pasado desapercibidas
- Hacen más interesante la entrevista para el entrevistado
- Permiten más espontaneidad
- Facilitan la forma de expresarse al entrevistador
- Son un buen recurso si el entrevistador no está preparado para la entrevista

Como puede ver, las preguntas abiertas tienen varias ventajas. Sin embargo, también tienen Muchas desventajas:

- Podrían dar como resultado muchos detalles irrelevantes.
- Posible pérdida del control de la entrevista.
- Permiten respuestas que podrían tomar más tiempo del debido para la cantidad útil de Información obtenida.
- Dan la impresión de que el entrevistador es inexperto.
- Podrían dar la impresión de que el entrevistador "anda de pesca" sin un objetivo real en la entrevista debe considerar con cuidado las implicaciones de utilizar las preguntas abiertas para entrevistar.

Las preguntas cerradas deben usarse cuando el analista de sistemas puede listar eficazmente todas las posibles respuestas a la pregunta y cuando todas las respuestas listadas son mutuamente excluyentes, es decir, que al elegir una se impida la elección de cualquiera de las demás.
Preguntas de respuestas dicotómicas y múltiples: Las primeras constituyen uno de los tipos más básicos de preguntas, al ser éstas fáciles de formular, contestar y tabular. En ellas, la información se subdivide dicotómicamente en dos categorías. Las preguntas de respuestas múltiples se emplean cuando la alternativa de respuesta para la pregunta es superior a dos. Este último tipo de preguntas aseguran que todos los encuestados respondan en la misma dimensión.
Preguntas de escalas de medición de actitudes y respuestas: Las escalas son instrumentos de medida que se basan en la idea de clasificación, aprovechando a la par las propiedades semánticas de las palabras y las características de los números. Existen diferentes tipos que reflejan distintos niveles de medida. No obstante, para medir la percepción de los usuarios

de información contamos con escalas de variables cuantitativas; escalas métricas numéricas y de intervalos y escalas de variables cualitativas distinguimos varios tipos de escalas cualitativas: escalas de categorías detalladas, escalas de valores, escalas de jerárquicas, escalas de importancia, escalas de suma constante, escala Likert, y escala de diferenciales semánticos.

1.17 SONDEOS

Un tercer tipo de pregunta es el sondeo o seguimiento. El sondeo más profundo es el más simple: la pregunta "¿Por qué?" Otros sondeos son "¿Me puede dar un ejemplo?" y "¿Me lo puede explicar con más detalle?" El propósito del sondeo es ir más allá de la respuesta inicial para conseguir mayor significado, clarificar, obtener y ampliar la opinión del entrevistado. Los sondeos pueden constar de preguntas abiertas o cerradas.
El sondeo es fundamental. La mayoría de los entrevistadores principiantes muestran reticencia al uso de los sondeos y, por consiguiente, aceptan respuestas superficiales. Por lo regular agradecen que los empleados les concedan entrevistas y se sienten obligados hasta cierto punto a aceptar cortésmente las respuestas tajantes.

Cómo colocar las preguntas en una secuencia lógica

Así como hay dos formas generalmente reconocidas de razonamiento inductivo y deductivo, también hay dos formas similares de organizar sus entrevistas. Una tercera combina los métodos inductivo y deductivo.
Uso de una estructura de pirámide La organización inductiva de preguntas de la entrevista se puede visualizar como si se tuviera una forma de pirámide. Con base en esta forma, el entrevistador empieza con preguntas, a menudo cerradas, muy detalladas. Posteriormente, el entrevistador extiende los temas permitiendo preguntas abiertas y respuestas más generalizadas.
Debe utilizar una estructura de pirámide si cree que su entrevistado necesita motivación para profundizar en el tema. También es conveniente utilizar una estructura de pirámide para la secuencia de las preguntas cuando desea una opinión concluyente del tema. Tal es el caso de la pregunta final: "En general, ¿qué opina de la seguridad de los datos versus la importancia del acceso a Internet?". Uso de una estructura de embudo En el segundo tipo de estructura, el entrevistador adopta un método deductivo al iniciar con preguntas generales y abiertas, y luego limitar las posibles respuestas utilizando preguntas cerradas. El uso del método de específica estructura de embudo proporciona una forma cómoda y sencilla de empezar una entrevista.

La secuencia de preguntas en forma de embudo también es útil cuando el entrevistado tiene opiniones fuertes acerca del tema y necesita libertad para expresar sus emociones. Uso de una estructura de diamante con frecuencia es mejor una combinación de las dos estructuras anteriores, lo cual da como resultado una estructura de diamante. Esta estructura implica empezar de una manera muy específica, después se examinan los aspectos generales y finalmente se termina con una conclusión muy específica.

El entrevistador empieza con preguntas cerradas sencillas que permiten calentar el proceso de la entrevista. A la mitad de la entrevista, se le pide al entrevistado que dé su opinión sobre temas amplios que obviamente no tienen una respuesta "correcta". Posteriormente, el entrevistador limita de nuevo las preguntas para obtener respuestas específicas, con lo cual propicia, tanto para él como para el entrevistado, una forma de cerrar la entrevista. La estructura de diamante combina las fortalezas de los otros dos métodos, pero tiene la desventaja de tomar mucho más tiempo que cualquiera de las otras estructuras.

El final de la entrevista es un punto apropiado para hacer una pregunta importante: "¿Hay algo que no hayamos tratado y que usted sienta que es importante que yo sepa?" considerada por lo general como una pregunta sistemática por el entrevistado, con frecuencia la respuesta será "No". Sin embargo, a usted le interesan los casos en que esta pregunta supera las trabas y da paso al flujo de muchos datos nuevos.

Al terminar la entrevista, haga un resumen y de retroalimentación sobre sus impresiones generales. Informe al entrevistado qué procede y lo que usted y otros miembros del equipo harán. Pregúntele al entrevistado con quién debe hablar a continuación. Establezca la próxima cita para realizar una entrevista de seguimiento, agradezca al entrevistado por su tiempo y despídase.

Redacción del informe de la entrevista

Aunque la entrevista misma haya concluido, su trabajo de análisis de los datos de ésta apenas comienza. Necesita captar la esencia de la entrevista a través de un informe escrito. Es indispensable que escriba dicho informe lo más pronto posible después de la entrevista. Este paso es otra forma de asegurar la calidad de los datos de la entrevista. Cuanto más tiempo espere para hacer el informe de su entrevista, más dudosa será la calidad de sus datos.

Después de este resumen inicial, entre en mayor detalle, registre los puntos principales de la entrevista y sus propias opiniones. Repase el informe de la entrevista con el entrevistado en una reunión de seguimiento. Este paso le ayuda a clarificar lo que el entrevistado pretendía y le permite a éste saber que usted está bastante interesado en tomarse el tiempo necesario para entender sus puntos de vista y percepciones.

1.18 CHECKLIST O CUESTIONARIOS

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya que someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para el llenado sistemático de sus Cuestionarios, de sus Checklists. Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talento del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar el Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo. Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo

apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

Checklist de rango.

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

Ejemplo de Checklist de rango:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

1: Muy deficiente.
2: Deficiente.
3: Mejorable.
4: Aceptable.
5: Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. El llenado del Checklist no debe realizarse en presencia del auditado.

Para (Kendall, 2005), el uso de cuestionarios es una técnica de recopilación de información que permite a los analistas de sistemas estudiar las actitudes, creencias, comportamiento y características de muchas personas importantes en la organización que podrían resultar afectadas por los sistemas actuales y los propuestos. Las actitudes consisten en lo que las personas de la organización dicen que quieren, las creencias son lo que las personas realmente piensan que es verdad; el comportamiento es lo que los miembros de la organización hacen, y las características son propiedades de las personas o cosas. Es posible cuantificar las respuestas conseguidas a través de cuestionarios (también conocidos como encuestas) que usan preguntas cerradas. Si encuesta personas a través de correo electrónico o la Web, puede utilizar software para convertir las respuestas electrónicas directamente a tablas de datos para análisis mediante una aplicación de hoja de cálculo o paquetes de software estadísticos. Las respuestas a cuestionarios que utilizan preguntas

abiertas se analizan e interpretan de otras maneras. La redacción que utilice el analista de sistemas influye en las respuestas a preguntas sobre actitudes y creencias. Al usar cuestionarios, el analista podría estar buscando cuantificar lo que se haya descubierto en las entrevistas. Además, éstos podrían usarse para determinar qué tan extendido o limitado es en realidad un sentimiento expresado en una entrevista. Por otra parte, los cuestionarios se pueden usar para encuestar a una muestra considerable de usuarios de sistemas con el fin de detectar problemas o poner de manifiesto cuestiones importantes antes de que se realicen las entrevistas.

Hay muchas similitudes entre ambas técnicas, y quizá lo ideal sería usarlas en conjunto, ya sea dando seguimiento en una entrevista a las respuestas confusas del cuestionario o diseñando los cuestionarios con base en lo que se descubra en las entrevistas. Sin embargo, cada técnica tiene sus propias funciones específicas, y no siempre es necesario o conveniente utilizarlas en combinación.

Planeación del uso de cuestionarios

A primera vista los cuestionarios podrían parecer una manera rápida de recopilar grandes cantidades de datos sobre la opinión que los usuarios tienen del sistema actual, sobre los problemas que experimentan con su trabajo y sobre lo que la gente espera de un sistema nuevo o uno modificado. Aunque es cierto que se puede recopilar mucha información a través de los cuestionarios sin invertir tiempo en las entrevistas cara a cara, el desarrollo de un cuestionario útil implica una considerable cantidad de tiempo de planeación. Cuando se decide encuestar a los usuarios por medio del correo electrónico o la Web, enfrenta aspectos de planeación adicionales acerca de la confidencialidad, la autenticación de identidad y problemas de múltiples respuestas (Kendall, Analisis y diseño de sistemas, 2005).

Lo primero que debe usted decidir es qué fines persigue al utilizar una encuesta. Por ejemplo, si desea saber qué porcentaje de usuarios prefiere una página de preguntas frecuentes (FAQ) como un medio de aprender aspectos sobre nuevos paquetes de software, un cuestionario podría ser la técnica correcta. En cambio, si lo que desea es un análisis profundo del proceso de toma de decisiones de un gerente, una entrevista es una mejor opción (Kendall, Analisis y diseño de sistemas, 2005).

A continuación se mencionan algunas directrices que le pueden servir para decidir si es apropiado el uso de cuestionarios. Considere el uso de cuestionarios si:

- Las personas que necesita encuestar se encuentran en ubicaciones dispersas (diferentes instalaciones de la misma corporación).
- Una gran cantidad de personas está involucrada en el proyecto de sistemas, y es importante saber qué proporción de un grupo dado (por ejemplo, los directivos) aprueba o desaprueba una característica específica del proyecto propuesto.

- Está haciendo un estudio preliminar y desea medir la opinión general antes de que se determine el rumbo que tomará el proyecto de sistemas.
- Desea tener la certeza de que en las entrevistas de seguimiento se identificará y abordará cualquier problema relacionado con el sistema actual.

Una vez que haya determinado que tiene buenos motivos para usar un cuestionario y que haya precisado los objetivos que se cumplirán por medio de éste, puede proceder a elaborar las preguntas.
A continuación se menciona algunos lineamientos útiles para la elección del lenguaje del cuestionario:

- Use el lenguaje de los encuestados siempre que sea posible. Utilice una redacción sencilla.
- Esfuércese por ser específico en lugar de divagar en la redacción. También evite las preguntas demasiado específicas.
- Haga preguntas breves.
- No sea condescendiente con los encuestados ni los subestime con opciones de lenguaje de bajo nivel.
- Evite la parcialidad en la redacción. Evitar la parcialidad implica también evitar preguntas ofensivas
- Dirija las preguntas a los encuestados adecuados es decir, aquellos que las puedan responder. No dé por sentado que éstos tendrán demasiado conocimiento.
- Asegúrese de que el aspecto técnico de las preguntas es preciso antes de incluirlas.
- Use software para verificar que el nivel de redacción de las preguntas sea apropiado para los encuestados.

Uso de escalas en los cuestionarios

El escalamiento es el proceso consistente en asignar números u otros símbolos a un atributo o característica con propósitos de medición. Las escalas son a menudo arbitrarias y en algunos casos no son únicas.
Por lo general, los analistas de sistemas utilizan dos diferentes formas de escalas de medición:

- las escalas nominales y
- las escalas de intervalos.

A continuación se relacionan una serie de características para cada escala de medición.

ESCALAS DE MEDICION DE CUESTIONARIOS	
NOMINALES	**INTERVALOS**
Clasifican cosas	Entre cada numero son iguales
Formas de medición mas débiles	Operaciones matemáticas en cuestionarios
obtención de totales para cada clasificación	Representan magnitudes y distancias
Representan categoría o un grupo	Comparaciones de igualdad y desigualdad
Relación de igualdad y desigualdad	Orden entre sus valores

Tabla 7: Escalas de medición de cuestionarios (Kendall, Analisis y diseño de sistemas, 2005).

La validez es el grado en que la pregunta mide lo que el analista pretende medir. Por ejemplo, si el propósito del cuestionario es determinar si la organización está lista para un cambio trascendental en las operaciones por computadora, la confiabilidad mide la consistencia. Si el cuestionario se aplica una vez y a continuación se aplica nuevamente bajo las mismas circunstancias y en ambos casos se obtienen los mismos resultados, se dice que el instrumento tiene consistencia externa. Si el cuestionario contiene apartados y éstos tienen resultados equivalentes, se dice que el instrumento tiene consistencia interna. Ambos tipos de consistencia, la externa y la interna, son importantes. La construcción real de escalas es una tarea seria. La construcción negligente de escalas puede originar alguno de los siguientes problemas:

- Condescendencia.
- Tendencia central.
- Efecto de halo.

La condescendencia, es un problema causado por encuestados que califican a la ligera. Un analista de sistemas puede evitar el problema de la condescendencia moviendo la categoría "promedio" a la izquierda o derecha del centro.
La tendencia central, es un problema que ocurre cuando los encuestados califican todo como promedio. El analista puede mejorar la escala (1) haciendo más pequeñas las diferencias en los dos extremos, (2) ajustando la fuerza de los descriptores o (3) creando una escala con más puntos.
El efecto de halo, es un problema que surge cuando la impresión que se genera en una pregunta influye en la próxima pregunta. Por ejemplo, si usted está evaluando a un empleado sobre quien tiene una impresión muy favorable, podría darle una calificación alta en cada categoría o característica, sin tomar en cuenta si es un punto fuerte del empleado. La solución es poner una característica y varios empleados en cada página, en lugar de un empleado y varias características en una página.

INSTRUMENTOS DE METODOS DE EVALUACION		
INSTRUMENTOS	**VENTAJAS**	**DESVENTAJAS**
SONDEO	Bajo costo, Mayor rapidez en la obtención de resultado, técnica más utilizada y permite obtener información de casi cualquier tipo de población.	Requiere para su diseño de profesionales con buenos conocimientos de teoría, es necesario dar un margen de confiabilidad de los datos.
ENTREVISTA	Se puede llegar a todo público, seguridad de un mayor número de informaciones y flexibilidad en su desarrollo.	Alto costo por persona entrevistada, personas no estén dispuestas a conceder la entrevista, las respuestas del entrevistado dependen del entrevistador.
CUESTIONARIO	Facilitan la recopilación de información, evitan la dispersión de la información y hacen impersonal la aportación de respuestas	Falta de profundidad en las respuestas, se necesita una buena elección del universo y de las muestras utilizadas y la interpretación y el análisis de los datos pueden ser muy simples.

Tabla 8: Instrumentos de métodos de evaluación.

1.18.1 Tipos de indicadores:

Los indicadores son elementos informativos del control de cómo funciona una actividad, pues hacen referencia a parámetros estables que sirven de magnitud de comprobación del funcionamiento de ésta. Son los elementos básicos de las técnicas de control de gestión. La utilidad y fiabilidad del control de gestión se vincula necesariamente a la utilidad y fiabilidad de los indicadores.

Existen tipos de indicadores como:

Estratégicos: La contribución al logro de los objetivos estratégicos en relación con la misión de la unidad responsable.

De gestión: Informan sobre los procesos y funciones clave.

Indicadores de servicio: Miden la calidad con que se genera productos y servicios, en función de estándares, así como del grado de satisfacción de clientes y proveedores.

Escala de medición: es una caracterización de los objetos que se desea medir mediante una variable cuantitativa y una cualitativa.

Escala Nominal: La escala de medida nominal, puede considerarse la escala de nivel más bajo, y consiste en la asignación, puramente arbitraria de números o símbolos a cada una de las diferentes categorías en las cuales podemos dividir el carácter que observamos, sin que puedan establecerse relaciones entre dichas categorías, a no ser el de que cada elemento pueda pertenecer a una y solo una de estas categorías.

Escala Ordinal o de likert:

En caso de que puedan detectarse diversos grados de un atributo o propiedad de un objeto, la medida ordinal es la indicada, puesto que entonces puede recurrirse a la propiedad de "orden" de los números asignándolo a los objetos en estudio de modo que, si la cifra asignada al objeto A es mayor que la de B, puede inferirse que A posee un mayor grado de atributo que B. La asignación de números a las distintas categorías no puede ser completamente arbitraria, debe hacerse atendiendo al orden existente entre éstas.

Escalas de intervalos iguales: La escala de intervalos iguales, está caracterizada por una unidad de medida común y constante que asigna un número igual al número de unidades equivalentes a la de la magnitud que pose. Esta escala, además de poseer las características de la escala ordinal, encontramos que la asignación de los números a los elemento es tan precisa que podemos determinar la magnitud de los intervalos (distancia) entre todos los elementos de la escala. A el elemento observado. Podemos decir que la escala de intervalos es la primera escala verdaderamente cuantitativa y a los caracteres que posean esta escala de medida pueden calculársele todas las medidas estadísticas a excepción del coeficiente de variación.

Escala de coeficientes o Razones:

El nivel de medida más elevado es el de cocientes o razones, y se diferencia de las escalas de intervalos iguales únicamente por poseer un punto cero propio como origen; es decir que el valor cero de esta escala significa ausencia de la magnitud que estamos midiendo. Si se observa una carencia total de propiedad, se dispone de una unidad de medida para el efecto.

1.19 ESCALAMIENTO TIPO LIKERT

(Hernández, 1991) comenta que este método fue desarrollado por Rensis Likert a principios de los treinta; sin embargo, se trata de un enfoque vigente y bastante popularizado. Consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios ante los cuales se pide la reacción de los sujetos a los que se les administra. Es decir, se presenta cada afirmación y se pide al sujeto que externe su reacción eligiendo uno de los cinco puntos de la escala. A cada punto se le asigna un valor numérico. Así, el sujeto obtiene una puntuación respecto a la afirmación y al final se obtiene su puntuación total sumando las puntuaciones obtenidas en relación a todas las afirmaciones.

Asimismo, pueden hacerse distintas combinaciones como "totalmente verdadero" o "completamente no". Y las alternativas de respuesta pueden colocarse;
EJEMPLO

- Muy de acuerdo
- De acuerdo
- Ni de acuerdo, ni en desacuerdo
- En desacuerdo
- Muy en desacuerdo

O bien utilizando recuadros en lugar de paréntesis:

- Definitivamente sí
- Probablemente sí
- Indeciso
- Probablemente no
- Definitivamente no

Es indispensable comentar que el número de categorías de respuesta debe ser el mismo para todas las afirmaciones.

Consideraciones sobre la escala Likert

A veces se acorta o incrementa el número de categorías, sobre todo cuando los respondientes potenciales pueden tener una capacidad muy limitada de discriminación o por el contrario muy amplia.

Como se construye una escala Likert

En términos generales, una escala Likert se construye generando un elevado número de afirmaciones que califiquen al objeto de actitud se administran aun grupo piloto para obtener las puntuaciones del grupo en cada afirmación. Estas puntuaciones se correlacionan con las puntuaciones del grupo a toda la escala (la suma de las puntuaciones de todas las afirmaciones), y las afirmaciones cuyas puntuaciones se correlacionan significativamente con las puntuaciones de toda la escala, se seleccionan para integrar el instrumento de medición. Asimismo, debe calcularse la confiabilidad y validez de la escala.

Maneras de aplicar la escala Likert

Existen dos formas básicas de aplicar una escala Likert. La primera es de manera auto administrada: se le entrega la escala al respondiente y éste marca respecto a cada afirmación, la categoría que mejor describe su reacción o respuesta. Es decir, marcan su respuesta. La segunda forma es la entrevista; un entrevistador lee las afirmaciones y alternativas de respuesta al sujeto y anota lo que éste conteste. Cuando se aplica vía

entrevista, es muy necesario que se le entregue al respondiente una tarjeta donde se muestran las alternativas de respuesta o categorías.
Al construir una escala Likert se debe asegurar que, las afirmaciones y alternativas de respuesta serán comprendidas por los sujetos a los que se les aplicara y que éstos tendrán la capacidad de discriminación requerida. Ello se evalúa cuidadosamente en la prueba piloto.

1.20 DISEÑO Y APLICACION DE CUESTIONARIOS

Muchos de los mismos principios que se aplican al diseño de formularios para la captura de datos también son importantes aquí. A pesar de que el propósito de un cuestionario es recopilar información sobre actitudes, creencias, comportamiento y características cuyo impacto puede alterar sustancialmente el trabajo de los usuarios, los encuestados no siempre muestran interés en responder. Recuerde que, en conjunto, los miembros de una organización a menudo reciben demasiadas encuestas, muchas de las cuales están mal planteadas y son triviales.
Un cuestionario bien diseñado puede ayudar a superar parte de esta reticencia a responder.
A continuación se mencionan algunas reglas para diseñar un buen cuestionario:

- Deje bastante espacio en blanco.
- Proporcione suficiente espacio para escribir las respuestas.
- Facilite a los encuestados que marquen con claridad sus respuestas.
- Mantenga un estilo consistente.

Cuando se diseñan cuestionarios para la Web, se deben aplicar las mismas reglas que utilice al diseñar cuestionarios impresos. La mayoría de los paquetes de software le permiten insertar alguno de los formatos de captura de datos más comunes.
Las cuatro reglas pueden ayudar a conseguir una mejor tasa de respuestas al cuestionario. Por lo que respecta a las preguntas no hay una manera de ordenarlas que se considere como la mejor. Una vez más, conforme ordene las preguntas, debe pensar en los objetivos que persigue con el cuestionario y a continuación determinar la función de cada pregunta en la consecución de sus objetivos. También es importante considerar el cuestionario desde el punto de vista del encuestado. Algunos lineamientos para ordenar las preguntas son:

- Colocar primero las preguntas más importantes para los encuestados.
- Agrupar los elementos de contenido similar.
- Incorporar primero las preguntas menos polémicas.

Se necesita que los encuestados se sientan lo más cómodos e interesados posibles con las preguntas que les haga, sin que los abrume algún tema en particular.

1.20.1 Aplicación de cuestionarios

La decisión sobre quién recibirá el cuestionario se toma en conjunto con la tarea de establecer los objetivos que se persiguen con los resultados del mismo. El muestreo, ayuda al analista de sistemas a determinar la clase de representación que se necesita y el tipo de encuestados que deben recibir el cuestionario a los encuestados.
Los destinatarios a menudo son escogidos como representativos debido a su jerarquía, tiempo de servicio en la compañía, deberes, o interés especial en el sistema actual o propuesto. Asegúrese de incluir suficientes encuestados para conseguir una muestra razonable en caso de que algunos cuestionarios no sean devueltos o algunas hojas de respuestas sean completadas incorrectamente y tengan que desecharse.

Métodos para aplicar el cuestionario

El analista de sistemas tiene varias opciones para aplicar el cuestionario, y el método de administración es a menudo determinado por el estado de la empresa. Entre las opciones para aplicar el cuestionario se encuentran las siguientes:

- Citar al mismo tiempo a todos los encuestados.
- Entregar personalmente los cuestionarios en blanco y recogerlos cuando estén terminados.
- Permitir a los encuestados que llenen el cuestionario por sí mismos en su trabajo y que lo dejen en una caja colocada en algún punto central.
- Mandar por correo los cuestionarios a los empleados de las sucursales e indicarles una fecha límite, instrucciones y enviarles sobres con envío prepagado para que devuelvan los cuestionarios llenos.
- Aplicar el cuestionario a través de correo electrónico o la Web.

Cada uno de estos cinco métodos tiene ventajas y desventajas. El más común es permitir que los encuestados llenen el cuestionario por sí mismos en el momento que lo prefieran. Las tasas de respuesta con este método son un poco más bajas que con los demás métodos, porque la gente olvida el formulario, lo pierde o lo ignora intencionalmente. No obstante, la contestación del cuestionario por parte de los encuestados en el momento que lo prefieran les permite sentir que su anonimato está garantizado y dar como resultado respuestas menos

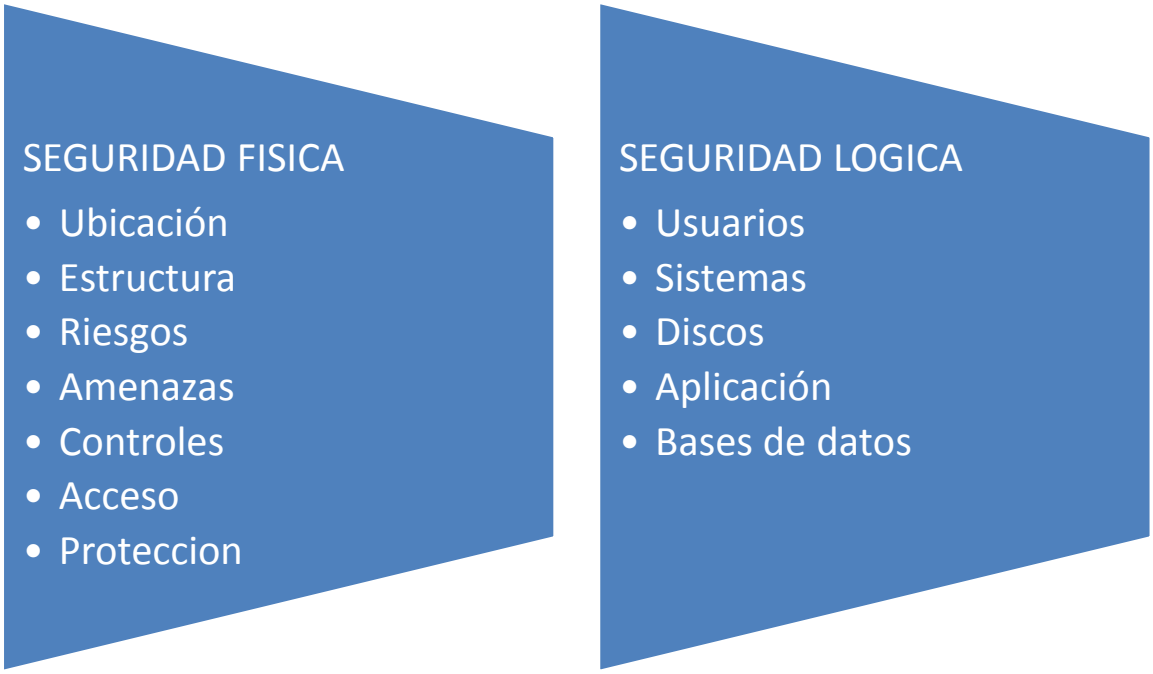
cautelosas que las de otros encuestados. Las encuestas por correo electrónico y la Web entran en la categoría de cuestionarios resueltos por los usuarios en el momento que lo prefieran.

2. APORTACION AL TEMA

La aplicación de una auditoría de seguridad en el centro de computo es importante, ya que a través de esta metodología es donde se obtendrán los resultados de las amenazas que pudieran ocasionar los riesgos en la información que se almacene en cualquier centro de computo, con la aplicación de cuestionarios de respuestas cerradas se conseguirán los resultados para poder diagnosticar la seguridad, se utilizará una metodología de tipo cualitativo/subjetivo, estas están basadas en profesionales de gran nivel de experiencia y formación capaces de dictar recomendaciones, técnicas operativas y jurídicas.

2.1 DEFINICION DEL OBJETIVO Y VARIANTES EN LA SEGURIDAD DE UN CENTRO DE CÓMPUTO

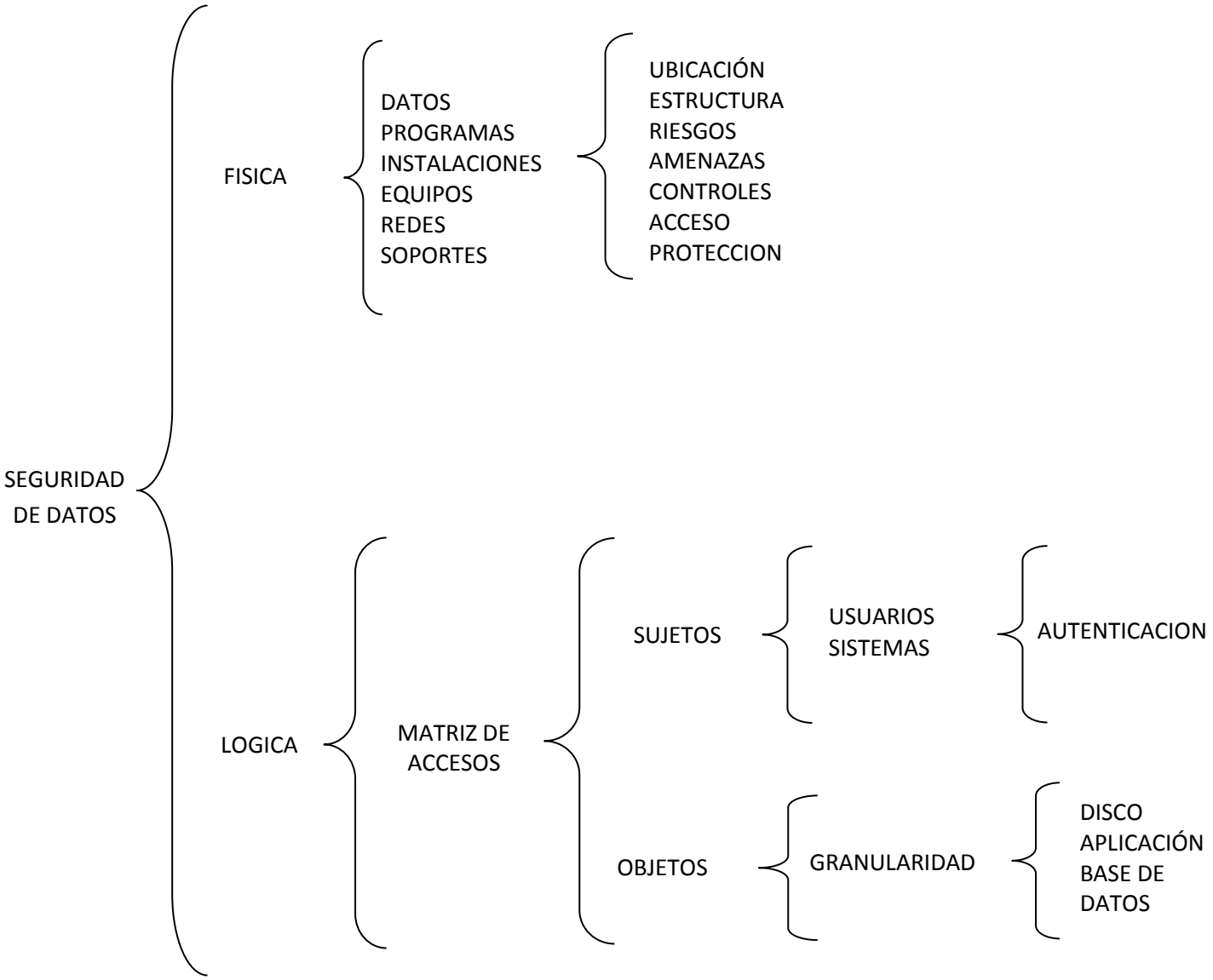
La aportación específica que se hace en el presente trabajo consta del diseño y estructura de un cuestionario como instrumento de medida a la seguridad en un centro de cómputo, el cual se sugiere utilizar en el proceso de la Auditoría Informática en el área de seguridad.
El auditor revisa o audita los controles de seguridad con la ayuda de un checklist o cuestionario que consta de una serie de preguntas o cuestiones a verificar. La evaluación consiste en identificar la existencia de unos controles de seguridad establecidos.
Los cuestionarios se sugiere sean por los auditores, como una guía de referencia, para asegurar que se han revisado todos los controles de seguridad.
En nuestro caso particular se ha el cuestionario en los siguientes apartados:



Esto está fundamentado de acuerdo al autor (Peso, 2001) que se tomó como referencia y nos sirvió como base para aportación de nuestro trabajo buscando realizar cuestionarios que nos facilitaran la realización de una auditoría de seguridad para un centro de computo y poder dar así una ponderación de acuerdo a los indicadores que se componen de la seguridad física y lógica y obtener un promedio de porcentaje total de cada indicador.

Siguiendo con la planeación de cuestionarios o checklist a continuación se muestran las vertientes de seguridad como lo menciona (Peso, 2001) los cuales define como fundamentos de seguridad, tomados para la auditoría de seguridad en la red de información para el centro de cómputo.

2.1.1 Fundamentos de seguridad



2.2 ESTRUCTURA DEL INSTRUMENTO DE MEDICION

Como ya se definió anteriormente las dos variantes y sus fundamentos de la seguridad en los centro de computo se mencionan los indicadores de ítems donde se obtendrá la evaluación de los cuestionarios para conocer el resultado arrojado por cada uno de ellos y en consecuencia obtener el promedio de la ponderación que muestra la auditoría de seguridad realizada al centro de cómputo.

La siguiente tabla muestra los indicadores, que están compuestos por la seguridad física y seguridad lógica, estos indicadores tienen un número de ítems que son el número de preguntas que tiene cada uno de los cuestionarios, que serán el método para la realización de la auditoría, los ítems cuentan con un rango, estos son los números de preguntas abarcadas en cada elemento de acuerdo a la clasificación de seguridad, y por ultimo cuenta con la ponderación (escala de medición) que fue tomada de acuerdo al valor de importancia de cada elemento a evaluar de los centros de computo, para así obtener un promedio que del 100% de la suma del total de ítems tomando como referencia el ejemplo de algunas empresas que aportaron información acerca de los elementos principales que se deben evaluar en los centros de computo y de la investigación de algunos autores (Peso, 2001), (Hernández, 1991) y (Kendall, Analisis y diseño de sistemas, 2005), para realizar la escala de medición.

SEGURIDAD FISICA

INDICADOR	NUMERO DE ITEMS	RANGO DE ITEMS	PONDERACION (ESCALA DE MEDICION)
UBICACIÓN	11	11-11	20%
ESTRUCTURA	9	9-9	10%
RIESGOS	5	5-14	10%
AMENAZAS	9	9-14	20%
CONTROLES	6	6-11	10%
ACCESO	5	5-11	10%
PROTECCION	13	13-13	20%
TOTAL DE PROMEDIO:			**100%**

SEGURIDAD LOGICA

INDICADOR	NUMERO DE ITEMS	RANGO DE ITEMS	PONDERACION (ESCALA DE MEDICION)
USUARIOS	17	17-17	30%
SISTEMAS	10	10-10	10%
FISICOS	12	12-12	20%
TECNICOS	9	9-9	20%
ADMINISTRATIVOS	17	17-17	20%
TOTAL DE PROMEDIO:			**100%**

2.3 METODOLOGIA DE ANALISIS DE RIESGOS

La metodología de riesgos en la seguridad de información está diseñada para ayudar a los profesionales de seguridad del centro de cómputo a desarrollar sus estrategias para proteger la disponibilidad, integridad y confidencialidad de los datos de información que se encuentran en los sistemas informáticos de la red de información del centro de cómputo, como ya se menciono el instrumento de medición la metodología ofrece un acercamiento con los usuarios mediante un cuestionario a esta importante tarea y, como precaución final, también implica el establecimiento de políticas y planes de contingencia en caso de desastre.

Las listas de amenazas ayudan a los administradores de la seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se puedan utilizar para ello se capturara el trafico de la red de información para así poder saber que se tiene que hacer mediante este tipo de ataques. La realización de ataques simulados en sistemas de pruebas permitirá evaluar los lugares en los puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia. Esta metodología proporcionará los conocimientos que el centro de cómputo puede utilizar y la información que hay que distribuir antes y durante los incidentes. Una vez recopilada la información el administrador del centro de cómputo debe delegar responsabilidades del control de incidentes a los encargados de proteger y asegurar la información.

2.4. DISEÑO DE LA FORMA COMO INSTRUMENTO DE EVALUACION

Para realizar la auditoría de seguridad en un centro de computo, es necesario realizar una metodología para obtener resultados que ayuden a mejorar la seguridad de información en el centro de cómputo, para ello se pretende realizar varios cuestionarios que están integrados por los elementos de la clasificación de la seguridad física y lógica.
En los siguientes formatos de cuestionarios se tomará el siguiente diseño siguiendo las recomendaciones de Benjamín Franklin en el diseño de formas en las organizaciones:

ENCABEZADO:

- Nombre y logotipo de la empresa (centro de cómputo) que será evaluado en la auditoría de seguridad.
- Fecha de aplicación del cuestionario realizado al personal del centro de cómputo.
- Clave del formato compuesto por un código que ayude a la secuencia de cada uno de los formatos, la clave se conforma de dos letras AT después de tres números que empezara desde 000.
- La clasificación de cada cuestionario correspondiente a los elementos de la seguridad.
- Objetivo de cada cuestionario para medir su nivel de vulnerabilidad.
- Notas de lo que se tomara en cuenta para la evaluación de cada cuestionario.
- Instrucciones de llenado para cada pregunta del cuestionario.

CONTENIDO:

- Datos generales del entrevistado como es su nombre y el cargo o puesto que se tiene para conocer el nivel de experiencia en el centro de computo.
- Numero consecutivo del total de preguntas que contiene cada uno de los cuestionarios.
- Preguntas tomadas de acuerdo a la información de cada elemento de seguridad de acuerdo a la clasificación de seguridad física y lógica.
- Escalamiento tipo likert para obtener un análisis más concreto, claro y posible de cada una de las preguntas, obteniendo respuestas clasificadas en: definitivamente si, indeciso o definitivamente no.

PIE:

- Nota de agradecimiento por la realización del cuestionario por parte del entrevistado.

2.5 DISEÑO DE FORMATO DE CUESTIONARIO PARA LA AUDITORIA DE SEGURIDAD

LOGOTIPO DE LA EMPRESA

NOMBRE DE LA EMPRESA

AUDITORIA INFORMÁTICA

CLAVE DEL FORMATO

No. AT001

CUESTIONARIO A USUARIOS DEL CENTRO DE COMPUTO
SEGURIDAD FÍSICA: Infraestructura

FECHA DE APLICACION:

Objetivo: Medir el nivel de vulnerabilidades existentes en equipos de los usuarios y puedan introducir algún tipo de virus.
Nota: Se realizara un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, sobre el funcionamiento de su equipo de red y las protecciones básicas que este posee.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

ENCABEZADO

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				

CONTENIDO

Gracias por su apoyo!!!

PIE

Se presenta un reporte de evaluación por cada criterio evaluado en cada uno de los cuestionarios para la realización de la auditoría de seguridad en el centro de computo, que servirá como reporte para el análisis del instrumento de evaluación, en el cual se enumeran los problemas detectados mediante el análisis de la auditoría de seguridad, así como las recomendaciones que se darán para que el centro de computo tenga una mayor seguridad en una fecha probable de implementación y el nombre de la persona responsable que se hará responsable de dar respuesta a las repercusiones.

2.6 REPORTE DE LA EVALUACIÓN DE LOS USUARIOS DEL CENTRO DE CÓMPUTO

DIRECCIÓN:

AUDITORIA A: **OJA No:**

FECHA DE INICIO: **ECHA DE FINALIZACIÓN:**

NOMBRE DEL AUDITOR:

Problemas detectados:

Alternativas de solución:

Repercusiones:

Recomendaciones:

Fecha de la implementación:

Firma: _____ Firma: _____

Elaboró: Revisó:

2.7 ELABORACION DE CUESTIONARIOS BASADO EN LOS FUNDAMENTOS DE SEGURIDAD EN CENTROS DE CÓMPUTO

2.7.1 Cuestionarios sobre la seguridad física

2.7.1.1 Formato para medir la seguridad física: Ubicación.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE EVALUACION DEL ENTORNO DEL CENTRO DE CÓMPUTO SEGURIDAD FISICA: Ubicación	CLAVE DEL FORMATO No. AT001

FECHA DE APLICACION:

Objetivo: Recolectar información general y específica sobre los diferentes aspectos que rodean los centros de cómputo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, para conocer acerca de su entorno.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Se considera adecuada la ubicación actual del centro de cómputo?			
2	¿Considera que el acceso al centro de cómputo, es el idóneo?			
3	¿El espacio físico con el que cuenta el centro de cómputo se considera adecuado?			
4	¿Hay comodidad de acuerdo a las distribuciones que se tienen con el mobiliario y equipo de oficina dentro del centro de cómputo?			
5	¿Existe demasiado ruido que interfiera en el centro de cómputo?			
6	¿Son adecuadas las condiciones ambientales con respecto a la iluminación que se tiene?			
7	¿Las condiciones ambientales con respecto a la ventilación que se tienen son las adecuadas?			
8	¿Son adecuadas las condiciones ambientales con respecto			

	a limpieza?			
9	¿Las condiciones con respecto a ergonomía son las idóneas?			
10	¿Considera que la distribución de las computadoras está acorde a las necesidades de los usuarios?			
11	¿Se evalúan las condiciones ambientales por algún ente encargado?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad física en el área de estructura.

2.7.1.2 Formato para medir la seguridad Física: Estructura.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE EVALUACION DE LA INFRAESTRUCTURA DEL CENTRO DE CÓMPUTO SEGURIDAD FISICA: Estructura	CLAVE DEL FORMATO No. AT002

FECHA DE APLICACION:

Objetivo: Recolectar información general y específica sobre los diferentes aspectos que rodean los centros de computo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, para saber si la infraestructura es adecuada o no.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Considera adecuada la infraestructura del centro de cómputo, que actualmente posee su centro?			
2	¿Se hacen notificaciones a los superiores de los problemas existentes de infraestructura del centro de cómputo?			
3	¿Se realizan remodelaciones en la infraestructura?			
4	¿Considera adecuada las condiciones eléctricas para el funcionamiento del centro de cómputo?			
5	¿Se han detectado fallas eléctricas en algún equipo?			
6	¿Se notifica a los superiores de los problemas existentes con fallas eléctricas?			
7	¿Los toma corrientes del centro de cómputo se encuentran debidamente protegidos con polarización?			
8	¿Los dados térmicos están distribuidos correctamente?			
9	¿Se realizan remodelaciones en el centro de cómputo?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad Física en el área de amenazas.

2.7.1.3 Formato para medir la seguridad lógica: Amenazas.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE EVALUACION DE LA SEGURIDAD DEL CENTRO DE CÓMPUTO SEGURIDAD FISICA: Riesgos y Amenazas	CLAVE DEL FORMATO No. AT003

FECHA DE APLICACION:

Objetivo: Investigar las actualizaciones que realiza el centro de computo de acuerdo a las políticas de seguridad del centro de computo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, sobre las vulnerabilidades que se generan en los laboratorios del centro de computo.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Hay controles para hacer cumplir las políticas se seguridad por contraseña en todas las cuentas?			
2	¿Existen controles que hagan cumplir las políticas de seguridad para las cuentas de usuarios y administradores?			
3	¿Existe una opción de autenticación para el acceso administrativo o cargo de los dispositivos y hosts?			
4	¿Existe la opción de autenticación para los accesos a la red y los hosts internos de los usuarios internos?			
5	¿El bloqueo de cuentas esta activado para impedir el acceso a las cuentas tras una serie de intentos de registro fallido?			
6	¿Hay controles para hacer cumplir las políticas de las aplicaciones clave?			
7	¿Se conocen los controles de contraseña implementados en las aplicaciones?			
8	¿Existe un método de autenticación más común usado en las aplicaciones clave?			
9	¿Las informaciones clave guardan mensajes en archivos con la bitácora del uso para análisis y auditoría?			
10	¿Las aplicaciones utilizadas validan datos de entrada?			

11	¿La información utilizada para los usuarios es encriptado?			
12	¿Las aplicaciones claves encriptan la información critica y sensible que procesan?			
13	¿El almacenamiento de la información es eficiente?			
14	¿El centro de cómputo cuenta con la recuperación de errores?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad física en el área de Control y acceso.

2.7.1.4 Formato para medir la seguridad física: Control y acceso.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE ADMINISTRACION Y CONTROL DEL CENTRO DE COMPUTO SEGURIDAD FISICA: Controles y Acceso	CLAVE DEL FORMATO No. AT004

FECHA DE APLICACION:

Objetivo: conocer los motivos y puntos vulnerables de la administración y control llevada en el centro de cómputo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, saber los ataques que se pueden esperar y las formas de defenderse contra ellos.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿El centro de cómputo es el que configura los sistemas o esta tarea la efectúan otros proveedores o distribuidores de software?			
2	¿Las terminales o servidores se han creado basándose en una configuración documentada o en una imagen formal?			
3	¿Se han aplicado controles de seguridad físico para garantizar la seguridad de la propiedad del centro de cómputo?			
4	¿Cuáles controles de seguridad utiliza?			
5	¿Ha considerado desastres de tipo natural?			
6	¿Utiliza algún método para evitar algún tipo de desastre?			
7	¿Existe personal de vigilancia cerca del área de cómputo?			
8	¿Se han establecido medidas de seguridad en la sección de informática en cuanto un lugar especifico para salvaguardar los recursos tecnológicos?			
9	¿Existen controles preventivos para evitar causas de riesgos o desastres como (letreros, extintores, etc.) dentro de las instalaciones del centro de cómputo?			
10	¿Se supervisan las actividades de los usuarios para			

	determinar las acciones que ejecutan?			
11	¿Se cambian las claves de acceso al sistema o equipos con frecuencia?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad física en el área de Protección.

2.7.1.5 Formato para medir la seguridad física: Protección.

LOGOTIPO DE LA EMPRESA	**NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA**	CLAVE DEL FORMATO **No. AT005**

CUESTIONARIO DE EVALUACION DEL MOBILIARIO Y EQUIPO DEL CENTRO DE CÓMPUTO
SEGURIDAD FISICA: Protección

FECHA DE APLICACION:

Objetivo: Recolectar información general y específica sobre los diferentes aspectos que rodean los centros de cómputo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, para saber cómo se encuentra el mobiliario y equipo.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Es necesario mejorar el tipo de distribución del mobiliario y equipo que actualmente se posee?			
2	¿Se cuenta con el equipo y mobiliario adecuado para el Centro de cómputo?			
3	¿Es cómodo y suficiente la cantidad de mobiliario para el equipo de cómputo?			
4	¿Actualmente se están dejando de realizar actividades por falta de equipo de cómputo o recursos tecnológicos?			
5	¿Existen equipos de cómputo adicionales que reemplacen los dañados?			
6	¿Existe un lugar específico para guardar la papelería y herramientas de trabajo?			
7	¿Existe servicio de mantenimiento para el mobiliario y equipo?			
8	¿Existen medidas de seguridad para			

	proteger el mobiliario y equipo?			
9	¿Se tiene un lugar para el mobiliario y equipo dañado totalmente?			
10	¿Cuenta con alguna persona en quien recaiga la responsabilidad del cuidado y mantenimiento del mobiliario y equipo?			
11	¿Se renueva el mobiliario y equipo con frecuencia?			
12	¿se hace algún tipo de acción con el equipo en des uso?			
13	¿La cantidad de computadoras con las que cuenta el centro de cómputo son las adecuadas?			

Gracias por su apoyo!!!

2.7.2 Cuestionarios sobre la seguridad Lógica

2.7.2.1 Formato para medir la seguridad lógica: Usuarios.

LOGOTIPO DE LA EMPRESA	**NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA** **CUESTIONARIO A USUARIOS DEL CENTRO DE COMPUTO** **SEGURIDAD LOGICA: Usuarios**	**CLAVE DEL FORMATO** **No. AT006**

FECHA DE APLICACION:

Objetivo: Medir el nivel de vulnerabilidades existentes en equipos de los usuarios y puedan introducir algún tipo de virus.
Nota: Se realizara un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, sobre el funcionamiento de su equipo de red y las protecciones básicas que este posee.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVA MENTE "SI"	INDECISO	DEFINITIVA MENTE "NO"
1	¿Usted es el único que tiene acceso a su equipo?			
2	¿Tiene contraseña para poder acceder a su equipo?			
3	¿Cambia regularmente su contraseña?			
4	¿Cada cuanto tiempo la cambia?			
5	¿Lo informaron de políticas de seguridad que deberá cumplir en su equipo?			
6	¿Existe alguna norma o formato para la creación de la contraseña?			
7	¿Tiene permiso para descargar e instalar cualquier tipo de programas en su equipo de trabajo?			
8	¿Tiene autorización para meter dispositivos USB en su equipo?			
9	¿Cuándo se encuentra ausente bloquea su equipo?			
10	¿Le han dado alguna plática o curso sobre la seguridad informática?			
11	¿Su equipo ha tenido ataques de virus?			
12	¿Ha perdido algo de información en su equipo?			
13	¿Procesa información fuera del centro de cómputo?			
14	¿Tiene acceso a internet en su equipo?			
15	¿Tiene permiso a todas las páginas de internet?			

16	¿Accede a páginas de internet que no tengan relación con su trabajo?			
17	¿Utiliza programas que no tienen relación con su trabajo?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad Lógica en el área de sistemas.

2.7.2.2 Formato para medir la seguridad lógica: Sistemas.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE INFORMACION DE SISTEMAS Y RED DEL CENTRO DE CÓMPUTO SEGURIDAD LOGICA: Sistemas	CLAVE DEL FORMATO No. AT007

FECHA DE APLICACION:

Objetivo: Conocer la forma de administración y control que posee sobre los sistemas de información.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, para saber si posee una buena administración y control sobre los sistemas.
Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿El centro de cómputo utiliza firewalls u otros controles de acceso para proteger sus registros e información?			
2	¿El centro de cómputo aplica estos controles en todas las oficinas?			
3	¿El centro de cómputo usa una red DMZ para separar redes internas y externas de los servicios albergados?			
4	¿El centro de cómputo usa firewall en los host para proteger a los servidores?			
5	¿El centro de cómputo usa hardware o software de detección de intrusos par identificar los ataques a la seguridad?			
6	¿Se utiliza antivirus acorde con la cantidad de empleados en la empresa?			
7	¿El tiempo de respuesta para envió y recepción de datos desde las terminales es el adecuado?			
8	¿Se puede acceder a la red del centro de cómputo de forma remota?			
9	¿La red tiene más de un segmento?			
10	¿La red dispone de conexión inalámbrica?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad Lógica en el área de Discos.

2.7.2.3 Formato para medir la seguridad lógica: Discos.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE INFORMACION ACERCA DE LOS DISCOS DEL CENTRO DE CÓMPUTO SEGURIDAD LOGICA: Discos	CLAVE DEL FORMATO No. AT008

FECHA DE APLICACION:

Objetivo: Conocer el perímetro abarcado de la red de acuerdo a la medida de protección existentes.
Nota: Se realizara un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, sobre las vulnerabilidades en comparación con las medidas de protección del centro de cómputo.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Tiene conexión permanente a internet?			
2	¿El centro de cómputo permite acceso ilimitado a sus empleados para navegar en internet?			
3	¿Los usuarios internos y externos usan los recursos del mismo segmento de red?			
4	¿El centro de cómputo permite que los empleados accedan a la red del mismo?			
5	¿Permite que sus empleados utilicen sistemas que no sean de producción como pueden ser servidores web personales o equipos que actúen como host de proyectos personales?			
6	¿El centro de cómputo se permite a los empleados procesar información corporativa fuera de las instituciones?			
7	Si la Red de Información no está disponible, ¿El centro de cómputo puede trabajar?			
8	¿El centro de cómputo comparte oficina con otras entidades?			
9	¿Amplía el centro de cómputo su red, mediante la adquisición de nuevas áreas con sus entornos correspondientes?			
10	¿Permite el centro de cómputo que los empleados			

	descarguen a sus equipos de trabajos o equipos portátiles datos corporativos o datos confidenciales de los clientes?			
11	¿Limita el centro de computo el acceso a la información en la función de los roles de los usuarios?			
12	¿Implanta el centro de cómputo nuevos servicios o aplicaciones antes de evaluar los posibles riesgos de la seguridad?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad Lógica en el área de aplicación.

2.7.2.4 Formato para medir la seguridad lógica: Aplicación.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE EVALUACION DE LA APLICACIÓN DEL CENTRO DE CÓMPUTO SEGURIDAD LOGICA: Aplicación	CLAVE DEL FORMATO No. AT009

FECHA DE APLICACION:

Objetivo: Recolectar información general y específica sobre los diferentes aspectos que rodean los centros de cómputo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, para evaluar los recursos humanos.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Se desarrollan programas de capacitación para el administrador, encargado e instructor del centro de cómputo?			
2	¿Se imparten capacitaciones para los docentes de la institución por parte del administrador, encargado e instructor del centro de cómputo?			
3	¿Se le hacen sugerencias al administrador, encargado e instructor del centro de cómputo para el mejoramiento del mismo?			
4	¿Se toman en cuenta las sugerencias proporcionadas?			
5	¿Se han detectado o identificado las necesidades actuales y futuras de capacitación del personal del área?			
6	¿Se lleva a cabo la supervisión de las funciones del administrador, encargado e instructor del centro de cómputo?			
7	¿Presenta el Administrador, encargado e instructor del centro de computo sugerencias para mejorar las condiciones del centro de computo?			

8	¿Existe un sustituto para realizar las funciones dentro del centro de computo en caso de no presentarse el Administrador, encargado e instructor del centro de computo?			
9	¿Existen políticas institucionales para sancionar la indisciplina del administrador, encargado e instructor del centro de cómputo?			

Gracias por su apoyo!!!

Cuestionarios sobre la seguridad Lógica en el área de base de datos.

2.7.2.5 Formato para medir la seguridad lógica: Bases de datos.

LOGOTIPO DE LA EMPRESA	NOMBRE DE LA EMPRESA AUDITORIA INFORMÁTICA CUESTIONARIO DE EVALUACION DE LAS BASES DE DATOS DEL CENTRO DE CÓMPUTO SEGURIDAD LOGICA: Bases de datos	CLAVE DEL FORMATO No. AT010

FECHA DE APLICACION:

Objetivo: Recolectar información general y específica sobre los diferentes aspectos que rodean los centros de cómputo.
Nota: Realizar un sondeo realizado mediante un cuestionario de preguntas sencillas a los usuarios, para conocer la gestión administrativa.

Instrucciones: lea cada pregunta y marque con una "x" la respuesta que corresponda a su opinión.

Datos Generales del entrevistado	
Nombre del entrevistado:	
Cargo o puesto:	

NO.	PREGUNTA	DEFINITIVAMENTE "SI"	INDECISO	DEFINITIVAMENTE "NO"
1	¿Existen manuales de procedimientos para la gestión administrativa dentro de los centros de cómputo?			
2	¿Considera que están elaborados de acuerdo a las necesidades que se tienen en los centros de cómputos?			
3	¿Considera que es conveniente la revisión de estos para una posible modificación?			
4	¿Al no cumplir con la aplicación de los manuales, se presiona o sanciona por parte de los superiores?			
5	¿Se lleva a cabo un control de todos los activos de los centros de cómputo?			
6	¿Existen normas para llevar el control de los activos?			
7	¿El tipo de control de activos que se está llevando dentro del centro de cómputo es el adecuado?			
8	¿Considera que se debe modificar el tipo de control de inventario con el que cuenta actualmente el centro de cómputo?			
9	¿El administrador, encargado e instructor de centro de cómputo, maneja de una forma adecuada el			

	control de inventario?			
10	¿Se han generado pérdidas en cuanto a los activos del centro de cómputo?			
11	¿Se cuenta con inventarios actualizados del centro de computo y aula informática?			
12	¿Se actualiza el inventario con regularidad?			
13	¿Existe un responsable específicamente para llevar el control de inventario?			
14	¿Existe un formato específicamente para llevar el control de inventario del equipo de cómputo dañado?			
15	¿Existe un formato específicamente para llevar el control de inventario de otros recursos tecnológicos dañados?			
16	¿Hay limitantes con las que cuenta el administrador encargado e instructor para la actualización de inventario?			
17	¿Considera que la aplicación de un manual de auditoría informática le ayudaría a mejorar la gestión administrativa del centro de cómputo?			

Gracias por su apoyo!!!

Con el alcance de la auditoría de seguridad realizada al centro de cómputo con relación al instrumento de medición que fueron dirigidos los cuestionarios, se abarcó un replanteamiento respecto a la información del centro de computo de cómo debe ser manejada y evaluada para su seguridad y que los usuarios del centro de computo tengan el conocimiento adecuado de cómo llevar a cabo las recomendaciones señaladas por el auditor.

El siguiente formato de reporte contiene los datos de la empresa (centro de computo) que será evaluada con la auditoría de seguridad, el cual estará detallado por los problemas detectados en base al instrumento de medición, las alternativas de solución que se darán para llevar a cabo los problemas detectados, las repercusiones que se tendrán en la implementación, así como algunas recomendaciones que se efectuaran y por último la fecha en la que se realizara la implementación y la firma de la persona responsable, todo esto para llevar el control de la información con relación a la auditoría informática y así tener concentrada la información solicitada.

2.8 FORMATO TIPO CARTA DE AUDITORÍA

La auditoría de seguridad concluye con el siguiente formato tipo carta de auditoría que será el informe final, mencionando la fecha en la que se concluyó la recopilación de información del centro de cómputo y también se menciona el alcance que se obtuvo con la auditoría.

Morelia, Michoacán, _____ de _____ de 20_____

Sr._____
Encargado del área auditada.

Presente:

A continuación se presenta un informe final de la Auditoría interna realizada en el área de: _____
Que está a su cargo.

Por lo tanto se anexa el reporte.

El alcance del proyecto comprende las siguientes áreas especificadas a continuación:

- Seguridad física
- Seguridad lógica.

Aspectos a evaluar en la auditoria:

Los cuestionarios para la auditoría de seguridad están conformados por las siguientes evaluaciones:

SEGURIDAD FISICA

UBICACION	•EVALUACION DEL ENTORNO
ESTRUCTURA	•EVALUACION DE LA INFRAESTRUCTURA
RIESGOS	•EVALUACION DEL SOFTWARE
AMENAZAS	•EVALUACION DE LA SEGURIDAD
CONTROLES	•EVALUACION DEL HARDWARE
ACCESO	•EVALUACION DEL CONTROL DE ACTIVOS FIJOS
PROTECCION	•EVALUACION DEL MOBILIARIO Y EQUIPO

SEGURIDAD LOGICA

USUARIOS	•EVALUACION DE INFORMACION DE USUARIOS
SISTEMAS	•EVALUACION DE LA INFORMACION
Disco	•EVALUACION DE LA INFORMACION ACERCA DE LA RED
Aplicacion	•EVALUACION DE APLICACION DE SOFTWARE
Base de datos	•EVALUACION DE ADMINISTRACION DE INFORMACION

NOTA: Cada área evaluada o aspecto, deberá llevar una descripción breve sobre su correspondiente análisis de lo encontrado en la evaluación; así como también las repercusiones, alternativas de solución, y todo lo que el auditor estime conveniente o necesario mencionar.

ATENTAMENTE

Grupo Auditor:

Firma: _____ **Firma:** _____

Elaboró Revisó

Firma: _____

Autorizó

2.9 ELEMENTOS A EVALUAR EN CENTROS DE COMPUTOS REALES

Para conocer cuáles son los principales elementos a evaluar en una auditoría de seguridad, se baso en la información teórica y práctica, en lo teórico se tomo de algunos autores de la seguridad informática y en lo práctico se hizo entrevistas a dos empresas de la ciudad de Morelia (AAK Y COCOTRA), por medio de un formato de evaluación en el que se detalla la importancia que tienen estos elementos, ya que son los primordiales en estas empresas. La evaluación está conformada por tres sencillas preguntas que fueron:

- ¿Cuáles son las características de su centro de cómputo?: En esta pregunta se sabrá cómo está conformado su centro de cómputo y cuanto personal labora en el mismo.

- ¿Cuáles son los principales elementos a revisar en su centro de cómputo?: El responsable aportara los elementos primordiales para llevar más a detalle la auditoría de seguridad.

- ¿Por qué considera que se deben evaluar estos elementos? Se obtendrá una respuesta clara y precisa de porque la importancia de evaluar los elementos comentados y no otros.

Esta evaluación de elementos es muy importante ya que con el resultado arrojado del informe, se podrá anexar al instrumento de medición para que sea considerado para

la realización de la auditoría de seguridad. Para lograrlo se realizó el siguiente formato:

2.10 EVALUACION DE ELEMENTOS PARA LA AUDITORIA DE SEGURIDAD EN UN CENTRO DE CÓMPUTO

NOMBRE DE LA EMPRESA:
GIRO COMERCIAL:
EXPERIENCIA LABORAL:

CARACTERISTICAS DEL CENTRO DE COMPUTO:

ELEMENTOS A REVISAR DEL CENTRO DE COMPUTO:

¿PORQUE CONSIDERA QUE SE DEBEN EVALUAR ESTOS ELEMENTOS?

2.11 APLICACIÓN DEL INSTRUMENTO DE EVALUACION (CUESTIONARIOS)

La auditoría de seguridad fue realizada en la empresa Aarhuskarlshamn S.A. de C.V.(AAK) mediante la elaboración de una evaluación de elementos y cuestionarios que incluyeron preguntas cerradas, esto para probar la factibilidad del instrumento y/o hacer las aportaciones y mejoras al instrumento. Esta empresa se encuentra establecida en la ciudad de Morelia, Michoacán en Avenida Héroes de Nocupétaro 1022 Col. Industrial. Se evalúa el área de sistemas la cual cuenta con un centro de cómputo.

AAK, refina aceites vegetales para los productos especializados que satisfagan las necesidades de sus clientes. En colaboración con sus clientes, AAK se desarrolla una posición de liderazgo mundial con un alto nivel de rentabilidad. AAK debe ser la primera opción para los clientes cuya producción se basa en aceites vegetales de alto valor añadido. Esto es lo que ha hecho AAK el principal productor mundial de grasas vegetales de especialidad. Los productos se utilizan como sustitutos de grasa láctea y manteca de cacao, como soluciones transfree para rellenos de chocolate y productos de confitería, así como por la industria cosmética.

HISTORIA

1871 Aarhus United

1910 Aarhus Palmekærnefabrik se establece y comienza la producción de tortas de aceite.

1940 Una red internacional se ha establecido. Las operaciones consolidadas y en el tiempo deben representar el 10 por ciento de las exportaciones de Dinamarca.

1960 Crecimiento de la producción moderna y ayudar a la compañía convertirse en un líder de mercado dentro de las grasas de la especialidad.

1970 Dinamarca entra en la UE, y las barreras arancelarias se erosionan. Bek-Nielsen entra como accionista mayoritario en 1978.

1982-1991 La globalización continúa, y el Reino Unido las filiales, EE.UU. y México se hayan establecido.

2003 Todas las operaciones se agrupan bajo el nombre colectivo de Aarhus United.

1918 Karlshamns

1932 La producción de harina de soja para la alimentación animal entre en funcionamiento.

1942 Kooperativa Förbundet adquiere la fábrica.

1965 Entregas importantes a la industria de la margarina privado sueco comienza.

1994 Inauguración de la fábrica de la crema la margarina y el hielo. Un laboratorio de investigación se construye.

1997 Las operaciones de Estados Unidos se venden, como es la margarina y la producción de helados.

2001 La cuota de Karlshamns cotiza en la Bolsa de Estocolmo.

2004 Melker Schörling adquiere las acciones en poder de Kooperativa Förbundet, convirtiéndose así en el mayor accionista de Karlshamns.Centrarse en las grasas de alta especialidad de valor añadido. La fusión

28 de septiembre 2005 BNS Industrier cambia su nombre a AarhusKarlshamn. Como consecuencia de la finalización BNS Industrier de las ofertas de Aarhus Unidos y Karlshamns la empresa cambia su nombre de BNS Industrier AB AarhusKarlshamn AB. El nuevo nombre de compañía se ha registrado en Bolagsverket.

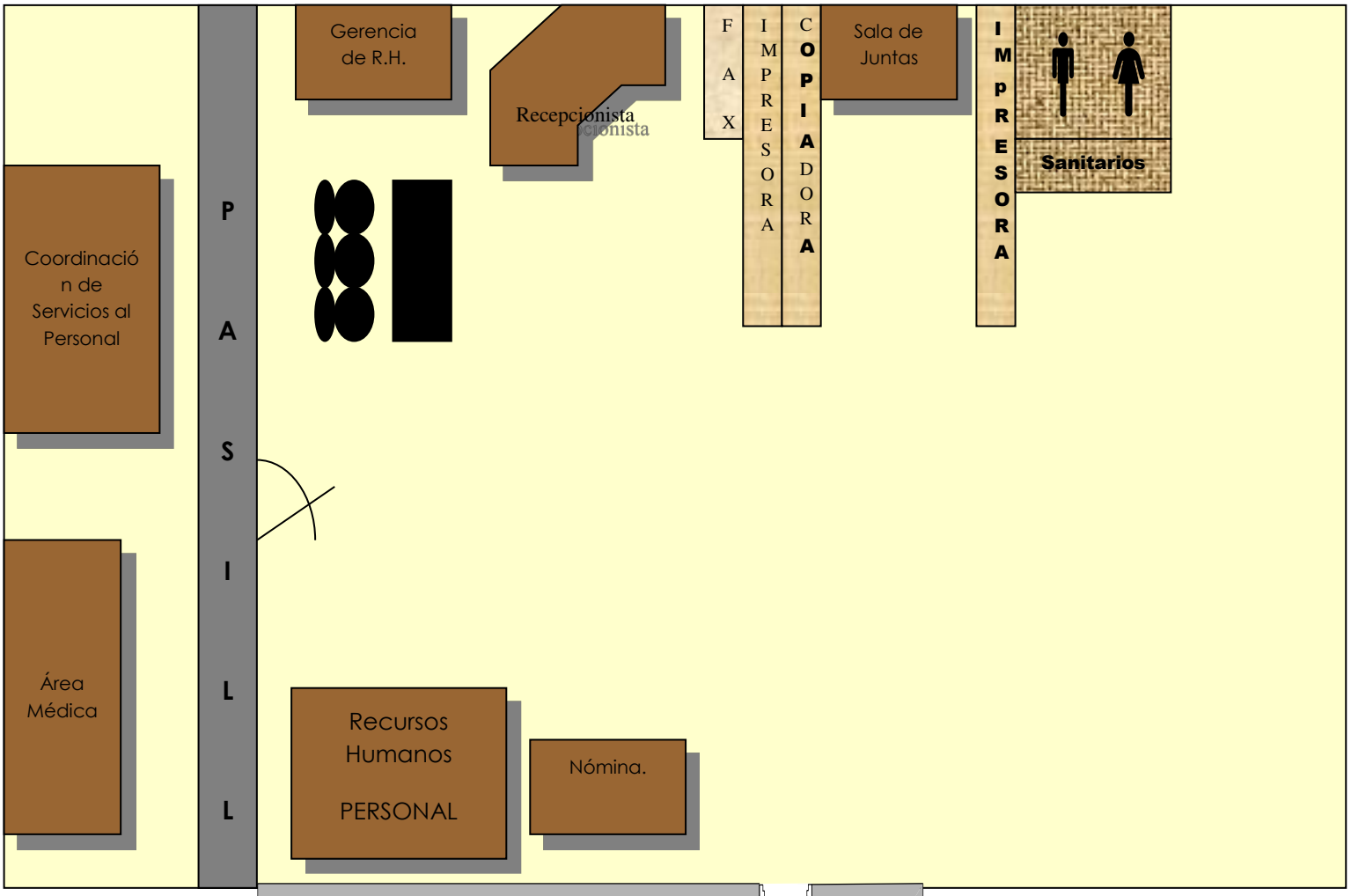
Operando en la participación AarhusKarlshamn comenzará en la Marknaden Nya el 29 de septiembre de 2005, bajo el ticker de la AAK.

22 de septiembre 2005 BNS Industrier ha recibido aceptaciones de los accionistas que representan el 94,3% en Aarhus Unidos y 95,7% en Karlshamns y completa las dos ofertas.

19 de septiembre 2005 BNS Industrier ha recibido el visto bueno de todas las autoridades de competencia pertinentes

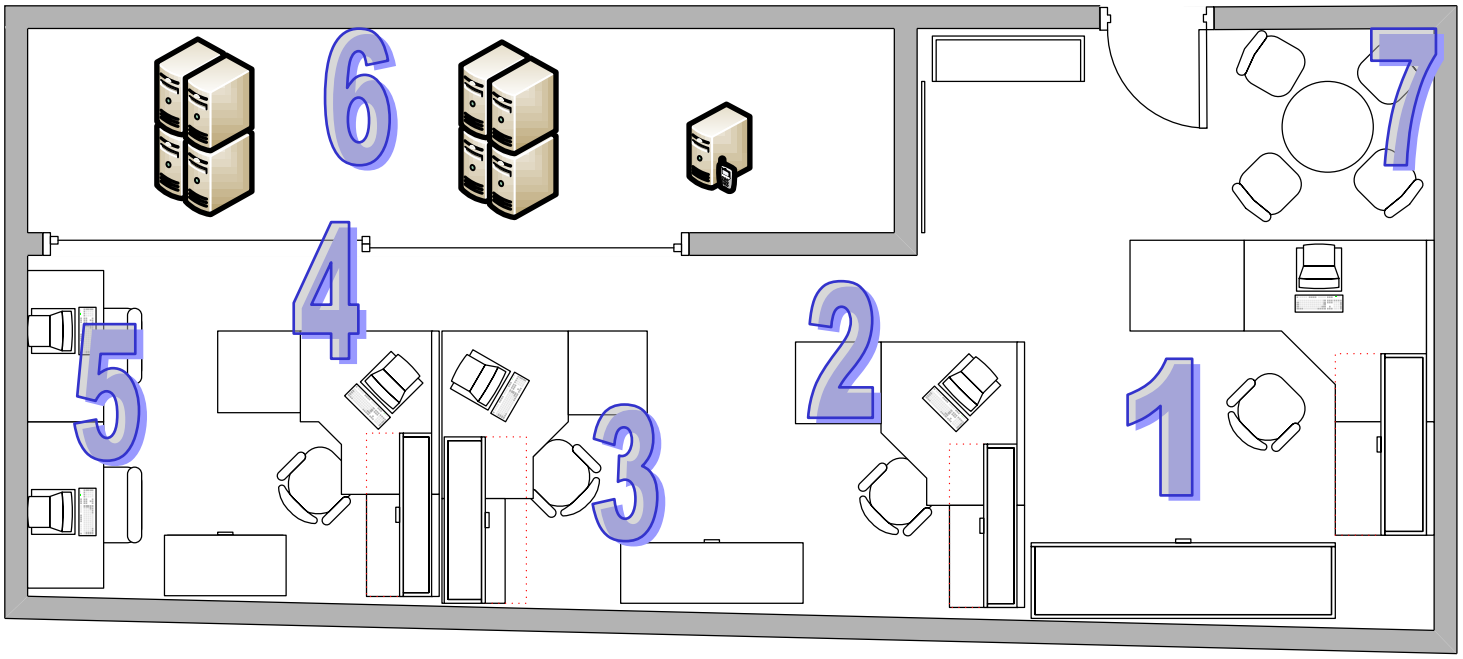
26 de mayo 2005 Aarhus Unidos y Karlshamns combinar. En un anuncio de bolsa de valores emitidos en la mañana del 26 de mayo de 2005, las empresas International ha anunciado su plan - en cooperación con Melker Schörling, el principal accionista de Karlshamns AB - para trabajar en pro de una fusión entre Aarhus United A / S y AB Karlshamns

PLANO DE OFICINA



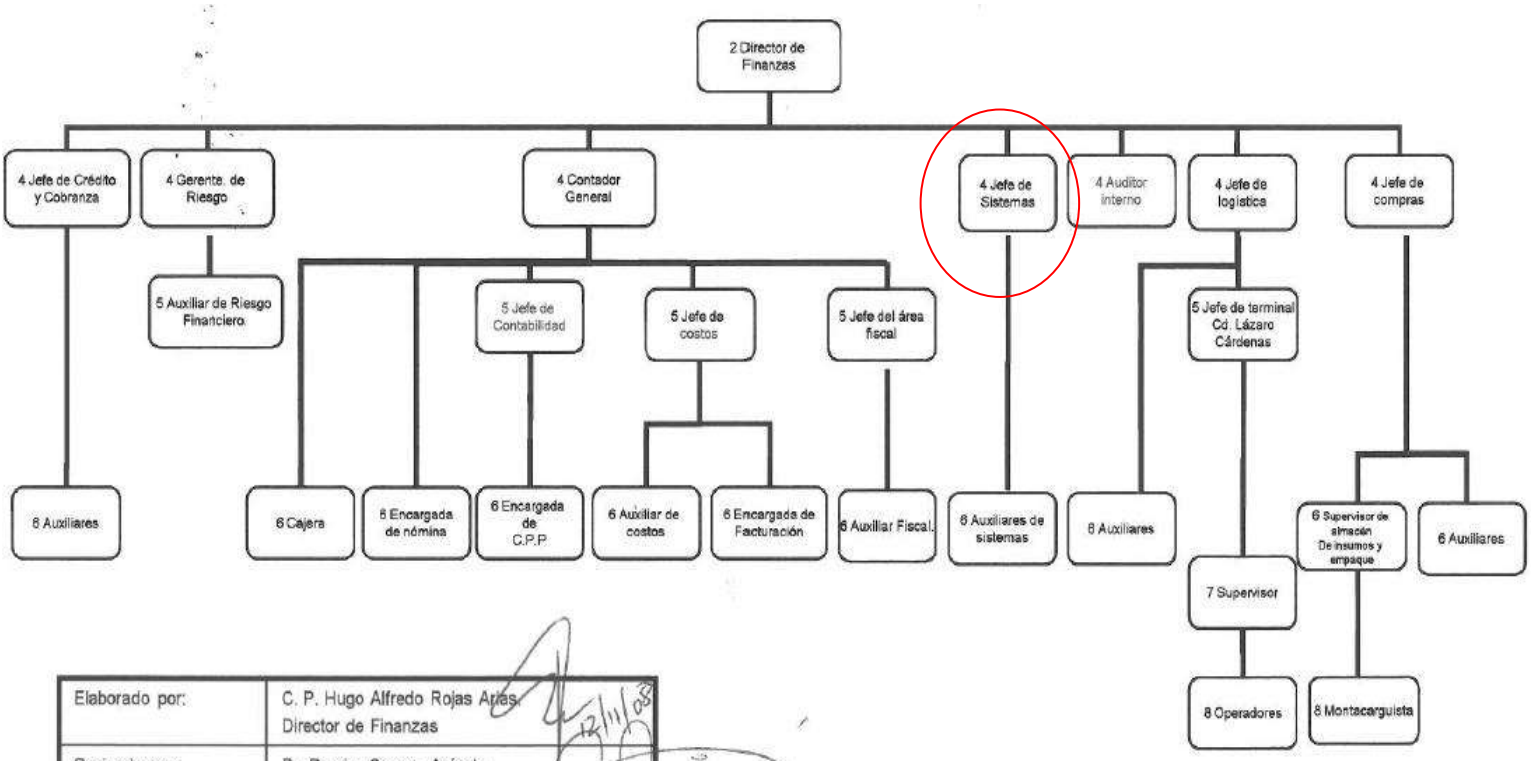
Área de sistemas (Centro de computo) (IT)

DISTRIBUCION DE EQUIPO EN AREA DE TRABAJO DEL CENTRO DE COMPUTO



1. Jefe de sistemas. (Julián Espino).
2. Auxiliar (Rodrigo Huerta).
3. Auxiliar (Alejandro García).
4. Auxiliar (Heriberto García) y (Practicante)
5. Auxiliar (Antonio Berni Brito) y (Practicante)
6. Cuarto de telecomunicaciones (SITE)
7. Área de sala de juntas, impresora y de área de equipos.

ORGANIGRAMA DE FINANZAS (SISTEMAS)



Elaborado por:	C. P. Hugo Alfredo Rojas Arias Director de Finanzas	
Revisado por:	Dr. Ramiro Corona Arévalo Gerente de Recursos Humanos	
Autorizado por:	Ing. Octavio Díaz de León Carrillo Director General	
Fecha de emisión:	01/03/02	Pagina 2 de 7
Fecha de revisión:	22/10/08	Revisión: ñ

El área de sistemas (centro de cómputo) depende de la dirección de Finanzas.

AUDITORIA DE LA SEGURIDAD EN EL CENTRO DE COMPUTO DE AARHUSKARLSHAMN S.A. DE C.V.

Se aplicó el instrumento de medición basado en la metodología de la aplicación de cuestionarios conformados por preguntas cerradas, al encargado (administrador) del centro de cómputo de esta empresa, el administrador de este centro de cómputo es el Ingeniero Julián Espino Echandi, quien contestó de acuerdo a su experiencia laboral en el área y conocimientos que ha obtenido en el tiempo que lleva en esta empresa.

Todo esto obtenido del reporte de los principales elementos a evaluar en este centro de computo, ya que son considerados para la seguridad la cual es básica y fundamental en el desarrollo de cualquier actividad o labor y la información que se tiene en esta empresa, ya que es el activo más importante que puede poseer, es por eso que el evaluar estos controles que puedan prevenir poner en riesgo la información e inclusive recuperarla después de un ataque o desastre son de suma importancia para asegurar el activo con mayor valor y la continuidad de la empresa basándose en esta auditoría de seguridad mitigando el impacto del riesgo.

La auditoría de seguridad de la red de información fue analizada por cada cuestionario que fue evaluado mediante la ponderación de los indicadores de seguridad física y lógica de acuerdo al número y rango de ítems, así obteniendo los siguientes resultados en la escala de medición:

SEGURIDAD FISICA

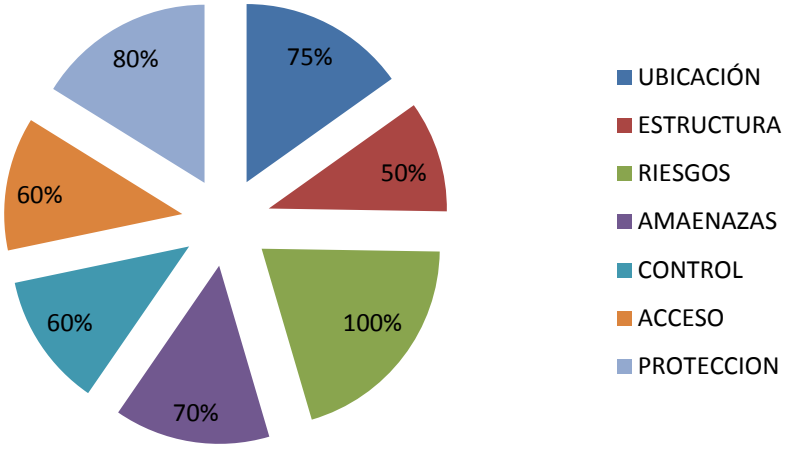
INDICADOR	NUMERO DE ITEMS	RANGO DE ITEMS	PONDERACION (ESCALA DE MEDICION)
UBICACIÓN	11	11-11	15%
ESTRUCTURA	9	9-9	5%
RIESGOS	5	5-14	10%
AMAENAZAS	9	9-14	14%
CONTROL	6	6-11	6%
ACCESO	5	5-11	6%
PROTECCION	13	13-13	16%
TOTAL DE PROMEDIO:			**72%**

SEGURIDAD LOGICA

INDICADOR	NUMERO DE ITEMS	RANGO DE ITEMS	PONDERACION (ESCALA DE MEDICION)
USUARIOS	17	17-17	26%
SISTEMAS	10	10-10	9%
FISICOS	12	12-12	15%
TECNICOS	9	9-9	19%
ADMINISTRATIVOS	17	17-17	15%
TOTAL DE PROMEDIO:			**83%**

La primera impresión del estado de la seguridad física en el centro de computo se presenta en el grafico 1 al haber aplicado el instrumento de medición realizando un sondeo de preguntas sencillas, sin entrar en detalles específicos, sobre el funcionamiento de la red y las protecciones básicas que posee como son la ubicación, estructura, riesgos, amenazas, control, acceso y protección se puede apreciar que el centro de computo de la empresa AAK, no cuenta con herramientas para minimizar el nivel de vulnerabilidades como son el uso de sistemas adecuados para prevenir todo tipo de desastre, y el control de acceso al personal no autorizado, que son los elementos clave para minimizar el riesgo de pérdida de equipo de computo y así también la información dentro del centro de computo, pero está lejos de un optimo rendimiento de seguridad, por lo que de un 100% como promedio total de la seguridad física solo se obtuvo el 72% de promedio en esta variante de la seguridad.

SEGURIDAD FISICA

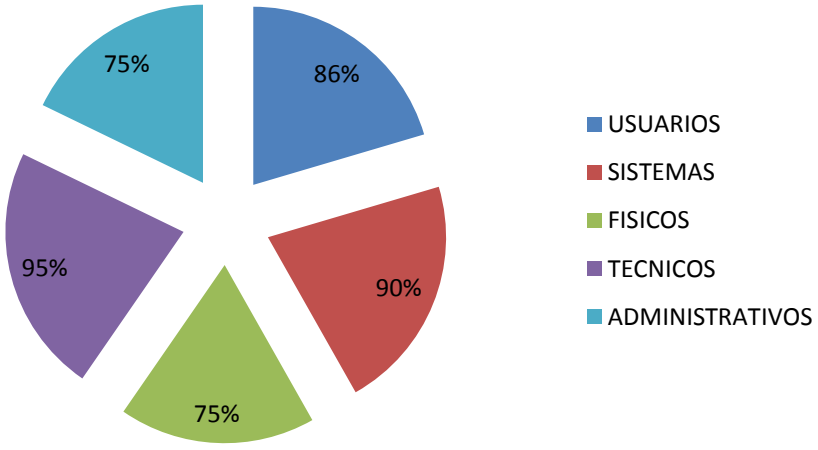


Como se observa en el grafico anterior el centro de computo no cuenta con la estructura adecuada, ya que se obtuvo la mitad de porcentaje y tampoco cuenta con el acceso y control adecuado por lo que no es seguro el equipo que se encuentra en este centro.

Los datos que generan el grafico 2, se enfoca a la seguridad lógica en base a los usuarios, sistemas, físicos, técnicos y administrativos, esto debido al tipo de preguntas realizadas en los cuestionarios, se aprecia baja la vulnerabilidad en comparación con las medidas de protección existentes, el centro de computo cuenta con firewalls (cortafuegos) y segmentación de la red entre otras protecciones.

Con las respuestas obtenidas por parte del administrador se puede decir que el centro de cómputo cuenta con un buen sistema de autenticación para el acceso a sus sistemas aunque no es el óptimo, como se muestra en el promedio total de cada uno de los elementos que complementan la seguridad lógica.

SEGURIDAD LOGICA



Sin duda alguna, una de las mayores fortalezas del centro de cómputo de la empresa AAK es la forma de administración y control que posee sobre los sistemas, esto debido a que cuenta con un buen sistema de procedimientos, además de contar con personal interno capacitado, para mantener la red en buen estado de comunicación y protección. En las actualizaciones que realiza el centro de cómputo, mantiene un bajo nivel de

vulnerabilidades, nivel que es generado en el centro de cómputo de la misma empresa el cual no funciona al 100% en conjunto con el resto de la infraestructura.

CONCLUSION

En el conjunto de todos los resultados, podemos concluir que la seguridad en el centro de computo de la empresa Aarhuskarlshman S.A. de C.V. posee una baja vulnerabilidad, en base a los resultados arrojados por la metodología de auditoría de seguridad como son: el panorama general de la red, el control y acceso al centro de computo sin las medidas necesarias para evitar accesos de personal no autorizado, la evaluación de la autentificación y en la administración y control que se tiene en la red de información de datos del centro de computo.

Además cabe referir que si alguna de estas vulnerabilidades es detectada por atacantes, el sistema se puede ver completamente comprometido. Ya que se tienen los resultados del análisis de la metodología de la auditoría de seguridad y se está en posición de tomar decisiones con respecto al mejoramiento de la seguridad, por lo tanto a continuación se muestran algunas alternativas y/o propuestas para disminuir las vulnerabilidades existentes de amenazas y riesgos informáticos.

Propuestas de seguridad

- Los usuarios deben usar autenticación múltiple para las conexiones remotas.
- El administrador del centro de computo debe de dar capacitación para los usuarios con respecto a la seguridad en la red y se deben tocar los temas:
  - Definición de seguridad
  - Deberes que debe cumplir para una seguridad integral
  - La importancia de las políticas en el centro de computo
  - Informes sobre actividades sospechosas
  - Confidencialidad en la información
  - Seguridad de correo electrónico incluyendo SPAM

- Seguridad de internet incluyendo navegación por la web de descargas de aplicaciones
- Seguridad informática incluyendo el uso de cortafuegos particulares y cifrado

El administrador de red debe informar al usuario sobre:

- Seguridad de las operaciones
- Seguridad de la infraestructura
- Seguridad de las aplicaciones
- Preparación para incidentes y reacciones por algún tipo de desastre natural
- Detectores de movimiento
- Verjas detectores de humo y fuego
- Guardias de seguridad y monitorización por televisión de circuito cerrado
- Sistemas de tarjetas de identificación sensores y alarmas
- Cerraduras y llaves
- Candados cifrados
- Extintores contra incendios
- Bloqueo de teclados
- Rotación de responsabilidades
- Programa de control de acceso
- Tarjetas inteligentes
- cifrado

RECOMENDACIONES

Como resultado de mi investigación relacionada con la aplicación de un instrumento de medición, basado en la aplicación de la auditoría de seguridad de la red de información en un centro de cómputo como propuesta en la solución de problemas cotidianos recomiendo lo siguiente:

Es recomendable que el administrador del Centro de Cómputo proponga respuestas a los problemas de riesgos y amenazas informáticas que puedan existir, con el propósito de que los usuarios no se acostumbren a resolver solo problemas con respuestas únicas.

PERSPECTIVAS

Lo que se puede esperar de este proyecto es que sirva de base, analice el escrito y lo comprenda, después lo ponga en práctica incluyendo algunas estrategias que contemplen el proyecto, para que en lo futuro se inicien nuevas propuestas que enriquezcan la problemática abordada en las amenazas informáticas y lograr el objetivo planteado.

Este trabajo servirá de consulta y apoyo para otros usuarios que se vean enfrentados en un problema igual o parecido, en la consulta ampliara su conocimiento para tratar el problema y cometer errores que perjudiquen las redes de información.

Se espera también con la aplicación de esta propuesta sirva de reconocimiento sobre utilidad en la Red de Información del centro de computo.

Para finalizar espero que mi proyecto de análisis y propuesta sea de utilidad para aquellos usuarios que deseen retomarlo y aplicarlo, para solucionar problemas en los centros de computo que tengan redes de información, dejando su criterio todas las modificaciones necesarias que enriquezcan este trabajo.

BIBLIOGRAFIA

Aguilera, P. (2005). *Seguridad informatica.*

Asensio, G. (2006). *Seguridad en internet.*

Calle, J. A. (2005). *Reingeniería y seguridad en el ciberespacio.*

Copyright. (2005). *Red hat enterprise linux 4: security guide.*

E., C. (2006). Auditoria informática. Mexico.

Elinos, L. A. (2011). *Auditoría informática.*

Falcon, J. C. (2006).

Firtman, S. (2005). *Seguridad informática.*

Fisher, R. P. (1988). *Seguridad en los sistemas informáticos.*

Francisco, A. (2009). Sniffer.

Gil, P. C. (1997). *Seguridad informática, técnicas criptograficas.*

Gómez, R. (2007). *Generalidades en la auditoría.*

Gustavo, T. (2006).

Hernández, R. (1991). *Metodología de la investigación.*

Israel, J. V. (s.f.). Analisis de diseño.

Kendall, K. y. (2005).

Kendall, K. y. (2005). *Analisis y diseño de sistemas.*

Lamere, J. M. (1987). *La seguridad informática.*

Martin, C. (2006).

Meza, R. C. (s.f.). Administración de centros de cómputo. Morelia, Michoacán.

Miret, B. R. (2006). *Seguridad informática.*

Peso, M. G. (2001). *auditoria informática un enfoque practico.*

Ramos, M. A. (2008). *Auditoria informática.* Mexico.

Ramos, M. Á. (2008). *Auditoria Informática.* Mexico.

Rivas, G. A. (1988). *Auditoria informática.*

Royer, J. M. (2004). *Seguridad en informática de empresas.*

Vieites, Á. G. (2006). *Enciclopedia de la seguridad informática.*