UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

METODOLOGÍA PARA EL DESARROLLO DE LA AUDITORÍA EN SEGURIDAD DE REDES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

SERAPIO VICTOR MORENO VEGA

PROMOCIÓN
2000-II

LIMA – PERU
2005

METODOLOGÍA PARA EL DESARROLLO DE LA AUDITORÍA EN SEGURIDAD DE REDES

Dedico este trabajo a:

Mis padres, Mis Hermanos, por el apoyo incondicional en mi carrera.

SUMARIO

El presente trabajo pretende describir una metodología de auditoría relacionada a la seguridad de la red utilizando la herramienta de objetivos de control para tecnología de información y tecnologías relacionadas (COBIT). La cual habilita una política clara y de buenas prácticas de control de tecnología de información a través de organizaciones.

En el capitulo I se presentan conceptos de tecnología de información, se explican conceptos de redes, seguridad a nivel de red, la organización administrativa y la necesidad de control y planeamiento eficiente.

El capitulo II se refiere a la administración de riesgos de tecnologías de información y comunicación (TIC), en el cual se describe el riesgo que presenta la tecnología de información en una entidad u organización cuando no se realiza una buena planificación, aquí se presentan conceptos de análisis de riesgos y las contramedidas para disminuir el riesgo de TIC así como también se revisa conceptos generales de la ISO 17.799 que está relacionado a la seguridad de información. También, se ve en este capitulo concepto de objetivos de control de tecnología de información (COBIT).

En el capitulo III se revisan los conceptos sobre Auditoría TIC el enfoque, las fases y normas.

El capitulo IV presenta un caso practico de auditoría sobre seguridad de redes, en el cual se detalla bajo la metodología COBIT, los diferentes procesos llevados para realizar la auditoría.

ÍNDICE

PRÓLOGO

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Verdaderamente, la información y los sistemas de información son influyentes en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos). Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar, sin embargo, también comprenden y administran los riesgos asociados con la implementación de la tecnología. Por lo tanto, la administración debe tener apreciación y un entendimiento básico de los riesgos y limitaciones del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

En el mundo cambiante en el cual las organizaciones deben enfrentar el reto de lograr un equilibrio entre sus objetivos institucionales y los riesgos que en sus procesos supone el uso de la tecnología, se requiere una administración completa de los riesgos en la seguridad en todos los ámbitos con un enfoque coordinado y estratégico, ya que cuando se aprovechan de las vulnerabilidades, el impacto puede ser significativo; desde el simple costo de la substitución del bien hasta pérdidas masivas. Cuando los problemas de seguridad afectan a los clientes, los impactos pueden ser críticos.

El problema más grande para muchos gerentes de seguridad es que su personal esté completamente consciente de la necesidad e importancia de mantener una seguridad en tecnologías de información y comunicación (TIC) efectiva dentro de la empresa. Si no existe una buena cultura de seguridad dentro del lugar de trabajo, la

efectividad de muchas inversiones de la organización en las medidas sistemáticas de prevención se verá disminuida.

Por lo tanto, la administración debe decidir la inversión razonable en seguridad y control en TIC y como lograr un balance entre riesgos e inversiones en control que es frecuentemente impredecible.

Existe una creciente necesidad entre los usuarios en cuanto a la seguridad de los servicios de TIC, a través de la acreditación y la auditoría de servicios de TIC proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados. Actualmente, es confusa la implementación de buenos controles TIC en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan una base general a ser establecida como primer paso. Ante esta confusión de diferentes estándares nace COBIT.

Objetivos de control para tecnología de información y tecnologías relacionadas (COBIT), ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas practicas de seguridad y control en TIC. COBIT es la herramienta innovadora para el gobierno de TIC.

COBIT, es una herramienta de gobierno de TIC que ha cambiado la forma en que trabajan los profesionales de TIC. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT ayuda a satisfacer las múltiples necesidades de la administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos de TIC. Provee buenas prácticas a través de un dominio y el marco referencial de los procesos y presenta actividades en una estructura manejable y lógica.

COBIT trae como resultado, el marco referencial general y las directrices de auditoría; el marco de referencia general describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TIC que son impactados en forma primaria por cada objetivo de control y de los objetivos de control detallados (anexo A), la directrices de auditoría contienen los pasos de auditoria correspondientes a cada uno de los 34 objetivos de control de TIC de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TIC con respecto a los 318 objetivos detallados de control (anexo A) recomendados para proporcionar a la gerencia certeza o algunas recomendaciones de mejoramiento.

CAPÍTULO I

1 TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC).

Actualmente toda empresa de acuerdo a su negocio implica el uso de tecnología de información en grado mayor o menor, por lo cual es necesario un conocimiento básico.

1.1 CONCEPTOS BÁSICOS DE REDES.

A lo largo de los años el uso intensivo de los computadores hizo surgir la necesidad de compartir datos almacenados en estos computadores y también de compartir los recursos de hardware y software. Por ejemplo, el compartimiento de una impresora por varios computadores o el uso de un software sin que sea necesario adquirir una licencia para cada computador. Una base de datos almacenada en un computador sin que sea necesario duplicarla.

1.1.1 REDES DE DATOS.

Consideraremos una red como un conjunto de computadores capaces de comunicarse entre sí, bien directamente, bien a través de otros. Como en toda comunicación, para que ésta sea posible, necesitamos un idioma que sea comprendido por todos los integrantes, en este caso, los computadores de la red. En este contexto el idioma es el protocolo de comunicación.

El aumento en el uso de los computadores hizo surgir la necesidad de compartir datos e informaciones almacenadas en cada uno de estos.

Se puede definir una red informática como un conjunto de equipos conectados entre si con la finalidad de compartir información y recursos.

1.1.2 MODELO OSI Y ETHERNET.

En 1978, la international standards organization, ISO (Organización Internacional de Estándares) divulgó un conjunto de especificaciones que describían la arquitectura de red para la conexión de dispositivos diferentes. El documento original se aplicó a sistemas que eran abiertos entre sí, debido a que todos ellos podían utilizar los mismos protocolos y estándares para intercambiar información.

En 1984, la ISO presentó una revisión de este modelo y lo llamó modelo de referencia de interconexión de sistemas abiertos (OSI) que se ha convertido en un estándar internacional y se utiliza como guía para las redes.

El modelo OSI es la guía mejor conocida y más ampliamente utilizada para la visualización de entornos de red. Los fabricantes se ajustan al modelo OSI cuando diseñan sus productos para la red; éste ofrece una descripción del funcionamiento conjunto de hardware y software de red por niveles para posibilitar las comunicaciones. El modelo también ayuda a localizar problemas proporcionando un marco de referencia que describe el supuesto funcionamiento de los componentes.

1.1.3 ARQUITECTURA DEL MODELO OSI.

La arquitectura del modelo de referencia OSI divide la comunicación en red en siete niveles. Cada nivel cubre diferentes actividades, equipos o protocolos de red. El modelo OSI define cómo se comunica y trabaja cada nivel con los niveles

inmediatamente superior e inferior. Por ejemplo, el nivel de sesión se comunica y trabaja con los niveles de presentación y de transporte.

Cada nivel proporciona algún servicio o acción que prepara los datos para entregarlos a través de la red a otro equipo. Los niveles inferiores (1 y 2) definen el medio físico de la red y las tareas relacionadas, como la colocación de los bits de datos sobre las placas de red (NIC, Network Interface Cards) y el cable. Los niveles superiores definen la forma en que las aplicaciones acceden a los servicios de comunicación. Cuanto más alto es el nivel, más compleja es su tarea. Los niveles están separados entre sí por fronteras llamadas interfaces. Todas las demandas se pasan desde un nivel, a través de esta interfaz, hacia el siguiente.

1.1.4 RELACIÓN ENTRE NIVELES DEL MODELO OSI.

La comunicación según el modelo OSI siempre se realizará entre dos sistemas. Supongamos que la información se genera en el nivel 7 de uno de ellos, y desciende por el resto de los niveles hasta llegar al nivel 1, que es el correspondiente al medio de transmisión (por ejemplo el cable de red) y llega hasta el nivel 1 del otro sistema, donde va ascendiendo hasta alcanzar el nivel 7. En este proceso, cada uno de los niveles va añadiendo a los datos a transmitir la información de control relativa a su nivel, de forma que los datos originales van siendo recubiertos por capas de datos de control. De forma análoga, al ser recibido dicho paquete en el otro sistema, según va ascendiendo del nivel 1 al 7, va dejando en cada nivel los datos añadidos por el nivel equivalente del otro sistema, hasta quedar únicamente los datos a transmitir. Los niveles OSI se entienden entre ellos, es decir, el nivel 5 enviará información al nivel 5 del otro sistema (lógicamente, para alcanzar el nivel 5 del otro sistema debe

recorrer los niveles 4 al 1 de su propio sistema y el 1 al 4 del otro), de manera que la comunicación siempre se establece entre niveles iguales, a las normas de comunicación entre niveles iguales es a lo que llamaremos protocolos. Este mecanismo asegura la modularidad del conjunto, ya que cada nivel es independiente de las funciones del resto, lo cual garantiza que a la hora de modificar las funciones de un determinado nivel no sea necesario rescribir todo el conjunto. En las familias de protocolos más utilizadas en redes de computadores (TCP/IP, IPX/SPX, etc.) nos encontraremos a menudo funciones de diferentes niveles en un solo nivel, debido a que la mayoría de ellos fueron desarrollados antes que el modelo OSI.

1.1.5 TOPOLOGÍA DE REDES.

Cuando hablamos de topología de una red, hablamos de su configuración. Esta configuración recoge tres campos: físico, eléctrico y lógico. El nivel físico y eléctrico se puede entender como la configuración del cableado entre máquinas o dispositivos de control o conmutación. Cuando hablamos de la configuración lógica tenemos que pensar en cómo se trata la información dentro de la red, como se dirige de un sitio a otro o como la recoge cada estación. Así pues, para ver más claro como se pueden configurar las redes explicaremos de manera sencilla cada una de las formas que pueden tomar.

1.1.5.1 TOPOLOGÍA EN ESTRELLA.

Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al nodo central de la red, que se encarga de gestionar las transmisiones de información por toda la estrella. Evidentemente, todas las tramas de

información que circulen por la red deben pasar por el nodo principal, con lo cual un fallo en él provoca la caída de todo el sistema.

Por otra parte, un fallo en un determinado cable sólo afecta al nodo asociado a él; si bien esta topología obliga a disponer de un cable propio para cada terminal adicional de la red. La topología de estrella es una buena elección siempre que se tenga varias unidades dependientes de un procesador, esta es la situación de una típica mainframe, donde el personal requiere estar accesando frecuentemente esta computadora. En este caso, todos los cables están conectados hacia un solo sitio, esto es, un panel central. Equipo como unidades de multiplexaje, concentradores y pares de cables solo reducen los requerimientos de cableado, sin eliminarlos y produce alguna economía para esta topología. Resulta económico la instalación de un nodo cuando se tiene bien planeado su establecimiento, ya que requiere de un cable desde el panel central, hasta el lugar donde se desea instalarlo.

1.1.5.2 TOPOLOGÍA EN BUS.

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable: el bus. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cual es la que le corresponde.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red.

Por otra parte, una ruptura del bus es difícil de localizar (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

Como ejemplo más conocido de esta topología, encontramos la red ethernet de xerox. El método de acceso utilizado es el CSMA/CD, método que gestiona el acceso al bus por parte de los terminales y que por medio de un algoritmo resuelve los conflictos causados en las colisiones de información. Cuando un nodo desea iniciar una transmisión, debe en primer lugar escuchar el medio para saber si está ocupado, debiendo esperar en caso afirmativo hasta que quede libre. Si se llega a producir una colisión, las estaciones reiniciarán cada una su transmisión, pero transcurrido un tiempo aleatorio distinto para cada estación.

El bus es la parte básica para la construcción de redes ethernet y generalmente consiste de algunos segmentos de bus unidos ya sea por razones geográficas, administrativas u otras.

1.1.5.3 TOPOLOGÍA EN ANILLO.

Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información.

En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando. La topología de anillo esta diseñada como una arquitectura circular, con cada nodo conectado

directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado. Este esquema de cableado muestra alguna economía respecto al de estrella.

El anillo es fácilmente expandido para conectar más nodos, aunque en este proceso interrumpe la operación de la red mientras se instala el nuevo nodo. Así también, el movimiento físico de un nodo requiere de dos pasos separados: desconectar para remover el nodo y otra vez reinstalar el nodo en su nuevo lugar.

1.1.6 PROTOCOLOS DE COMUNICACIONES.

Los protocolos son reglas y procedimientos para la comunicación.

El término protocolo se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Con respecto a los protocolos de red se puede decir:

- Existen muchos protocolos. A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.
- Algunos protocolos solo trabajan en ciertos niveles OSI. El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.

- Los protocolos también puede trabajar juntos en una jerarquía o conjunto de protocolos. Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

1.1.7 TIPOS DE REDES.

1.1.7.1 REDES DE ÁREA LOCAL (LAN).

Las redes de área local (Local Area Networks - LAN) son sistemas de comunicaciones que proporcionan interconexión a una variedad de dispositivos en un área restringida (recinto, edificio, campus, etc.) y que no utilizan medios de telecomunicación externos.

Supongamos que existe un conjunto de ordenadores interconectados entre si, y todos ellos necesitan imprimir datos. En vez de tener cada puesto o terminal una impresora se podría tener un servidor de impresoras, como una sola impresora para todos los computadores o terminales. De esta forma estamos compartiendo recursos tales como el hardware, y por otro lado estamos economizando, puesto que ahorramos comprar más impresoras para el resto de los equipos. Una red de área local, se suele proveer también para compartir información, así pues todos los puestos o terminales podrían trabajar sobre una única información, evitando una posible redundancia de datos u

otros problemas, con esto estaríamos compartiendo recursos como el software. Y al igual que en el caso anterior estamos también economizando, puesto que no necesitamos que todos los computadores de una LAN tengan mucha capacidad de disco duro, nos basta con que lo tenga un solo computador que será el que la almacene.

Son características de las LANs:

- Utilización de medios privados de comunicación.
- Amplitud que va desde metros hasta pocos kilómetros.
- Velocidad de transmisión elevada (de 1 a 100 Mbps, incluso mayores).
- Comunicación de igual a igual (Peer-to-Peer) de los dispositivos conectados.
- Posibilidad de conexión con otras redes mediante pasarelas o gateways.

Una LAN está formada por muchos segmentos de velocidades diferentes (diseño jerárquico), siendo un segmento un conjunto de estaciones interconectadas mediante una LAN de un único tipo, con idénticas características de acceso para todas las estaciones.

Los dispositivos de interconexión más utilizados en una red son:

- **Hubs**. dispositivos que interconectan a nivel físico (como un repetidor). Lo único que hacen es reconstruir la señal.
- **Puentes (bridges)**. interconectan a nivel de enlace de datos. Lo que hacen es copiar tramas. Además, también realizan un filtrado del tráfico en función de la dirección MAC.
- **Encaminadores (routers)**. son elementos de interconexión a nivel de red. Cuando recibe un paquete, analiza su dirección destino y con base en un

algoritmo de encaminamiento, decide por qué línea de salida retransmite el paquete.

- **Conmutadores (switches)**. son dispositivos que pueden interconectar a nivel dos o a nivel tres. La diferencia con respecto a los bridges y routers es la tecnología interna de interconexión. Los conmutadores realizan conmutación, con lo cual las colisiones no son posibles.

La tendencia hoy en día es a una mayor utilización de los conmutadores de los puentes y routers, ya que en un segmento que une dos conmutadores no pueden haber colisiones, y eso mejora le eficiencia de la red.

Por lo tanto, las redes conmutadas están ganando terreno a las redes compartidas.

Así, en una LAN, encontraremos normalmente hubs, que se encargan de distribuir la señal y dan lugar a colisiones, y conmutadores, que se encargan de encaminar el paquete a su destino y no dan lugar a colisiones.

1.1.7.2 REDES DE ÁREA METROPOLITANA (MAN).

Son una versión mayor de la LAN y utilizan una tecnología muy similar. Actualmente esta clasificación ha caído en desuso, normalmente sólo distinguiremos entre redes LAN y WAN.

1.1.7.3 WAN (RED DE ÁREAS EXTERNAS).

Son redes que se extienden sobre un área geográfica extensa. Contiene una colección de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Los cuales están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host

acceden a la subred de la WAN por un router. Suelen ser por tanto redes punto a punto.

Una WAN contiene numerosos cables conectados a un par de encaminadores. Si dos encaminadores que no comparten cable desean comunicarse, han de hacerlo a través de encaminadores intermedios. El paquete se recibe completo en cada uno de los intermedios y se almacena allí hasta que la línea de salida requerida esté libre.

Se pueden establecer WAN en sistemas de satélite o de radio en tierra en los que cada encaminador tiene una antena con la cual poder enviar y recibir la información. Por su naturaleza, las redes de satélite serán de difusión.

1.1.8 INTERNET.

Internet se usa con el fin de distribuir cualquier tipo de datos que podamos imaginar incluyendo, música y video, sin embargo, el rápido correo electrónico es el principal elemento de tráfico.

Ahora es posible que cualquier hogar que posea el equipo necesario se conecte a internet a través de la red telefónica ya existente. La supercarretera de los datos (supercarretera de la información), que está trayendo la televisión vía satélite a los hogares, también se está utilizando como una conexión a internet. Muchas organizaciones (incluyendo los gobiernos y las corporaciones públicas) están ofreciendo servidores de datos en internet, a los que se puede tener acceso por una pequeña cantidad de dinero. La serie de servidores se ha hecho conocida como world wide web (www) y toda una industria ha crecido a su alrededor.

Algunos productos para PC tale como: netscape e internet explorer y otros, permiten al usuario ingresar a la red navegando e investigando en las bases de datos en

cualquier parte del mundo. El acceso público se ha hecho popular a través de una cadena de cafés llamados "Ciber Cafés", en donde por una pequeña cantidad de dinero se puede comprar tiempo de computador para ingresar a la red.

1.1.9 INTRANET.

Intranet es el término que describe la implantación de las tecnologías de internet dentro de una organización, más para su utilización interna que para la conexión externa.

Esto se realiza de forma que resulte completamente transparente para el usuario, pudiendo éste acceder, de forma individual, a todo el conjunto de recursos informativos de la organización, con menos costo, tiempo y esfuerzo. Intranet e internet, son casi por completo distinciones semánticas, más que tecnológicas.

Intranet utiliza exclusivamente el modelo world wide web, adaptado a su situación y estructura interna, de forma que esta información quede en los límites planteados por la propia organización. Los miembros de la misma utilizarán, como es presumible, clientes web para acceder a la información. Se implantarán, por lo tanto, protocolos TCP/IP, y se utilizará el HTML para la creación de documentos.

La disparidad de plataformas y sistemas informáticos existentes en una organización, y los problemas para compartir información entre ellos, fuerzan a los responsables de los sistemas de información a buscar soluciones de integración, de resultados fiables y a un costo aceptable.

La utilización de la tecnología world wide web se debe a su facilidad de implantación, su bajo costo, y la rápida aceptación por parte del usuario, así como

por su portabilidad a las diferentes plataformas, y su capacidad para interactuar con aplicaciones diversas.

Los factores que influyen poderosamente en la utilización de la intranet pueden resumirse como sigue:

- Costo accesible.
- Fácil adaptación y configuración a la infraestructura tecnológica de la organización, así como gestión y manipulación.
- Adaptación a las necesidades de diferentes niveles: empresa, departamento, área de negocio. Sencilla integración de multimedia.
- Disponible en todas las plataformas informáticas.
- Posibilidad de integración con las bases de datos internas de la organización.
- Rápida formación del personal.
- Acceso a la internet, tanto al exterior, como al interior, por parte de usuarios registrados con control de acceso.
- Utilización de estándares públicos y abiertos, independientes de empresas externas, como puede ser TCP/IP o HTML.

1.2 SEGURIDAD EN REDES DE DATOS.

En la actualidad muchas empresas confían sus negocios, en gran manera, al comercio electrónico. La integración de internet con las operaciones de negocios ha traído como resultado un costo efectivo para las empresas. Por otro lado los usuarios residenciales utilizan accesos a internet de baja velocidad como cable modem y DSL (Digital Suscriber Line). El punto es que internet esta creciendo en capacidad de tráfico e medida que se brindan nuevos servicios.

Acompañado de este crecimiento de internet viene el incremento de amenazas de internet relacionado a ataques. Históricamente cuando se hablaba de un robo esto se asociaba a un intruso que interrumpía en propiedad privada y robaba algo de valor, es decir el ladrón debía tener un acceso físico a la propiedad para poder robarla. Sin embargo, internet permite que los robos se puedan efectuar desde cualquier lugar del mundo a una propiedad que tenga acceso vulnerable.

La implementación de seguridad en una red es crucial para mantenerla operando, así como la continuidad de la satisfacción del negocio.

Es necesario saber que hay numerosas localidades en una red que son susceptibles a ataques electrónicos. Entender cuales son estas áreas es el primer paso para mejorar la seguridad. También es vital conocer que tipos de herramientas usan los hackers contra la red. Los hackers usan varios tipos de herramientas para conseguir el acceso no autorizado a la red de datos. Todos estos ataques representan una constante amenaza a la red y lo más importante a la reputación de la compañía. Amenazas de seguridad se pueden distinguir en varias categorías.

1.2.1 AMENAZAS DE SEGURIDAD.

Los nuevos negocios usan el internet para captar millones de potenciales clientes. La extranet habilita eficiente y efectiva comunicación entre personas que realizan negocios. En intranet, los empleados pueden confiar en realizar reservaciones o llenar formulas de viajes. El servicio de e-mail es habilitado a cada empleado para comunicarse rápida y eficientemente con personas a través de mundo.

Un problema con la computadora de un usuario sería un problema para el usuario pero que pasa si falla la operación del comercio web, la compañía podría perder

millones de dólares por día. Los empleados no podrían producir si la red empieza a fallar. Además las redes no solo deben de estar operativas, también deben de estar interconectadas a otras redes para poder ser útiles. Es así que el factor seguridad debe de ser considerado pues cada host conectado a internet es susceptible a ataques, y sabemos que para estos ataques no hay límites geográficos. Sin embargo, los procedimientos de seguridad para prevenir ataques de hackers son usualmente menos pensados (si existen del todo). Una red insegura definitivamente será atacada, la única pregunta es ¿cuándo?. Aún si se piensa que la información no es importante para el hacker la seguridad de la red puede ser atacada. Los hackers buscan determinadas plataformas a atacar poniendo en práctica sus técnicas para futuros nuevos ataques. Ataques en la red tienen 2 atributos. El primer atributo es el nivel de entrenamiento de los hackers, el nivel puede ser bajo, no estructurado, o puede ser alto, estructurado. El segundo atributo es la localización física desde donde el ataque es lanzado, esto puede ser lanzado desde una red externa o una localización interna.

1.2.1.1 AMENAZA DE ATAQUE NO ESTRUCTURADO.

Muchos ataques no estructurados son realizados por script kiddies (personas que no tienen conocimientos en programación pero que hacen uso de los scripts desarrollados por programadores para realizar un ataque), algunos otros son ejecutados por hackers. En su mayoría estos ataques son realizados para obtener satisfacción personal, en poco porcentaje estos ataques son de naturaleza maliciosa. A pesar que la experiencia de estos atacantes es mínima, este tipo de ataques puede afectar la red y representa una significativa amenaza. En algunos casos simplemente ejecutando un script puedes dejar fuera de funcionamiento la red.

1.2.1.2 AMENAZA DE ATAQUE ESTRUCTURADO.

Estos ataques vienen de adversarios que son altamente motivados y técnicamente competentes. No como script kiddies (novatos), los atacantes tienen la competencia técnica para entender las nuevas herramientas existentes, adaptan las actuales herramientas de hacking y desarrollan nuevas herramientas personalizadas. Estos atacantes actúan solos o en pequeños grupos. Ellos entienden, desarrollan y usan sofisticadas técnicas de hacking para penetrar insospechadas organizaciones.

La motivación que hay detrás de estos atacantes es variada. El factor de motivación común es el dinero, activismo político, enojo o venganza, y retribución por algún daño. El crimen organizado, competencia industrial, y grupos de propagandistas contratan expertos para lanzar estos ataques. Otra de las motivaciones es el reto de adueñarse de los códigos fuente de competidores potenciales. La mayoría de los fraudes y robos recaen en esta categoría de ataque.

A pesar de sus motivaciones, los atacantes pueden causar serios daños en tu red. Un ataque exitoso puede destruir tu negocio por completo. Muchas veces la meta de ataques estructurados es destruir a un competidor.

1.2.1.3 AMENAZA DE ATAQUE EXTERNO.

Son conocidos también como ataques ejecutados sin acceso privilegiado a la red. Usuarios de computadoras alrededor del mundo pueden ser capaces de lanzar ataques externos. Esto nos dice que existen millones de potenciales atacantes a la red a través de internet.

Se usa un perímetro de defensa (firewall) como la primera línea de defensa contra amenazas de ataque externo. Organizaciones usualmente invierten mucho tiempo y dinero en mantener protegido su perímetro de defensa de ataques externos.

1.2.1.4 AMENAZA DE ATAQUE INTERNO.

En ataques internos, un atacante tiene algún nivel inicial de acceso al sistema. El acceso inicial puede ser la cuenta a un servidor o acceso físico a la red. Además, este acceso no es disponible al público en general. Descontentos ex-empleados, existentes empleados, y contratistas, usualmente tienen el acceso necesario para conducir ataques internos.

Algunas veces, un ataque estructurado a la red es conducida con la ayuda de alguien interno. En este caso el ataque llega a ser del tipo interno. Un ataque estructurado interno representa el más severo ataque que puede ser lanzado contra una red.

1.2.2 CONCEPTO DE SEGURIDAD.

Entender este concepto es importante para poder definir políticas de seguridad adecuadas en la red. Además, muchos ataques explotan la debilidad de una o más de estas políticas. Otras veces estas políticas ayudan a minimizar el ataque a la red.

La política de seguridad es una sentencia formal de reglas por la cual el acceso a la red es controlado. Todo el acceso a la información debe ser regido bajo estas reglas.

A continuación se nombrarán las áreas concernientes a las políticas de seguridad en las cuales se necesita dirigir esfuerzos para lograr una red segura:

- **Autenticación**. Se refiere al proceso de confiabilidad que determina la identidad de una entidad de comunicación. Esta entidad puede ser un usuario individual o un proceso de software.
- **Autorización.** Se refiere a las reglas que determinan quien tiene permiso para acceder a diferentes recursos de la red.
- **Confidenciabilidad.** Asegura que los datos están protegidos de ser divulgados por partes no autorizadas. Específicamente, la confidenciabilidad requiere que la información local, del computador (en memoria o disco) y en transito (a través de la red) sea accesible solo con privilegio de lectura para usuarios autorizados.
- **Integridad**. Un sistema protege la integridad de los datos si se previene modificaciones no autorizadas. Modificación incluye creación, cambios, escritura, eliminación y reenvió de mensajes transmitidos.
- **Disponibilidad**. Un sistema de computadoras activas esta disponible para partes autorizadas cuando haya necesidad de definir disponibilidad. El caso de ataque por denegación de servicio (DoS) es revertir la disponibilidad de recursos del sistema, algunas veces temporalmente y otras de manera permanente.

1.2.3 FASES DE UN ATAQUE.

Los ataques son usualmente divididos en tres distintas fases. La primera fase involucra la meta del ataque. La segunda fase es de reconocimiento, también conocida como concurrencia de información. Durante esta fase, el atacante se dedica a la recolección de información acerca de la red para determinar el objetivo del

ataque. Después de la recolección de información, el atacante pasa a la tercera fase que es la fase de ataque.

1.2.3.1 PRIMERA FASE: LA METAS DE UN ATAQUE.

Antes de atacar una red o sistemas, el atacante define sus metas u objetivos, como por ejemplo:

- Manipulación de datos.
- Acceso al sistema.
- Elevar privilegios.
- Denegar disponibilidad de recursos de red.

Un atacante podría tener una simple meta, tal como buscar algún sistema que este corriendo determinado sistema operativo (OS) para usar una nueva herramienta que ha encontrado. El atacante podría estar tratando de obtener comercios secretos bien protegidos de un competidor.

Como se menciono anteriormente, la motivación que mueve estas practicas pueden ser: revancha, activismo político, ganancia financiera.

1.2.3.2 SEGUNDA FASE: RECONOCIMIENTO ANTES DE UN ATAQUE.

La recolección de información es el segundo paso para lanzar un ataque. El éxito de esta fase es también la clave del éxito del ataque. Los atacantes hacen uso de dos mecanismos para la recolección de información:

- **Fuente de datos publico**. Algunas veces, un atacante busca el conocimiento a través de información pública disponible en la compañía. A pesar que esta

información es libremente disponible, esta información puede brindar al atacante información de la compañía como: donde el negocio esta ubicado, quienes están asociados a la compañía, el valor activo de la compañía y mucho más. Se puede recolectar usernames y nombres de los productos para ingresar como usuario invitado y atacar la red.

- **Escaneo y sondeo de información**. Un atacante empieza con una búsqueda de datos públicos o escaneo electrónico. A través del escaneo, el atacante usa reconocimiento remoto para encontrar un específico recurso en la red, remoto reconocimiento o recolección de información es un método no autorizado de mapeo de sistemas, servicios o vulnerabilidades de la red. La meta de recolección de información es localizar los puntos débiles en la red donde un ataque comúnmente es exitoso. Al ser localizado un específico punto de debilidad en una red, el atacante puede lanzar un ataque en el futuro. El atacante podría recolectar información de la red desde la propia conexión a internet. Otro potencial camino es buscar potenciales líneas dial-up usando una herramienta que marca un rango de números con la intención de buscar conexiones de módems.

Un atacante empieza su reconocimiento al escoger un específico objetivo de la red. Una manera de obtener información de los IPs que usa una red específica es brindada por el DNS (Domain Name Server). Este DNS simplemente resuelve el nombre de un host a su número IP.

El intruso hace uso de la técnica conocida como ping sweep (barrido de ping) que simplemente consiste en el envió de un paquete ICMP echo request a todas las direcciones IP de una red especifica, los hosts actualmente conectados a la red

responden con un echo reply que envía la información de la dirección IP del host que esta actualmente conectado. Luego de obtener la dirección IP, el atacante determina que servicios o puertos están habilitados en el host. De esta manera el intruso conocerá los servicios que se encuentran activos y si es posible acceder a la versión del servicio. También se puede obtener la información de que sistema operativo esta corriendo en cada host. Básicamente el atacante quiere conocer tanta información sea posible acerca de los sistemas de la red para incrementar la posibilidad de que el ataque sea exitoso.

Los maliciosos hackers también buscan específicos ítems, como:

a) Sistema operativo y vulnerabilidades.
b) Protocolo con conocidas debilidades.
c) Servicios en uso.
d) Topología de red.

Obteniendo la topología de la red, el atacante puede construir una poderosa herramienta que una fecha después puede conducir un ataque en la red. Los ataques contra la red caen en dos categorías:

- Ganar acceso.
- Denegación de servicio.

1.2.3.3 TERCERA FASE: EL ATAQUE.

Luego de que el atacante mapea la red, investiga conocidas vulnerabilidades que ha detectado en el sistema. Algunas veces, el atacante posee herramientas que están

listas para explotar las vulnerabilidades de la red. La meta del atacante en este caso es ganar acceso a los recursos de la red.

Si se logra el acceso a un host, una meta común del atacante es elevar sus privilegios en el sistema, privilegios de administrador. Con acceso privilegiado, el atacante tiene acceso no restringido a todos los datos y servicios de los host. Ganar acceso a un host es comprometerlo. Es decir, todos los programas y servicios del host no son confiables. Así relaciones confiables entre host son comprometidas y el atacante puede ganar acceso a otros host en la red. Frecuentemente este proceso sigue hasta que el atacante haya tenido el control total de la red.

Después de comprometer los host de la red, el atacante puede instalar back doors (puertas traseras) para futuros accesos sin ser detectado. También puede usar estos host para lanzar ataques contra otras redes. Ubicar un atacante puede ser difícil si este tiene muchas fuentes de ataque. Además esto puede representar una responsabilidad de riesgo en la compañía si este ataque desde el host causa daños a otras redes.

1.2.4 METODOLOGÍA DE ATAQUE.

A pesar de las motivaciones existentes o preferencias personales, un atacante tiene varias metodologías de ataques, algunas de las cuales son:

- **Aleatorio (Ad hoc, ramdom)**. Es un ataque no estructurado, el atacante que usa esta metodología es por lo general desorganizado y su ataque comúnmente falla. Con esta metodología es difícil encontrar objetivos en la red.

- **Metódico**. Proporciona una bien definida secuencia de pasos para atacar una red. Primero el atacante usa reconocimiento para ubicar los objetivos. Segundo, el atacante ubica exploits (programas de ataque), para atacar las vulnerabilidades encontradas durante la recolección de información. Muchas veces, un metódico atacante experimenta en sus exploits una práctica, ganando experiencia y efectividad. Finalmente, cuando la red es vulnerada empieza el ataque al objetivo de la red. Esta metodología de ataque proporciona una alta probabilidad de éxito.
- **Golpe quirúrgico (surgical strike)**. Frecuentemente, el atacante usa un script autómata contra una red. El ataque es completado en pocos segundos, antes de que administradores de sistemas o analistas de seguridad tengan tiempo de reaccionar y tomar una decisión. Esta metodología de ataque permite al atacante llevar su tarea efectivamente y así poder moverse rápidamente a nuevos objetivos en la red.
- **Paciente**. Nuestra metodología final es actualmente considerada una sub-metodología que puede ser aplicada en la metodología aleatoria (ad hoc) o a la metódica. Esto se refiere a como el atacante ejecuta rápidamente su ataque. Un atacante usualmente usa la metodología paciente para evitar ser detectado. Muchos IDS (sistemas de detección de intrusos) tienen dificultad en detectar ataques que ocurren sobre largos periodos de tiempo. Por ejemplo si un ping sweep (barrido de pings) es ejecutado por horas será detectado pero si el mismo ping sweep es ejecutado un mes posiblemente no será detectado.

1.2.5 PUNTOS DE ATAQUE EN LA RED.

Los principales puntos de ataques son los siguientes:

- Recursos de la red.
- Protocolo de la red.

1.2.5.1 RECURSOS DE RED.

Sistemas en la red representan un primer objetivo de ataque. Ataques contra estos recursos generalmente recaen en muchas categorías:

- **Manipulación o acceso de datos**. Muchos sistemas en la red tienen directorios compartidos que proporcionan un punto de entrada a un atacante. Una técnica común usada es buscar recursos compartidos que permitan conexiones anónimas (anonymous). Una conexión anónima no requiere autenticación. Además, estos recursos compartidos proporcionan al atacante un fácil acceso a los datos. Algunas veces estos datos proporcionan al atacante información de cómo escalar su ataque, tal como nombre de cuentas, y sobretodo, passwords. Otras veces, el atacante usa recursos compartidos anónimos para cargar un programa denominado "trojan hourse" en el sistema. Cuando usuarios privilegiados ejecutan el programa "trojan hourse" se instalará sigilosamente un back door (punto de acceso vulnerable) para el atacante o también este trojano puede atacar tu sistema.
- **Cuentas de Acceso**. Si un atacante logra tener acceso a una valida cuenta en la red, se incrementa tremendamente la posibilidad de obtener acceso privilegiado y eventualmente comprometer la red. El primer paso es la obtención de un nombre de cuenta valido. Muchas veces la cuenta de correo

de un usuario es la misma cuenta de dicho usuario en el sistema. Por otro lado la obtención de los passwords se puede lograr ejecutando programas basados en diccionario de passwords (password guessing programs). Estos programas repetidamente intentan logearse a la red con una cuenta usando variaciones de palabras de su dirección como password. En muchas redes, estos programas son efectivos encontrando una vulnerabilidad en user y passwords.

- **Acceso privilegiado**. Muchas cuentas no privilegiadas, como la cuenta anonymous, proporciona un acceso extenso a los recursos del sistema. Sin embargo, estas cuentas permiten la ejecución de pocos comandos y acceso restringido a archivos. Al obtener un acceso privilegiado, el atacante puede convertir una simple cuenta de acceso en una cuenta con privilegios ilimitados. Después de comprometer el sistema, el atacante puede instalar back doors (puntos vulnerables) y otros programas ocultos. Eliminar estos programas ocultos puede significar la re-configuración total del sistema operativo.
- **Relaciones confiables**. Las relaciones confiables son establecidas entre privilegiados hosts en la red. Esta confianza es basada normalmente en direcciones IPs o nombres de hosts. Un atacante puede evadir ambos mecanismos. Además, compromete un host en una relación confiable entonces los otros miembros de las relaciones serán pronto vulnerables.

1.2.5.2 PROTOCOLOS DE RED.

En lugar de atacar los recursos de la red, un atacante algunas veces ataca la integridad de los protocolos de red. Los protocolos en la red habilitan los recursos

para poder establecer las comunicaciones entre los hosts. Al manipular los protocolos de red, el atacante espera lograr el acceso a uno de los recursos de la red. Ataques a protocolos de red pueden ser divididos en dos categorías:

- **Intercepción.** Esto se refiere a cuando un atacante toma participación de la sesión establecida entre dos host que se comunican a través de algún protocolo. En esta situación el atacante puede simplemente escuchar la conversación o interferir alterando los datos transferidos. En este ataque el atacante necesariamente deberá estar instalado en la misma red a la que se conectan los hosts a ser atacados.

  El atacante puede tomar control de la existente conexión TCP entre dos host, después de tomar control de la sesión TCP, el atacante puede insertar datos y comandos como validas cuentas para iniciar la conexión. El protocolo TCP proporciona mínima verificación de integridad y no brinda confidencialidad.
- **Enmascaramiento**. Este ataque se caracteriza por enviar paquetes variando el IP fuente. Los protocolos basados en UDP son especialmente vulnerables a este tipo de ataques, como lo es el ARP. Por el contrario los protocolos basados en TCP usan secuencia de números para la autenticación. En el caso de UDP, este solo usa el IP fuente para la autenticación. En la actualidad existen numerosos programas para realizar estos ataques modificando el IP fuente, lo cual hace pensar que el ataque proviene de distintas partes.

1.3 ORGANIZACIÓN, ADMINISTRACIÓN Y CONTROL DE TIC.

En esta parte se presentará una estructura básica de un centro informático, las unidades que lo componen y el rol básico de ellas. Así mismo, los principales problemas que enfrentan las organizaciones en la administración de TIC.

1.3.1 ESTRUCTURA BÁSICA Y RESPONSABILIDADES DE UNA ÁREA INFORMÁTICA.

1 Los roles y responsabilidades para las operaciones de TIC.

Los roles y funciones de las operaciones TIC incluyen lo siguiente:

- **Planificación de la capacidad**. Por ejemplo, para asegurar que los sistemas computacionales continúen entregando un satisfactorio nivel de funcionamiento en el futuro. Esto involucrará que el personal de operaciones TIC calcule los futuros requisitos de las PCs, la capacidad de almacenamiento en disco y la capacidad de carga en la red.
- **Supervisión del cumplimiento**. Monitoreo del funcionamiento diario del sistema en términos de medidas, tales como el tiempo de respuesta.
- **Carga inicial de programa**. Inicializar un sistema o la instalación de un nuevo software.
- **Manejo de medios**. Incluye el control de los discos, cintas y cd-rom.
- **Cronograma de trabajo**. Un trabajo consiste normalmente en un proceso o una secuencia de procesos por lotes (batch), que se llevan a cabo durante la noche, o bien, corresponde a un procedimiento de

respaldo a través del cual se actualizan los archivos etc. Los trabajos normalmente se realizan en periodos de días, semanas, meses o años.

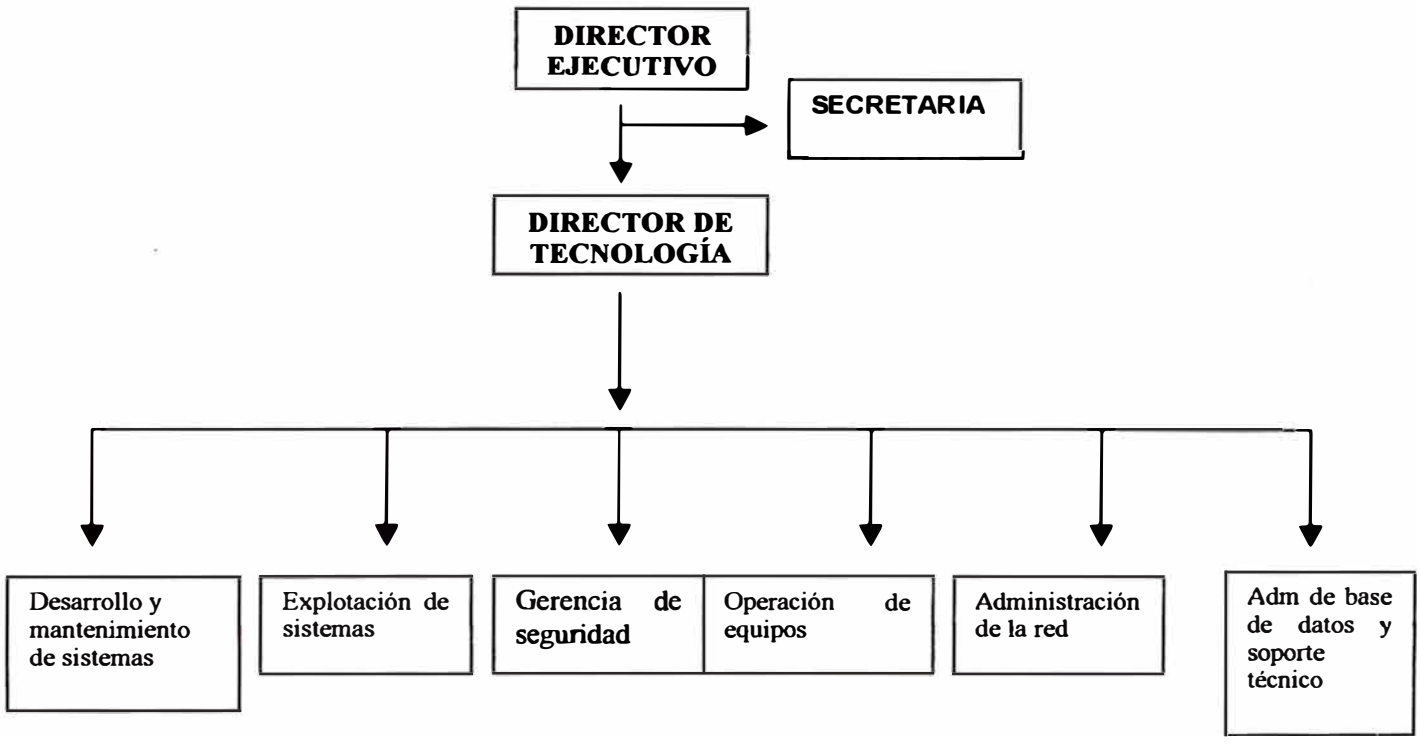
- **Respaldos y recuperación de desastres**. Los respaldos de los datos y software deben ser llevados a cabo regularmente por personal de operaciones TIC.
- **Ayuda al escritorio y administración de problemas**. Los servicios de ayuda al escritorio constituyen el vínculo cotidiano entre los usuarios con problemas en tecnología informática y el departamento de TIC. Existen usuarios que llaman cuando tienen problemas con la impresora o se olvidan de su contraseña. Los problemas se pueden resolver con programas individuales (aplicaciones y sistema), hardware, o telecomunicaciones.
- **Mantenimiento**. Esta relacionado con el hardware y software.
- **Monitoreo y administración de la red**. La mayoría de los computadores usados en negocios, incluyendo los que se utilizan en el gobierno, están conectados a redes. A la función operacional de TIC se le otorga la responsabilidad de asegurar que se mantengan los enlaces de comunicación y de proveer a los usuarios el nivel aprobado de acceso a la red.
- **Operaciones computacionales**. Este término está referido a los aspectos logísticos y de infraestructura del hardware y software. Operaciones computacionales apropiadas previenen al usuario de la necesidad de preocuparse de estos asuntos, asegurando que las aplicaciones de sistema estén a disposición en un horario determinado,

que funcionen como se espera, que los resultados de su proceso, tal como la impresión, sean producidos a tiempo. En un departamento de TIC bien administrado se espera encontrar operaciones computacionales que sean claras para los usuarios y que los apoyen cabalmente en el funcionamiento de sus roles.

2 Tipo de estructura de la administración de TIC.

Dentro de un típico departamento de TIC el director (o junta directiva, ejecutivo de administración, junta de directivos superiores) debería ubicarse en la parte superior del diagrama, enfatizando la importancia de TIC en la organización.

Organigrama de un centro de informática



A continuación se detalla cada modulo para describir sus roles dentro de la gerencia TIC:

- **Desarrollo y mantenimiento de sistemas**. Es la unidad que tiene como rol el desarrollo y mantenimiento de todos los sistemas de la organización. Su personal está compuesto por ingenieros de sistemas, analistas de sistemas, programadores, etc. En muchas organizaciones el mantenimiento se constituye en una unidad separada cuyos profesionales son especialistas en este tipo de actividad que no siempre es reconocida como importante.

- **Explotación de sistemas**. Tiene a su cargo la explotación de los sistemas, es decir, hacer que los sistemas estén operando, disponibles y entregando a los usuarios lo que deben entregar.

  Se encargan de ejecutar todas las rutinas necesarias para que se obtenga el producto de sistema y también las rutinas de seguridad y respaldo.

- **Gerencia de seguridad**. Es responsable por el planeamiento y ejecución de la política de seguridad de las informaciones de la institución. Aunque parece indispensable a una organización, muchas veces no existe la estructura ni la política de seguridad instituida.

- **Operación de equipos**. La operación de equipos es una de las más importantes actividades en un centro informático porque tiene su rol en toda la operación y mantenimiento de computadores y otros equipos necesarios. Además de los computadores y equipos de redes, es necesario que opere los

equipos de suministro de energía eléctrica, de aire acondicionado, de prevención y detección de incendios, de seguridad, etc. Fallas en el funcionamiento de estos equipos pueden comprometer toda la organización.

- **Administración de la red**. Tiene a su cargo la administración de todos los componentes físicos y el software de la red de computadores. Estos componentes físicos son los servidores de red, ruteadores, cableado, switches, etc. Los softwares son los sistemas operativos de red, programas de control de la red, programas de gerenciamiento y de control, tales como firewall y sistemas detectores de intrusos.

- **Administración de base de datos y soporte técnico**. La administración de las bases de datos es responsable por la administración de los datos y por mantener disponible las bases de datos a los sistemas y dar soporte técnico en software a los analistas y programadores de sistemas. Son dos cosas diferentes pero interconectadas. Sin embargo, en algunas organizaciones, la administración de datos está separada de la administración de la bases de datos. El soporte técnico es la actividad de ayuda a las demás para que utilicen correctamente los softwares. En estas unidades se ubican los especialistas en softwares de administración de base de datos, especialistas en sistemas operativos, y especialistas en lenguajes de programación, etc.

1.3.2 PROBLEMAS DE LAS ORGANIZACIONES EN LA ADMINISTRACIÓN DE TIC.

- **Insuficiencia de recursos informáticos.**

  Uno de los problemas más observados en las organizaciones es la insuficiencia de los recursos informáticos. Esa insuficiencia puede ser de cantidad o calidad de los equipos o de ambos.

  Hoy en día, la desactualización de los equipos de computo ocurre en dos o tres años. Existen organizaciones que no tienen un programa de actualización de los equipos de computo, el riesgo para estas organizaciones aumenta porque no van a poder utilizar nuevas versiones de softwares y otros recursos.

  También pocas organizaciones poseen recursos suficientes para comprar y mantener con la cantidad y cantidad de computadores necesarios.

- **Escasez de personal.**

  La escasez de personal técnico suficiente es un problema que se observa en la mayoría de los centros informáticos. Esto porque las necesidades de informatización son siempre más grande que la capacidad de los órganos de informática tienen que atender.

  Hoy en día se utiliza de la contratación de prestadores de servicios para suplir estas necesidades.

- **No actualización profesional**.

  La capacitación y el desarrollo del personal están estrechamente ligados a la planificación de los recursos. La administración de TIC debería saber qué técnicas tendría que conocer el personal, tanto en el presente como en el futuro. Se debería capacitar al personal para que logren tales requisitos. La necesidad de capacitación, tanto para el desarrollo de hardware y de software, es continua. Frecuentemente la capacitación en TIC es costosa y debería estar controlada por el presupuesto y los programas de capacitación.

  Para reducir la dependencia respecto de unos pocos empleados claves, el cliente puede utilizar una forma de capacitación cruzada, es decir, los miembros entrenados del personal realizan los trabajos de otros de sus colegas, en caso de que estos falten. Lo anterior, también provee una forma de planificación sucesiva. El cliente debería estar enterado que cuando el personal capacitado sustituye a otro miembro del personal, esto aumenta el riesgo de que ese personal tenga un conocimiento más detallado de todo el sistema, lo que incluye el conocer la existencia de cualquier control de compensación.

- **No utilización de estándares de calidad de desarrollo de sistemas (CMM, Common Criteria ISO 15.408, etc)**.

  La calidad de los sistemas o la baja calidad es uno problema presente en la mayoría de las organizaciones. Esta baja calidad lleva a aumentos de costos en mantenimiento de los sistemas. Para disminuir esa baja calidad se han creado algunos estándares de calidad de los softwares. Dos de esos son el

CMM de SEI (Software Engenering Institut) y el common criteria de la ISO (ISO/IEC 15.408).

1.3.3 MODELO DE MADUREZ DE CAPACIDAD (CMM).

La creciente necesidad, sumada a décadas de promesas incumplidas en cuanto a calidad, costos y cumplimiento en el desarrollo de software, condujo al instituto de Ingeniería de Software de los Estados Unidos a desarrollar el modelo CMM (Capability Maturity Model - Modelo de Madurez de Capacidad).

En principio creado para evaluar y mejorar la capacidad de los contratistas de software del departamento de defensa de los Estados Unidos, el modelo CMM se convirtió a través de los años en el más alto estándar de ingeniería en el mundo para todo tipo de compañías. Está fundamentado en prácticas reales de las compañías más avanzadas del planeta y refleja el estado del arte en procesos de desarrollo de software.

El CMM está compuesto de 316 prácticas claves agrupadas en 18 áreas y distribuidas en una jerarquía de cinco niveles, a través de los cuales una organización progresivamente alcanza mayor calidad, productividad y menores costos en el desarrollo de software. Los niveles progresan desde el 1, que representa el estado caótico, hasta el nivel 5, que representa el estado de optimización continua. Una organización en nivel 1, en el cual se encuentran la mayoría de los grupos de desarrollo en el mundo, produce software utilizando una aproximación de tanteo y error. Una organización en nivel 5 utiliza las mejores prácticas de ingeniería disponibles en el planeta, hace uso de procesos controlados, medibles y en continuo mejoramiento. Es altamente madura y sistemáticamente está en capacidad de

producir software de alta calidad. Según estadísticas del SEI, el tiempo promedio para avanzar entre los niveles de madurez es el siguiente:

- De nivel 1 a nivel 2, 23 meses.
- De nivel 2 a nivel 3, 22 meses.
- De nivel 3 a nivel 4, 28 meses.
- De nivel 4 a nivel 5, 17 meses.

Las diferencias básicas entre los niveles de madurez, según el SEI son las siguientes:

- **Nivel 1**. Inicial. En este nivel, los procesos y métodos de ingeniería no se encuentran definidos. Por esa razón, los proyectos son adelantados de manera incoherente, incontrolada y poco profesional. El éxito es eventual y depende del comportamiento heroico de algunos individuos, cuando estos poseen algún nivel de conocimiento. La mayoría de los grupos de desarrollo de software en el mundo operan a este nivel.
- **Nivel 2**. Repetible. Se establecen algunos procesos y métodos de ingeniería a nivel de proyectos, aún incipientes.
- **Nivel 3**. Definido. Los procesos, actividades y métodos relacionados con la ingeniería y administración de proyectos se encuentran documentados, estandarizados y construidos alrededor de un marco integrado para toda la compañía. Todos los integrantes de la organización los utilizan en su trabajo diario.
- **Nivel 4**. Administrado. La compañía opera bajo control estadístico de procesos, tanto en procesos como en productos. Los resultados de los procesos y la calidad de los productos son predecibles, y se controlan

siguiendo las técnicas inicialmente publicadas por Deming, Crosby y Juran, técnicas que se han convertido en una herramienta fundamental para las compañías de alta capacidad en el mundo.

- **Nivel 5**. Optimización. En este nivel, las organizaciones se encuentran en un proceso de mejoramiento continuo. Todos los procesos y técnicas modernas están en pie, lo mismo que la administración cuantitativa. Las organizaciones se enfocan en el mejoramiento a través de técnicas y procesos de prevención de defectos, cambios en tecnología y cambios en procesos. Menos del 0.1% de las organizaciones en el mundo se encuentran en este nivel de madurez.

1.3.4 EL COMMON CRITERIA DE LA ISO (ISO/IEC 15.408).

Common criteria es un estándar aceptado internacionalmente que proporciona el referente principal para la evaluación de la seguridad de productos y sistemas de TIC, en dos vertientes diferentes:

- Una estructura común para la definición de funciones de seguridad que incorpora o pretende incorporar un producto, sobre la base de unas hipótesis de uso y un nivel de riesgo establecido y definido previamente, llamada declaración de seguridad.
- Unos criterios de evaluación independiente homogéneos y reconocidos a nivel internacional, que garantizan que el producto o sistema reúna los requisitos establecidos en la declaración de seguridad.

El Common criteria forma parte de la International Standards Organization (ISO), un proceso de evaluación reconocido y desarrollado en colaboración con varias

industrias y agencias gubernamentales como la National Security Agency (NSA) en los Estados Unidos y otras agencias en el mundo.

El Common criteria esta dividido en tres documentos, el primero es una introducción, definiciones, conceptos y explica el modelo de evaluación, en la segunda parte se describen los requerimientos de seguridad, y finalmente el tercero define los criterios de evaluación así como los niveles predefinidos en el common criteria que son los Evaluation Assurance Levels (EALs).

1.3.5 DEFICIENCIA EN LA SEGURIDAD DE LOS SISTEMAS.

La seguridad de los sistemas es una preocupación mundial y con eso se gasta gran parte de los recursos financieros y técnicos de las organizaciones. Deficiencias en la seguridad tienen varias causas:

- **Falta de política de seguridad de informaciones**. La falta de esta política lleva a la construcción de sistema que no tienen como uno de sus fundamentos, la seguridad de las informaciones.
- **Mal uso de los recursos de seguridad disponibles**. Muchas veces las organizaciones poseen firewalls u otros dispositivos de seguridad y los utilizan mal. Los administradores de bancos de datos ofrecen dispositivos, pero sus usos son subutilizados.
- **Mal diseño y construcción de los sistemas**. La seguridad del sistema involucra cuestiones desde el diseño hasta la construcción. Si no se preocupa con la seguridad en el diseño difícilmente se va a obtener un sistema seguro.

1.3.6 DEFICIENCIAS EN LA CULTURA ORGANIZACIONAL RELATIVO A SEGURIDAD DE LA INFORMACIÓN.

La deficiencia o falta de cultura organizacional en seguridad de la información lleva a que ésta exponga sus procesos y sistemas a todos los tipos de amenazas a la seguridad de las informaciones.

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.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.

Las cuatro 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. Ejemplos de este ataque son

pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- **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. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación**. Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes adulterados en una red o añadir registros a un archivo.

Estos ataques se pueden clasificar de forma útil en términos de ataques pasivos y ataques activos.

- **Ataques pasivos.**

  En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

a) Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
b) Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
c) Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos de seguridad.

- **Ataques activos**.

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, que puede subdividirse en cuatro categorías:

a) **Suplantación de identidad**. El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

b) **Reactuación**. Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

c) **Modificación de mensajes**. Una porción del mensaje legítimo es alterado, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de euros en la cuenta A" podría ser modificado para decir "Ingresa un millón de euros en la cuenta B".

d) **Degradación fraudulenta del servicio**. Impide o inhibe el uso normal de la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

1.4 NECESIDAD DE UN CONTROL Y PLANEAMIENTO EFICIENTE DE TIC.

Las organizaciones gastan dinero anualmente en el equipo de TIC y los servicios que son vitales para lograr sus objetivos de misión, y que cumplen un rol progresivamente importante en el mejoramiento del desempeño organizacional y el hacer posible un gobierno capacitado electrónicamente. Para las actividades gubernamentales en particular, la habilidad para dar servicios electrónicamente

requiere gerencia y planificación efectiva de sus recursos de TIC y la infraestructura para asegurar que esos servicios sean dados en la manera más eficiente, fidedigna, y segura posible. El énfasis incrementado en la transferencia electrónica, el cambio de información y el servicio de entrega electrónico por organizaciones da un valor adicional en la capacidad de una organización para administrar eficazmente sus recursos TIC. La auditoría de prácticas de control y planeamiento de varias organizaciones ha dado a conocer varios errores en común. Estos incluyen los siguientes:

- La falla en la comprensión de las fortalezas y debilidades de tecnología nueva.
- La falta de alineación mensurable entre las metas organizativas y los objetivos de proyecto.
- Los proyectos son demasiados especializados o ambiciosos para manejarlos exitosamente.
- Las expectativas poco realistas.
- La falta de soporte organizativo y de aceptación.
- La capacidad limitada de diseñar y operar sistemas integrados de TIC.
- La aversión al riesgo extremo.

1.4.1 EL PLANEAMIENTO Y CONTROL DE LOS RECURSOS DE TIC.

Si el auditor tiene intención de conducir una auditoría de funcionamiento del control y planeamiento de TIC de una organización, entonces es muy útil para él, estar informado acerca de los avances y prácticas claves y enfoques para el control y

planeamiento de TIC. Este conocimiento le provee a él un armazón frente ante el cual pueda evaluar; si las organizaciones auditadas realmente siguieron un enfoque estructurado y si hicieron, si fue el adecuado. La información en esta parte se plantea bajo cuatro categorías coherentes con las prácticas manejo de la información generalmente aceptados y los controles contenidos en la auditoría de sistemas de información y el modelo de control de la fundación COBIT. El modelo COBIT delinea una serie de controles y prácticas de manejo de TIC y los controles organizados en los cuatro dominios: el planeamiento y la organización; la adquisición e implementación; la entrega y el soporte; y el monitoreo.

1.4.2 LA PLANIFICACIÓN Y ORGANIZACIÓN.

Una organización debería planear estratégicamente sus actividades de administración y adquisición del TIC para sostener eficazmente las metas de su misión y sus objetivos. Para hacerlo eficientemente, las actividades del control de comunicaciones planificadas, deben estar organizadas e integradas con un planeamiento organizativo, un presupuesto, administración financiera y administración de recursos humanos.

Existen varias prácticas claves para continuar las actividades de control, organización y planeamiento de TIC comenzando con la comprensión del valor estratégico de los servicios de TIC para la organización, así como un claro entendimiento de qué servicios se necesitan para conocer las necesidades de la organización en el futuro. Para asegurar que estas prácticas estén apropiadamente administradas, el personal debe estar identificado y respaldado y las políticas y procedimientos necesitan estar

establecidos para orientar estas prácticas. Finalmente, el auditor debería estar consciente que es su responsabilidad administrativa asegurar que los riesgos, calidad y servicio de TIC sean identificados y manejados, que las inversiones en el servicio de TIC sean justificadas apropiadamente y las medidas del funcionamiento sean establecidas para asegurar que los resultados planificados hayan sido ejecutados.

1.4.3 DETERMINACIÓN DEL CONTEXTO PARA EL PLANEAMIENTO ESTRATÉGICO DE TIC.

El planeamiento estratégico establece la dirección para la organización por medio de la creación de una visión, y la fijación de metas y objetivos de alto nivel para realizar aquella visión. Los conductores y dirección completa de la organización proporcionan el contexto para el planeamiento efectivo de TIC por medio de la identificación de las metas, objetivos y prioridades del núcleo de los negocios; los factores de éxito decisivos; las ideas de tecnología informática y negocios; y las relaciones externas que incluyen negocios y proveedores de tecnología informática. Con este contexto en su lugar, las metas y objetivos de la red pueden estar definidos y ayudar a conocer las metas del negocio en su conjunto. La valoración del impacto en las operaciones de negocios como resultado de errores de red puede ayudar a determinar qué servicios de telecomunicaciones son los más críticos para la organización.

1.4.4 ADQUISICIÓN E IMPLEMENTACIÓN.

Una buena adquisición de servicios y procesos de implementación deberá de establecerse para adquirir e implementar sistemas y servicios de TIC. El proceso comienza con el planeamiento para asegurarse que las capacidades adquiridas e implementadas reflejen los objetivos organizacionales que están en marcha. Una vez que el planeamiento se encuentre completo y las capacidades sean identificadas y una adecuada estrategia sea acordada, entonces se conducirá una competencia justa y abierta basada en las expectativas de servicios mensurables. El proyecto de adquisición e implementación deberá de ser manejado de acuerdo con los principios de manejo de proyectos generalmente aceptados. Finalmente, las capacidades instaladas e implementadas deberán de ser verificadas, validadas y probadas para asegurar que las necesidades de la misión y las expectativas sean satisfechas.

El planeamiento deberá de preceder a la actividad de adquisición para asegurarse que las capacidades implementadas reflejen las necesidades organizacionales y sus objetivos. Un claro entendimiento de los objetivos organizacionales deberá fluir del proceso de planeamiento estratégico previamente descrito. Asimismo, lo anteriormente descrito es la línea de base de los servicios existentes para que puedan proveer un punto de partida para desarrollar todos los elementos de la arquitectura de redes, patrones de tráfico de servicios, tendencias y sus costos relacionados. Construidos desde esta línea de base, los planificadores pueden enfocarse en identificar las tecnologías de red que necesiten, los planes existentes y futuros que estos servicios deban de comprender y las capacidades y represiones que se encuentren en las instalaciones y los proveedores de servicios que se encuentren en

el lugar. Con esta información, los planificadores pueden hacer juicios basados en un claro entendimiento de las capacidades actuales y planificadas de TIC, los requerimientos y las tecnologías, las necesidades emergentes o actualizar los conocimientos que deban de ser considerados, variaciones que existan en las instalaciones locales y servicios, y el costo actual de estos servicios.

El planeamiento deberá de resultar en la selección de una estrategia de contratación apropiada para la adquisición de las capacidades necesarias. Las cuestiones a considerar incluyen el determinar como obtener la mejor "mezcla" de los recursos de TIC para los servicios de entrega; esto implica la realización de un "outsourcing" total o parcial en la entrega de servicios o la utilización de recursos locales. También considerar que necesidades tendrán que ser hechas y como organizar el trabajo para ganar las mejores ventajas operativas antes de considerar el tipo de contrato a utilizar. Las opciones disponibles deberán de ser utilizadas y valoradas, con los criterios de evaluación y selección que reflejan las necesidades organizacionales y prioridades establecidas y consistentemente aplicadas con las alternativas disponibles. Se establecerá una consideración adicional si se centralizara el procuramiento de estos servicios para asegurar las economías de escala y para mejorar la calidad del servicio. Las oportunidades para realizar ahorros potenciales a través de la consideración de varias operaciones o funciones de adquisición deberán de ser consideradas en este tiempo, como el uso de soluciones compartidas para los servicios de TIC pudieran impedir la duplicación del esfuerzo.

Es importante para la organización que se adquiera eficientemente y efectivamente la solución correcta al precio justo y en el tiempo justo. Esto puede ser completado por

la unión de un proceso de adquisición competitivo que pueda adquirir servicios y las soluciones que cumplan con las necesidades claramente definidas de la organización y su compatibilidad con las políticas y procedimientos de la organización. Se considerará lo siguiente cuando se implemente el proceso de adquisición:

- Las adquisiciones deben de ser justas y abiertas, y ser consistentes con las metas de la organización y planes técnicos específicos.
- Las adquisiciones deben estar enfocadas en reunir y satisfacer los objetivos claramente definidos y documentados, el alcance y los requerimientos que reflejan las necesidades organizacionales.
- Las adquisiciones deberán de tener el compromiso y el apoyo de manejo administrativo a través de un administrador quien será el responsable para el éxito del proyecto.
- El planeamiento de las adquisiciones y los equipos de adquisición deberán de incluir la participación de toda la organización, incluyendo los usuarios, auditores, consultores, y otras partes interesadas, cada una con un tipo de responsabilidad definida con respecto a la adquisición.

1.4.5 MANEJO, OPERACIONES Y SOPORTE.

Un manejo de la organización deberá asegurar que las operaciones importantes y funciones de apoyo sean realizados regularmente en una manera ordenada. Por lo tanto, el manejo deberá establecer y seguir la rutina para sus operaciones y actividades de apoyo. Específicamente, un concepto de operaciones deberá de estar en lugar para organizar efectiva y eficientemente actividades que permitan la seguridad y la continuidad de los servicios de TIC, para resolver rápidamente los

problemas que surjan en la entrega de estos servicios y que aseguren que el personal de apoyo y recursos sean apropiadamente manejados.

La organización deberá de desarrollar una serie de operaciones detalladas que logren interactuar las relaciones entre los usuarios, las redes, sistemas y sus servicios y el ambiente organizacional que asegure que los servicios brindados satisfagan las necesidades organizacionales y las necesidades de manejo administrativo. Los procesos de operaciones de TIC y los procedimientos requeridos para satisfacer las operaciones y los requerimientos de apoyo deberán de estar establecidos y documentados. Los manuales de operación deberán contener:

- Políticas de organización.
- Operaciones de TIC, mantenimiento y soporte de procedimientos y controles.
- Procedimientos para enfrentar las contingencias y las situaciones como las fallas e interrupciones de operación o degradación del rendimiento de TIC.
- Manejo de la configuración y control.
- Procedimientos del usuario y controles.
- Entrenamiento.

Con estos procesos y procedimientos en curso, la organización deberá de establecer un responsable de las operaciones técnicas para monitorear el rendimiento de las redes y los cambios directos y procedimientos de restauración de los servicios. El rendimiento puede ser monitoreado y manejado efectivamente por medio del análisis continuo y la evaluación de los parámetros de servicio, la medición de los parámetros de servicio incluirá:

- La provisión del servicio a tiempo y con éxito.

- Calidad del servicio y disponibilidad al usuario final.
- Prevención de problemas de frecuencia, tendencias.
- Utilización de recursos.

Es importante comunicar las cuestiones de TIC, consideraciones, cambios, supervisión de operaciones programadas, y planes que puedan surgir a través de las operaciones del día a día, para un personal apropiado para minimizar la confusión y realizar la confianza. Por lo tanto deberá de establecerse una función de apoyo al consumidor para asistir y aconsejar a los usuarios de los eventos de servicio efectivo, como el mantenimiento programado, y para asegurar la solución de problemas de una forma pronta y responsable experimentada por parte del usuario. Estas actividades de apoyo, deberán de ser planeadas y monitoreadas, priorizar las tareas y recursos programados para entregar los servicios eficientemente para la organización y asegurar que los períodos pico sean tratados con poca a pequeña interrupción.

1.4.6 MANEJO DE RECURSOS HUMANOS Y REDES DE OPERACIÓN PARA MAXIMIZAR LOS BENEFICIOS DE TIC.

Deberán de manejarse tanto los valores humanos, redes y de capital consistentemente con las políticas organizacionales, y ambos objetivos tanto estratégicos como operacionales par asegurar una entrega eficiente de los servicios de TIC que alcancen las necesidades organizacionales. El capital humano puede ser manejado apropiadamente usando técnicas de manejo de personal adecuado como:

- El desarrollo de planes y estrategias específicas para contratar, entrenar y desarrollar profesionalmente al personal de telecomunicaciones.
- Asignar personal claramente definido y roles organizacionales responsabilidades además de definir los reportes asociados.
- El manejo de las actividades del personal de acuerdo con la política organizacional y procedimientos de manejo documentado de telecomunicaciones.

Además de los recursos humanos, los gastos de TIC deberán de ser manejados en una manera que identifica y atribuye los costos a los usuarios de servicios para asegurar su compromiso con los costos relacionados a este servicio. Esto deberá de ser cumplido por:

- El desarrollo de un sistema contable completo y preciso de los gastos además de los resultados relacionados.
- El monitoreo de los costos para asegurar que las tendencias son identificadas en el momento en que ocurren y las áreas de problema potencial que son manejados proactivamente.
- La revisión de las cuentas de TIC para los proveedores de servicio para su exactitud, particularmente en el eventual caso de cambio de frecuencia en los tipos de acceso o servicio.

1.4.7 MONITOREO.

El monitoreo de los procesos es asegurar el logro de los objetivos para los procesos de TIC. Se hace posible a través de la definición por parte de la gerencia de reportes

e indicadores de desempeño gerenciales, la implementación de sistemas de soporte así como la atención regular a los reportes emitidos y toma en consideración:

- Indicadores clave de desempeño.
- Factores críticos de éxito.
- Evaluación de la satisfacción de clientes.
- Reportes gerenciales.

El objetivo del monitoreo es:

- Recolectar datos de monitoreo.
- Evaluar el desempeño.
- Evaluar la satisfacción del cliente.
- Generar reportes administrativos.

CAPÍTULO II

2 ADMINISTRACIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC).

En el mundo cambiante en el cual las organizaciones deben enfrentar el reto de lograr un equilibrio entre sus objetivos institucionales y los riesgos que en sus procesos supone el uso de la tecnología, se requiere una administración completa de los riesgos en la seguridad en todos los ámbitos con un enfoque coordinado y estratégico.

Cuando se aprovechan de las vulnerabilidades, el impacto puede ser significativo; desde el simple costo de la substitución del bien hasta pérdidas masivas. Cuando los problemas de seguridad afectan a los clientes, los impactos pueden ser críticos.

Una evaluación y administración de riesgos efectiva, cubriendo todos los ámbitos del negocio traerá retornos significativos; minimizando las oportunidades de pérdidas, optimizando las soluciones y evitando duplicación de esfuerzos.

2.1 MODELAMIENTO Y ANÁLISIS DE RIESGOS.

2.1.1 MODELAMIENTO DE RIESGOS DE TIC.

Consiste en identificar las diversas formas en que los datos y los sistemas de información, así como las redes que los apoyan, están expuestos a riesgo. Este proceso involucra la evaluación de cada amplio rango de amenazas que podría atacar un sistema y el impacto que un ataque exitoso tendría en la empresa. El resultado final es una evaluación individual (a veces definido como "requerimiento de seguridad ") para cada tipo de amenaza que podría afectar al sistema en cuestión.

Los requerimientos de seguridad se usan para entregar una base para el proceso que sigue, que es la "administración de riesgos".

Riesgo es una combinación de amenaza, vulnerabilidad e impacto. Si no hay amenaza, entonces no hay riesgo.

Con frecuencia se usa el término riesgo para representar tanto la amenaza, o la probabilidad de que una amenaza ocurra. Aunque la amenaza y la probabilidad son componentes importantes del riesgo, no son los únicos factores que se van a aplicar.

A continuación se describen algunas definiciones relacionadas con amenazas de riesgo a un sistema:

- **Propiedades de TIC**. Son una parte componente de un sistema de computación. Existen cinco tipos de propiedades de TIC: datos, sistemas de aplicaciones, tecnologías, instalaciones y personal.
- **Amenaza**. Un incidente involuntario (por ejemplo: fuego, daño premeditado, robo) que pueda eliminar, inutilizar, dañar o destruir una propiedad de TIC.
- **Vulnerabilidad**. Un punto débil que puede ser explotado por una amenaza.
- **Impacto**. Las consecuencias de la existencia de un punto débil en un sistema y que fue explotado por una amenaza.
- **Probabilidad**. En este contexto, la probabilidad de que una amenaza ataque con éxito un sistema computacional.
- **Riesgo**. Una medida de la exposición a la cual un sistema computacional esta sujeto. Es una función de la probabilidad de que un ataque a un sistema tenga éxito y del impacto que resultaría.

De este modo, en el contexto de seguridad de TIC, riesgo compromete tres componentes; amenazas, junto con sus asociados, vulnerabilidades e impactos.

Las medidas de riesgo se clasifican según el tipo de riesgo con el que están relacionadas; por ejemplo, se debe aplicar evaluaciones separadas a los riesgos de siniestro, robo y error en el diseño del programa, ya que cada una de estas amenazas es diferente en su naturaleza. Algunos enfoques de las evaluaciones de riesgo los expresan simplemente como "alto", "medio" o "bajo"; a su vez, se usan enfoques más sofisticados, ya sea para escalas de evaluación más amplias o para el uso de un enfoque gráfico que permite comparar los resultados de la revisión del análisis de riesgo con las normas de la industria apropiada.

2.1.2 EL COSTO EFECTIVO DE LA SEGURIDAD.

La seguridad no es gratis. De hecho puede ser muy cara en términos de los costos de adquisición, así como por los costos asociados con la instalación, el testeo, la operación y el mantenimiento.

De allí que el profesional de la seguridad de TIC debe ser capaz de demostrar que los costos involucrados en la implementación de medidas de prevención son completamente justificados, en términos de los valores de las propiedades de TIC que estén en riesgo, la escala de los riesgos que enfrentan y las consecuencias que tendrían para las empresas el que ellas se vieran comprometidas, interrumpidas o dañadas de cualquier modo.

Por lo tanto, el análisis de riesgo identifica los tipos de riesgos de TIC que se necesita controlar junto a las razones que las justifican. Asimismo, indica el nivel de inversiones que se justifican para entregar un nivel adecuado de protección a través

de la aplicación de medidas preventivas apropiadas. Una adecuada conducción del análisis de riesgo y los controles de riesgo de TIC (durante los cuales se escogen las medidas preventivas) son la base de una adecuada relación costo y efectividad de la Seguridad de TIC.

2.1.3 COMPROMISO DEL USUARIO.

El problema más grande para muchos gerentes de seguridad es que su personal esté completamente consciente de la necesidad e importancia de mantener una seguridad de TIC efectiva dentro de la empresa. Si no existe una buena cultura de seguridad dentro del lugar de trabajo, la efectividad de muchas inversiones de la organización en las medidas sistemáticas de prevención se verá disminuida.

El conocimiento de los usuarios de los problemas de seguridad se puede aumentar por medio de la participación en la revisión de seguridad. Además, el equipo de revisión debe trabajar con la comunidad del usuario para identificar la necesidad del costo efectivo de las medidas preventivas debido a que:

a) Ellos conocen mejor qué medidas preventivas son aceptables en el entorno de trabajo.
b) Es más probable que apoyen las medidas preventivas seleccionadas si ayudan a escogerlas.
c) El esquema más efectivo para asegurarse respecto a que existan sólo las medidas preventivas con un costo justificado es solicitar a la gerencia del usuario que pague por la seguridad que necesita. Es muy probable que los usuarios se resistan a pagar por las medidas preventivas si no han participado en su selección.

2.1.4 PRINCIPIOS DEL ANÁLISIS DE RIESGO.

El análisis de riesgo involucra:

a) Modelamiento empresarial; para determinar qué sistema de información soporta y cual son las funciones del negocio.

b) Análisis del impacto; para determinar la sensibilidad de las funciones claves de la empresa respecto a una violación de la confidencialidad, integridad o disponibilidad.

c) Análisis de dependencia; para determinar los puntos de acceso a los sistemas de información y las propiedades que deben existir para entregar un servicio a una función empresarial.

d) Análisis de la vulnerabilidad y de las amenazas; para determinar los puntos débiles en la configuración y la probabilidad de que los eventos exploten la debilidad identificada causando impacto en términos de violación de la confiabilidad, integridad o disponibilidad.

2.1.5 ANÁLISIS DE RIESGO DE TIC.

En general, el análisis de riesgo de TIC implica la identificación de cuáles son las propiedades que están en peligro y luego formular las siguientes preguntas:

- ¿Qué tipo de amenazas enfrentan?.
- ¿Cuáles son las posibles causas e impactos?.
- ¿Cuál es la posibilidad que la amenaza tenga éxito?.
- ¿Cómo saber si la amenaza logró su objetivo?.
- ¿Qué hacer para prevenir el impacto?.
- ¿Cómo recuperarse si una amenaza se materializa?.

- ¿Producirán otros riesgos los cursos de acción alternativos que se tomen?. De ser así, ¿serán muy severos?.

Se necesitan varias etapas para responder a estas preguntas, y el proceso completo es bastante lento. Se necesita recopilar mucha información, asimilarla y posteriormente, se efectuaran estimaciones, dictámenes y transacciones.

2.1.5.1 EL LÍMITE DE LA REVISIÓN.

Es esencial acordar el límite de una inspección de análisis de riesgo de TIC con la administración desde el comienzo. Esto implicará, la clara definición de todo el objetivo de la revisión y además, se acordará cuáles son los activos de TIC incluidos y cuáles no lo están. El propósito es:

a) Entender claramente lo que la inspección trata de realizar.
b) Proporcionar una estructura para la planificación del proyecto y la conducción del análisis.
c) Evitar entregar un falso sentido de seguridad al pasar por alto aquellos activos de TIC que son esenciales para el funcionamiento exitoso del sistema.

En algunos sistemas, especialmente en aquellos de tamaño pequeño, puede ser obvio poner un límite lógico para la revisión. Pero, los grandes sistemas inter-conectados presenta problemas mucho más difíciles, especialmente si poseen pocos recursos y un tiempo limitado. En esta situación, es necesario analizar las partes representativas del sistema y reunir información suficiente para crear un rango de modelos sobre los cuales basar la administración del riesgo.

Otro factor complicado a considerar son las áreas inaccesibles dentro del límite de inspección. El ejemplo más común es cuando los vínculos de comunicación de los

datos ingresan al dominio de las autoridades de la telecomunicación. Probablemente será imposible que los inspectores puedan juzgar si dichas autoridades mantendrán o no un nivel de seguridad adecuado dentro de su dominio.

2.1.5.2 METODOLOGÍA PARA REALIZAR EL ANÁLISIS DE RIESGO.

El mejorar un cálculo de probabilidad de un incidente de seguridad que afecte a una organización es más problemático que evaluar las propiedades de TIC. La persona que realice tales cálculos debe tener bastante conocimiento y experiencia de la evaluación de riesgo.

En el mercado, hay varias metodologías de análisis de riesgo, y algunas se han incluido en el software de PC. Ellas acceden a dos categorías generales: cuantitativa y cualitativa.

- **El método cuantitativo**. Tiene como objetivo equilibrar los costos de implementación frente a los posibles costos de defecto para implementarlo, como lo que se expresa por una Expectativa de Perdida Anual (ALE).

  La ALE está basada en el concepto que en cualquier período rotativo de doce meses ocurrirán "n" incidentes originados por cualquier tipo de amenaza ('n' puede ser fraccionario para los incidentes que se han presentado frecuentemente). Si cada incidente da por resultado un promedio de pérdida "i", luego ALE será el producto de ambos, vale decir: "n*i". La inversión en medidas preventivas con un costo anual "$", por ende, se justificará si se espera que den como resultado una reducción de la ALE que es mucho mayor que "$".

El problema del enfoque ALE es que, para que sea efectivo, se necesita una historia completa de los incidentes en la seguridad y de los impactos relacionados con ella. Si esto no existe, los cálculos ALE se deben basar en la experiencia que tienen organismos parecidos que se compara siempre que se pueda disponer de ellos y existe la posibilidad que éstos no sean suficientemente representativos. Este enfoque también requiere que los impactos se midan en términos monetarios, lo que no siempre es práctico.

- **Método cualitativo**. Está basado en los resultados de cuestionario(s) que han sido diseñado(s) para evaluar los posibles niveles de una serie de amenazas y sus respectivas vulnerabilidades.

  En concordancia con cualquier enfoque del cuestionario, la relevancia de algunas preguntas variará de acuerdo a las circunstancias, mientras el cuestionario en sí puede que no sea lo suficientemente completo o apropiado en situaciones poco comunes. Esto significa que el experto deba ajustar las indicaciones estándares del cuestionario y esto puede agregar el riesgo de que se tergiverse el método.

2.2 CONTROL DEL RIESGO DE TIC.

El control de riesgos persigue la identificación, selección e implementación de las medidas preventivas que la entidad ha desarrollado para reducir los niveles identificados de riesgo a niveles aceptables. Es imposible reducir todos los riesgos; incluso, si esto fuera posible, sería demasiado costoso y el resultado sería poco viable. Por lo tanto, el control de riesgo es mucho más un asunto de compromiso

entre lo que es deseable, lo que es factible y lo que es producible. Implica habilidad técnica, buen conocimiento de la empresa y su fuerza laboral, como también, un buen criterio.

2.2.1 CONTRAMEDIDAS.

Una contramedida es una verificación o restricción sobre un sistema que ha sido diseñado para aumentar su seguridad. Las medidas preventivas caen dentro de varios tipos diferentes y actúan de diferentes maneras. Un buen entorno de seguridad tiene una mezcla de contramedidas que se potencian mutuamente para proporcionar una "seguridad exhaustiva". De este modo, si una contramedida falla existe la oportunidad de que otra funcione. Por ejemplo, si un pirata informático logra su objetivo y accede a un sistema, los perfiles de seguridad individual, la codificación de datos y el registro (junto con su revisión) continuarán proporcionando una buena medida de protección y, si su implementación es adecuada, deberían alertar a la administración respecto a un defecto de los controles.

Las medidas preventivas de seguridad computacional se clasifican en las siguientes categorías generales:

- **Físicas**. Están diseñadas para proteger a un sistema contra amenaza físicas. Incluye daños por fuego, agua, caída de rayos; fallas en el mantenimiento de un ambiente de operación adecuado, en términos de temperatura, humedad, limpieza, calidad de suministro de energía; así como de incidentes que derivan del acceso físico, por ejemplo, el robo y el daño doloso al equipo.

- **Técnicas (o lógicas)**. Son aquellas implementadas por el software del computador. Las medidas preventivas técnicas para restringir el uso y acceso al sistema operativo del computador, redes, programas utilitarios (como redactores y compiladores) y programas de aplicación.
- **De procedimiento**. Son aquellas que se ejecutan manualmente. Por ejemplo, puede que sea necesario verificar que todas las personas que quieran ingresar a la sala de computación tengan autorización. Este requerimiento puede ser implementado como procedimiento de contramedidas ubicando a un guardia en la puerta, cuyo trabajo es ejecutar las inspecciones necesarias, así como registrar los nombres, horas, fechas, etc de todos los que ingresen. Se puede destinar un control especial con el objeto de revisar la validez de todas las entradas de datos del computador, después de que se ha ingresado al sistema y antes de que sea procesada la información, para confirmar que esté completa y que no contenga ítemes no autorizados o invalidados.

Cuando una o más de estas categorías de contramedidas falten, va a existir un riesgo incontrolable. Por supuesto, es el administrador quien decide si esta situación es aceptable; sin embargo, un sistema debe tener algún valor para la organización (de otra manera, ¿por qué tenerlo?) y como resultado, debería tener alguna justificación para protegerlo, por lo menos con las medidas preventivas básicas, que son aceptadas como una práctica positiva.

Dentro de cada categoría general descrita anteriormente, los diferentes tipos de contramedida actuarán de diferente manera. Aunque la seguridad exhaustiva requiera una combinación de tipos de contramedidas, algunas proporcionan mayor

seguridad que otras. La siguiente lista muestra los tipos de contramedidas en orden descendente de efectividad. Hay medidas preventivas que actúan para:

- **Reducir la amenaza**. En un sistema, el control efectivo de contraseñas junto con los perfiles de seguridad individual reducirán la amenaza de acceso no autorizado a un sistema.
- **Reducir la vulnerabilidad**. En un sistema, frente a una amenaza en particular, las medidas preventivas en esta categoría tienen el objeto de reducir la posibilidad de que una amenaza, si es que ocurre, dañe el sistema. Por ejemplo un edificio construido con materiales que retarden el fuego será menos vulnerable a la amenaza del fuego que un edificio de madera.
- **Reducir el impacto**. En esta categoría las medidas preventivas se pueden reducir, distribuyendo datos confidenciales a través de un número de bases de datos por separado, cada uno con su propio control de acceso, significa que cada defecto de seguridad da como resultado sólo una cantidad limitada de información que ha sido revelada. Otro enfoque para reducir el impacto es eliminar del sistema toda la información más confidencial.
- **Detectar un incidente**. Las medidas preventivas que corresponden a esta categoría están diseñadas para detectar si fue una violación de seguridad efectiva o si tan sólo fue un intento. Se pueden utilizar los registros del computador para saber como se utilizó el sistema computacional y cómo puede el Software activar automáticamente una alarma, en caso de ocurrir cualquier serie de eventos específicos (por ejemplo. intentos reiterados y sin éxito para conectarse). Otras medidas de este tipo incluyen aquellas diseñadas para detectar fuego, filtraciones de agua e intrusos.

- **Recuperarse del impacto**. Las medidas preventivas en esta categoría son el último recurso de defensa. Se diseñaron para restablecer el servicio normal luego de haber fallado todos los controles anteriores y de haber tenido éxito el intento de dañar al sistema. Los procedimientos para apoyar al sistema, la recuperación del sistema, el plan en caso de desastre y cambios de controles están dentro de esta categoría.

La contramedida de procedimiento antes descrita puede ser informal; sin embargo, es más probable que sea ejecutada correcta y consistentemente (y también se puede revisar) si es descrita con instrucciones detalladas, a veces conocidas como procedimientos de operación de seguridad, que ha sido respaldada formalmente por los directivos superiores como un requisito de la empresa. Como no siempre es evidente después del suceso, si el control de procedimiento se llevó a cabo en forma adecuada, se debe mantener alguna forma de registro por parte de quién lo ejecutó, ya sea como un resultado o como una acción que era necesaria.

La contramedida sistemática incluye algunos modelos del hardware (en un sentido amplio) o del software. Una puerta cerrada y una llave es un ejemplo simple de una contramedida de control de acceso automático; otros ejemplos son las contraseñas, detectores de humedad y calor, sistemas de monitoreo por televisión con circuito cerrado (CCTV) y el software diseñado para generar y validar firmas digitales. En general, las medidas preventivas sistemáticas tienen un precio más alto de implementación que las medidas preventivas de procedimiento, pero, si se manejan adecuadamente, otorgan ventajas en velocidad, espacio y consistencia de la operación.

Aunque las medidas preventivas de procedimiento pueden ser autónomas, aquellas de tipo sistemático pueden estar asociadas con éstas, siempre y cuando se operen correctamente. Este requerimiento se debe tomar en cuenta cuando la contramedida sistemática se ha considerado no sólo porque los procedimientos de respaldo incrementan los costos de operación, sino también porque los procedimientos de respaldo inadecuado pueden fácilmente dar como resultado una contramedida sistemática poco efectiva y que otorga un falso sentido de seguridad.

Un ejemplo común de fallas en el respaldo de una contramedida sistemática son los procedimientos inadecuados en la administración de las contraseñas. El Software de contraseñas generalmente puede verificar una contraseña en contra de su identificador asociado, pero, para que la revisión sea totalmente efectiva, deben existir procedimientos que aseguren que:

a) Los usuarios aprecian la importancia de las contraseñas y la necesidad de mantenerlas en secreto.
b) Las contraseñas sean difíciles de adivinar, por lo tanto, su formato debe cumplir con un estándar mínimo (por ejemplo: una contraseña alfa numérica de 6 dígitos).
c) Las contraseñas sean cambiadas periódicamente, o al momento de una violación, para así reducir el riesgo de daños provenientes de una contraseña que ya ha sido comprometida.
d) Se les asignen contraseñas a los nuevos usuarios y a aquellos que las olviden, como una manera de prevenir que otros las intercepten y logren acceso no autorizado al sistema.

e) Los reiterados intentos de acceso sin éxito sean apropiadamente detectados e investigados, con el objeto de alertar a los administradores respecto de un posible ataque a los sistemas, por medio de la suposición de contraseñas.

f) Las contraseñas redundantes sean prontamente eliminadas del sistema, para hacerlas menos vulnerables al uso no autorizado.

De manera similar, cuando son afectados los perfiles de seguridad, generalmente el software puede garantizar que creará un perfil de seguridad, sin embargo, los procedimientos manuales son necesarios para asegurar, en primer lugar, que los perfiles de seguridad individual se establezcan de manera correcta, que estén actualizados y que se eliminen prontamente cuando ya no se requieran.

2.2.2 SELECCIÓN DE MEDIDAS PREVENTIVAS.

La selección de medidas preventivas requiere que se consideren varios factores:

- ¿Qué medidas preventivas se están ya aplicando?.
- ¿Cuán efectivas son las medidas preventivas que se están aplicando?.
- ¿Existe alguna contramedida que sea innecesaria?.
- ¿Qué contramedida adicional es necesario aplicar?.
- ¿Cuál es la solución que tiene la mejor relación costo-efectividad y que proporciona una protección adicional?.
- ¿Qué solución con la mejor relación costo-efectividad tiene la mayor probabilidad de que sea aceptable para la fuerza de trabajo?.

Durante el análisis de riesgo, el equipo examinador debe grabar las contramedidas que ellos encontraron y también, realizar una evaluación acerca de si ellas son efectivas o necesarias (los cambios en los sistemas y en la organización pueden haber reducido los riesgos en algunas áreas dejando una costosa sobre-provisión de seguridad).

En general, varios factores influyen en la selección de las contramedidas:

- La probabilidad de que una contramedida específica sea efectiva en una situación en especial.
- Su costo, en términos de gestión, instalación, capacitación y mantenimiento; en el caso del software, las cuotas de las licencias también pueden aumentar el costo.
- La cantidad de propiedades de TIC que las medidas preventivas protegerán en caso de cualquier amenaza en particular.
- El nivel de riesgo en donde la contramedida proporciona una protección.
- De qué impactos protege.
- El tipo de contramedida (por ejemplo: reducir una amenaza, reducir la vulnerabilidad, reducir el impacto, detectar, recuperar).

La protección completa requiere que la seguridad se "establezca en forma exhaustiva". Esto significa que se deben considerar las medidas preventivas físicas, lógicas y de procedimientos; y, como ningún sistema de seguridad es perfecto, se debe reconocer que un incidente de seguridad ya sea accidental, deliberado o de origen natural va afectar en cualquier momento a algún sistema; por lo tanto, se tiene que buscar un equilibrio entre aquellas que actúan para prevenir las amenazas,

aquellas que detectan las amenazas que se han materializado y, aquellas que están en condiciones de recuperarse del (o los) impacto(s) resultante(s). Sin embargo, donde se deba hacer una selección (generalmente debido a las restricciones presupuestarias), las contramedidas preventivas deben proporcionar una protección más efectiva que aquellas que son básicamente de carácter detectivo o correctivo.

Algunas medidas preventivas reducirán la exposición a más de una amenaza: el número de amenazas que una contramedida controla efectivamente se define como la "extensión de control".

La extensión de control, es un punto importante que se debe considerar al momento de seleccionar las contramedidas que permiten una cobertura más amplia al más bajo costo. Por ejemplo, el acceso no autorizado a los datos a menudo es controlado por los sistemas de contraseñas. Esta amenaza también se podría controlar (aunque con menos efectividad) llevando la contabilización del uso de los sistemas por parte de los usuarios responsables por sus acciones. De este modo, un sistema de identidad personal única (por ejemplo: la conexión IDs) y las conexiones automáticas del computador, junto con revisiones periódicas de las conexiones producidas por el sistema, pueden controlar por sí solos el límite de la mala conducta en el caso de que el personal este consciente de que pueden ser descubiertos. Además, las bitácoras del computador también se pueden utilizar para controlar otros problemas tales como: rastrear la causa de porqué el hardware, el software y la comunicación de los datos, y analizar cómo funciona el programa. De este modo, el uso razonable de las bitácoras del computador tiene una expansión del control más amplia que las contraseñas.

Mientras que los controles técnicos no se deben anular si parecen necesarios, generalmente, es más costoso comprar y mantener los técnicos que los de procedimiento. Por lo tanto, es importante equilibrar los costos en la expansión de control frente a los niveles de riesgo y, es aquí donde la seguridad de las metodologías automatizadas puede ofrecer una ventaja diferente cuando se realizan esos cálculos.

2.2.3 CONTROLES DE REFERENCIA.

"Los controles de referencia", "los códigos de práctica" o "los estándares mínimos" representan un nivel normal de protección que todos los sistemas deben cumplir o exceder. Los controles de referencia para una organización en particular establecerán un nivel que es apropiado para los tipos de amenazas que enfrentan sus sistemas, y los impactos que causaría la revelación no autorizada, la destrucción o la modificación de información entregada por ellos. El propósito de los controles de referencia es asegurar que exista un mínimo nivel de seguridad en toda la organización, sin tener que incurrir en los gastos de una completa revisión de la administración del análisis de riesgo para cada sistema. Cuando una organización está conectada a los sistemas de información de otras organizaciones, debe formar parte de su relación contractual un acuerdo respecto al estándar de controles de referencia.

Los controles de referencia asumen normalmente que las amenazas enfrentan un sistema de información irreprochable y que el impacto de una violación será moderado; por lo tanto, ellos aplican el requerimiento "normal" de seguridad. Cuando las amenazas a un sistema son particularmente altas, se debe realizar un

análisis de riesgo formal para identificar cualquier contramedida adicional que se necesite para reducir los riesgos a un nivel aceptable.

2.3 PROPOSICIONES PARA LA ADMINISTRACIÓN DE LOS RIESGOS (CONTROLES O SALVAGUARDAS RECOMENDADOS Y MONITOREO).

Después del análisis de los riesgos y la evaluación de los procedimientos de control implementados por la organización para resguardarse de ellos, procede que el auditor analice la situación de exposición al riesgo en que se encuentra la organización.

Es en esta etapa en la cual el auditor debe mostrar su experiencia y dominio sobre la materia, especialmente al tener que generar una fuente de sugerencias y recomendaciones para fortalecer los procedimientos de control, de manera tal que se minimice el nivel de exposición.

Respecto de las tecnologías, quizás en enfoque más amplio y concreto en el cual se puede basar el auditor para satisfacer estos requerimientos, es el enfoque de objetivos de control para tecnología de información y tecnologías relacionadas (COBIT).

Para los efectos de seleccionar las mejores prácticas de control y seguridad frente a las TIC, hoy por hoy, se cuenta con varias herramientas, entre las cuales están:

- **ISO 17.799**. Es un conjunto de controles que considera las mejores prácticas en seguridad de información incluyendo las políticas, prácticas, procedimientos, estructuras, organizacionales y funciones del software.
- **ISO 15.408**. El objetivo es prevenir el acceso no autorizado, modificación o pérdida de uso, similar a confidencialidad, integridad y disponibilidad.

- **SP 800-14+27**. El documento proporciona una base de los principios de seguridad y prácticas para el uso, protección y diseño de los sistemas de información gubernamental.
- **SAS 94**. Esta norma requiere que el auditor financiero considere la tecnología de información como parte del control interno.
- **COBIT**. Objetivos de control para tecnología de información y tecnologías relacionadas.

De todos éstos, los más difundidos son la ISO 17.799 y el enfoque de control COBIT, de los cuales el informe se va a tratar en base al enfoque COBIT.

2.3.1 ISO 17.799.

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera sujeto a auditoría y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la organización internacional de normas en diciembre de 2000, ISO 17.799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17.799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

2.3.1.1 MARCO DE LAS RECOMENDACIONES.

ISO 17.799 hoy en día es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17.799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes. Así, la norma discute la necesidad de contar con cortafuegos, pero no profundiza sobre los tres tipos de cortafuegos y cómo se utilizan, lo que conlleva a que algunos detractores de la norma digan que ISO 17.799 es muy general y que tiene una estructura muy imprecisa y sin valor real.

La flexibilidad e imprecisión de ISO 17.799 es intencional por cuanto es difícil contar con una norma que funcione en una variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 17.799 simplemente ofrece un conjunto de reglas a un sector donde no existían.

2.3.1.2 ÁREAS DE CONTROL DE ISO 17.799.

Las diez áreas de control de ISO 17.799 son:

- **Política de seguridad**. Se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte.
- **Organización de la seguridad**. Sugiere diseñar una estructura de administración dentro de la organización que establezca la responsabilidad de

los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

- **Control y clasificación de los recursos de información**. Necesita un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.
- **Seguridad del personal**. Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También, determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe implementar un plan para reportar los incidentes.
- **Seguridad física y ambiental**. Responde a la necesidad de proteger las áreas, el equipo y los controles generales.
- **Manejo de las comunicaciones y las operaciones**. Los objetivos de esta sección son:
    - Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
    - Minimizar el riesgo de falla de los sistemas.
    - Proteger la integridad del software y la información.
    - Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
    - Garantizar la protección de la información en las redes y de la infraestructura de soporte.

- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

- **Control de acceso**. Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.
- **Desarrollo y mantenimiento de los sistemas**. Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.
- **Manejo de la continuidad de la empresa**. Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.
- **Cumplimiento**. Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17.799 concuerda con otros requisitos jurídicos, como la directiva de la Unión Europea que concierne la privacidad, la ley de responsabilidad y transferibilidad del seguro médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Billey (GLBA por su sigla en inglés). También requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

2.3.1.3 BENEFICIOS DE LA NORMA TÉCNICA ISO 17.799.

Una empresa que implementa la norma técnica ISO 17.799 puede ganar frente a los competidores que no la tiene. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa que tenga alguna norma implementada sobre el tema. Además, una empresa certificada en seguridad de información tendrá en cuenta lo siguiente:

- Mayor seguridad en la empresa.
- Planeación y manejo de la seguridad más efectivos.
- Alianzas comerciales más seguras.
- Mayor confianza en el cliente.
- Auditorías de seguridad más precisas y confiables.
- Menor responsabilidad civil.

2.3.2 OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÒN Y TECNOLOGÍAS RELACIONADAS (COBIT).

COBIT, es una herramienta de gobierno de TIC que ha cambiado la forma en que trabajan los profesionales de TIC. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TIC necesitan ser administrados por un conjunto

de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas practicas de seguridad y control en tecnología de información, COBIT se fundamenta en los objetivos de control existentes de la information systems audit and control foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los objetivos de control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa.

2.3.2.1 MISIÓN DE COBIT.

La misión de COBIT es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes, los usuarios finales y auditores; en la cual se detalla a continuación:

- **La gerencia**. Para apoyar sus decisiones de inversión en TIC y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- **Los usuarios finales**. Quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- **Los auditores**. Para soportar sus opiniones sobre los controles de los proyectos de TIC, su impacto en la organización y determinar el control mínimo requerido.

- **Los Responsables de TIC**. Para identificar los controles que requieren en sus áreas.

También, puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de TIC en las empresas.

2.3.2.2 CARACTERÍSTICAS DEL COBIT.

COBIT presenta las siguientes características:

- Orientado al negocio.
- Alineado con estándares y regulaciones.
- Basado en una revisión crítica y analítica de las tareas y actividades de TIC.
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

2.3.2.3 PRINCIPIOS DEL COBIT.

El enfoque del control en TIC se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TIC que deben ser administrados por procesos de TIC.

El desarrollo de COBIT ha traído como resultado la publicación del marco referencial general y de los objetivos de control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del proyecto de investigación COBIT.

Se determinó que las mejoras a los objetivos de control originales deberían consistir en:

- El desarrollo de un marco referencial para control en TIC como fundamento para los objetivos de control en TIC y como una guía para la investigación consistente en auditoría y control de TIC.
- Una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho.
- Una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en TIC y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.).
- Una revisión crítica y actualización de las guías actuales para desarrollo de auditorias de sistemas de información.

Sin excluir ningún otro estándar aceptado en el campo del control de sistemas de información que pudiera emitirse durante la investigación, las fuentes han sido identificadas inicialmente como:

- Estándares técnicos de ISO, EDIFACT, etc.
- Códigos de conducta emitidos por el Council of Europe, OECD, ISACA, etc.
- Criterios de calificación para sistemas y procesos de TIC: ITSEC, ISO9000, SPICE, TickIT, etc.
- Estándares profesionales para control interno y auditoria: reporte COSO, GAO, IFAC, IIA, ISACA, estándares CPA, etc.
- Prácticas y requerimientos de la industria de foros industriales (ESF, 14) y plataformas patrocinadas por el gobierno (IBAG, NIST, DTI).

- Nuevos requerimientos específicos de la industria de la banca y manufactura de TIC.

El desarrollo de COBIT tiene como resultado en la publicación de:

- **Resumen ejecutivo**. El cual, adicionalmente a esta sección de antecedentes, consiste en una síntesis ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT) y el marco referencial (el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TIC el cual se detalla en el anexo A).
- **Marco referencial**. Que describe en detalle los 34 objetivos de control de alto nivel (anexo A) e identifica los requerimientos de negocio para la información y los recursos de TIC que son impactados en forma primaria por cada objetivo de control.
- **Objetivos de control**. Los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 318 objetivos de control detallados y específicos a través de los 34 procesos de TIC (anexo A).
- **Directrices de auditoría**. Las cuales contienen los pasos de auditoria correspondientes a cada uno de los 34 objetivos de control de TIC de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TIC con respecto a los 318 objetivos detallados de control

(anexo A) recomendados para proporcionar a la gerencia certeza o algunas recomendaciones de mejoramiento.

- **Conjunto de herramientas de implementación**. El cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

2.3.2.4 LOS PRINCIPIOS DEL MARCO REFERENCIAL.

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TIC se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la tecnología de información que deben ser administrados por procesos de TIC.

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

- **Requerimientos de calidad**. Calidad, costo, entrega (de servicio).
- **Requerimientos Fiduciarios (COSO)**. Efectividad y eficiencia de operaciones, confiabilidad de la información, cumplimiento de las leyes y regulaciones.
- **Requerimientos de seguridad**. Confidencialidad, integridad, disponibilidad.

La calidad ha sido considerada principalmente por su aspecto 'negativo' (no fallas, confiable, etc.), lo cual también se encuentra contenido en gran medida en los

criterios de integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo, atractivo, desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de objetivos de control de TIC. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega (de servicio) de la calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el costo es también considerado que queda cubierto por la eficiencia.

Para los requerimientos fiduciarios, COBIT no intentó reinventar la rueda, se utilizaron las definiciones de COSO para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones.

Sin embargo, la confiabilidad de información fue ampliada para incluir toda la información y no sólo información financiera.

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, fue descubierto que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

El marco referencial consta de objetivos de control de TIC de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TIC al considerar la administración de sus recursos.

Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta típicamente con requerimientos de control diferentes a los de actividades discretas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TIC, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios.

Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TIC.

Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos:

- Recursos de TIC.
- Requerimientos de negocio para la información.
- Procesos de TIC.

Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente. Por ejemplo, los gerentes de la empresa pueden interesarse en un

enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos).

Un gerente de TIC puede desear considerar recursos de TIC por los cuales es responsable. Propietarios de procesos, especialistas de TIC y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control.

Las definiciones para los dominios mencionados son las siguientes:

- **Planeación y organización**.

  Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

- **Adquisición e Implementación**.

  Para llevar a cabo la estrategia de TIC, las soluciones de TIC deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

- **Entrega y soporte.**

  En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- **Monitoreo.**

  Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

En resumen, los recursos de TIC necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

Los objetivos de control de TIC han sido organizados por proceso y actividad, pero también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista estratégico como se explicó anteriormente, sino también para facilitar enfoques combinados o globales, tales como instalación y implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de TIC por un proceso.

También, deberá tomarse en cuenta que los objetivos de control COBIT han sido definidos en una manera genérica, por ejemplo, sin depender de la plataforma

técnica, aceptando el hecho de que algunos ambientes de tecnología especiales pueden requerir una cobertura separada para objetivos de control.

2.3.2.5 DIRECTRICES DE AUDITORÍA.

Las directrices de auditoria ofrecen una herramienta complementaria para la fácil aplicación del marco referencial y los objetivos de control COBIT dentro de las actividades de auditoria y evaluación. El propósito de las directrices de auditoría es contar con una estructura sencilla para auditar y evaluar controles, con base en prácticas de auditoria generalmente aceptadas y compatibles con el esquema global COBIT.

Los objetivos y prácticas individuales varían considerablemente de organización a organización y existen muchos tipos de practicantes dedicados a actividades relacionadas con la auditoría; por ejemplo, auditores externos, auditores internos, evaluadores, revisores de calidad, y asesores técnicos. Por estas razones, las directrices de auditoría tienen una estructura genérica y de alto nivel.

Los auditores deben cumplir con algunos requerimientos generales para proporcionar a los directivos y a los poseedores de los procesos de negocios, seguridad y asesoría respecto a los controles en una organización: ofrecer una seguridad razonable de que se está cumpliendo con los objetivos de control correspondientes; identificar dónde se encuentran las debilidades significativas en dichos controles; justificar los riesgos que pueden estar asociados con tales debilidades y finalmente, aconsejar a estos ejecutivos sobre las medidas correctivas que deben adoptarse. COBIT ofrece políticas claras y prácticas eficaces en materia de seguridad y control de información, así como tecnología asociada. Por tanto, las directrices de auditoría firmemente

basados en los objetivos de control, toman la opinión del auditor a partir de la conclusión de auditoría, remplazándola con criterios normativos.

2.3.2.6 ESTRUCTURA GENERAL DE LAS DIRECTRICES DE AUDITORÍA.

El modelo más común para evaluar el control es el modelo de auditoría. Otro enfoque que se está adoptando cada vez más es el modelo de análisis de riesgos, todos aquellos involucrados en la evaluación del control pueden inclinarse por cualquiera de los dos modelos.

Los objetivos de la auditoría son:

- Proporcionar administración con aseguramiento razonable de que se están cubriendo los objetivos de control.
- En donde existan debilidades de control significativas, justificar los riesgos resultantes, y aconsejar a la administración sobre acciones correctivas.

La estructura generalmente aceptada del proceso de auditoría es:

- Identificación y documentación.
- Evaluación.
- Pruebas de cumplimiento.
- Pruebas justificantes.

El proceso de TIC, por lo tanto, se audita mediante:

- **La obtención** de un entendimiento de los riesgos relacionados con los requerimientos del negocio y de las medidas relevantes de control.

- **La evaluación** de la conveniencia de los controles establecidos.
- **La valoración** del cumplimiento por medio de probar si los controles establecidos están funcionando como se espera, de manera consistente y continúa.
- **La justificación** del riesgo de que los objetivos de control no se estén cumpliendo mediante el uso de técnicas analíticas y/o consultando fuentes alternativas.

Con el objetivo de brindar asistencia a la administración en la forma de asesoría de aseguramiento, se ha desarrollado esta estructura dentro de un marco referencial fundamentado en los requerimientos del COBIT:

- Presentación en un enfoque de niveles.
- Orientación hacia los objetivos del negocio.
- Manejado en función del proceso.
- Los recursos que necesitan administrarse.
- Los criterios de información que se requieren.

En el nivel más alto, este enfoque general de auditoría está apoyado por:

- El marco referencial de COBIT, particularmente el resumen con la clasificación de procesos de TIC, los criterios de información aplicables y los recursos de TIC.
- Los requerimientos para el proceso de auditoria mismo.
- Los requerimientos genéricos para la auditoría de procesos de TIC.
- Los principios generales de control.

El segundo nivel está compuesto por las directrices detalladas de auditoría para cada uno de los procesos de TIC.

Las directrices han sido presentadas en una plantilla estándar que sigue la estructura general de obtención, evaluación, valoración y justificación. Esta plantilla ha sido aplicada a las directrices de auditoría genéricos de TIC, así como también a las directrices de auditoría detallados.

En el tercer y último nivel, el auditor puede complementar las directrices de auditoría para cubrir las condiciones locales, conduciendo la fase de planeación de auditoria con puntos de atención de auditoria que influyen sobre los objetivos detallados de control mediante:

- Criterios específicos del sector.
- Estándares de la industria.
- Elementos específicos de la plataforma.
- Técnicas detalladas de control empleadas.

De importancia para este nivel está el hecho de que los objetivos de control no son necesariamente aplicables siempre y en cualquier lugar. Por lo tanto, se sugiere que se realice una evaluación de riesgos de alto nivel para determinar sobre qué objetivos se necesita enfocarse específicamente y cuáles pueden ignorarse.

Todos estos elementos se ofrecen para apoyar la planeación y la realización de las auditorias de TIC y para una mejor aplicación integrada de los lineamientos detallados de auditoria. Los lineamientos no son exhaustivos y no son aplicables universalmente.

El nivel de información de apoyo (lineamientos genéricos, requerimientos del proceso de auditoria y observaciones de control) ayudará a los auditores a desarrollar el programa de auditoria que necesitan.

2.3.2.7 RELACIÓN ENTRE LOS OBJETIVOS DE CONTROL Y LAS DIRECTRICES DE AUDITORÍA.

Los objetivos han sido desarrollados a partir de una orientación al proceso porque la administración está buscando asesoría a proactivo sobre cómo tratar el problema de mantener TIC bajo control. Los objetivos de control ayudan a la administración a establecer el control sobre el proceso, las directrices de auditoría ayudan al auditor o asesor a asegurar que el proceso está realmente bajo control, de tal manera que los requerimientos de información necesarios para lograr los objetivos del negocio serán satisfechos.

La relación entre estos dos conceptos es el proceso, por lo que las directrices de auditoría han sido desarrolladas para cada uno de los procesos, en oposición para cada uno de los objetivos de control.

En cuanto al marco referencial de control representado por el modelo de cascada, las directrices de auditoría pueden verse como los elementos que proporcionan retroalimentación a partir de los procesos de control para los objetivos del negocio.

Los objetivos de control son la guía que baja por la cascada para tener el proceso de TIC bajo control.

Algunas veces, las directrices de auditoría son traducciones literales de los objetivos de control; con mayor frecuencia, las directrices buscan la evidencia de que el proceso esté bajo control.

2.3.2.8 DESCRIPCIÓN DE LOS NIVELES DE RIESGO DE TIC.

1 Bajo. Las áreas de tecnología de la información enmarcadas en este grupo tienen bajo nivel de riesgo. Si hay deficiencias, éstas son de naturaleza menor y pueden ser fácilmente administradas, por ejemplo el personal no esta conciente de la responsabilidad que tiene con la institución.

2 Medio Bajo. Las áreas de tecnología de la información enmarcadas en este grupo también tienen bajo nivel de riesgo, pero se observan debilidades, que pueden ser corregidas en el curso normal del negocio con un esfuerzo adicional limitado, por ejemplo no existe una clara política de atención con los usuarios y los proveedores tanto en hardware como software.

3 Medio. Las áreas de tecnología de la información enmarcadas en este grupo están experimentando una combinación de factores adversos que requiere acciones correctivas de relativa urgencia. Los problemas están identificados y requieren preocupación y monitoreo superior a lo normal, por ejemplo no existe documentación de los diferentes sistemas que se desarrollan, manual de usuarios para el manejo de los diferentes módulos.

4 Medio Alto. Las áreas de tecnología de la información enmarcadas en este grupo operan en condiciones inaceptables en cuanto al riesgo que asumen. Está presente una gran probabilidad de falla operacional y/o información financiera pero las debilidades no son tan severas como para comprometer una inmediata falla del área de sistemas informáticos. Es necesario que se promueva acciones correctivas de urgencia, por ejemplo no existen políticas de seguridad de información (entrega de claves a los diferentes sistemas, backups, acceso a internet, ingreso y salida de los equipos de TIC de la entidad, etc).

5 Alto. Las áreas de tecnología de la información enmarcadas en este grupo presentan una combinación de debilidades y tendencias adversas que están en un punto en que la continuación de la operación del área de sistemas informáticos está en duda. Es necesario que se promueva acciones correctivas y se ejerza seguimiento continuo, por ejemplo no existe un planeamiento de TIC alineado a la entidad, trayendo como consecuencia una adquisición y implementación de TIC que no concuerde con la finalidad de la entidad.

2.3.2.9 MODELO DE MADUREZ.

- Se refieren a los requerimientos de negocio.
- Son escalas que permiten comparaciones entre sí.
- Son reconocibles como un perfil de la empresa en relación con el Gobierno de TIC y control.

El modelo de madurez se puede cuantificar de la siguiente manera

0 No-Existente. Carencia total de cualquier proceso reconocible.

La organización no ha reconocido siquiera que hay un asunto que atender.

1 Inicial. Hay evidencia de que la organización ha reconocido que existe una situación a ser atendida. No hay, sin embargo, procesos estandarizados sino enfoques que tienden a ser aplicados en casos individuales. El enfoque general de la gerencia es desorganizado.

2 Repetible. Se han desarrollado procesos al grado de que procedimientos similares se llevan a cabo por personas distintas, quienes son responsables de una misma tarea.

No existe entrenamiento o comunicación formal de procedimientos estándar y la responsabilidad se deja a un individuo.

3 Definido. Se han estandarizado y documentado procedimientos y comunicado a través de entrenamiento. Sin embargo se ha dejado al individuo, el seguir estos procesos, y es probable que las desviaciones no sean detectadas. Los procedimientos no son sofisticados pero son la formalización de la existencia de prácticas.

4 Administrado. Es posible monitorear y medir el cumplimiento con procedimientos y tomar acción donde los procesos parecen no estar funcionando efectivamente. Los procesos se encuentran bajo mejora constante y proporcionan una buena práctica. Automatización y herramientas se utilizan en forma limitada y fragmentada.

5 Optimizado. Los procesos han sido refinados a un nivel de mejores prácticas, basados en los resultados de mejoras continuas y modelos de madurez con otras organizaciones. TIC es utilizada en una forma integrada para automatizar el flujo de trabajo, proporcionando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte rápidamente.

CAPÍTULO III

3 FUNDAMENTOS DE AUDITORÍA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN.

En años recientes, ha sido cada vez más evidente para los legisladores, usuarios y proveedores de servicios la necesidad de un marco referencial para la seguridad y el control de TIC. Un elemento critico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de TIC. En esta sociedad global (donde la información viaja a través del ciberespacio sin las restricciones de tiempo, distancia y velocidad) esta crítica emerge de:

- La creciente dependencia en información y en los sistemas que proporciona dicha información.
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber-amenaza" y la guerra de la información.
- La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Verdaderamente, la información y los sistemas de información son influyentes en las organizaciones (desde la plataforma del usuario hasta las redes locales o amplias, cliente servidor y equipos). Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede

proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener apreciación y un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

La administración debe decidir la inversión razonable en seguridad y control en TIC y como lograr un balance entre riesgos e inversiones en control de un ambiente de TIC frecuentemente impredecible. La administración necesita un marco referencial de prácticas de seguridad y control de TIC generalmente aceptadas para medir comparativamente su ambiente de TIC, tanto el existente como el planeado.

Existe una creciente necesidad entre los usuarios en cuanto a la seguridad de los servicios TIC, a través de la acreditación y la auditoría de servicios de TIC proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados. Actualmente, sin embargo, es confusa la implementación de buenos controles de TIC en sistema de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales.

Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan una base general a ser establecida como primer paso.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar frente a la gerencia su opinión acerca de los

controles internos. Sin contar con un marco referencial, esta se convierte en una tarea demasiada complicada. Esto ha sido mostrado en varios estudios recientes acerca de la manera en la que los auditores evalúan situaciones complejas de seguridad y control en TIC, estudios que fueron dados a conocer casi simultáneamente en diferentes partes del mundo. Incluso, la administración consulta cada vez mas a los auditores para que la asesoren en forma proactiva en lo referente a asuntos de seguridad y control de TIC.

3.1 CONCEPTO DE AUDITORÍA TIC.

El concepto de auditoría en forma genérico se define como:

La disciplina que mediante técnicas y procedimientos aplicados en una organización por personas independientes a la operación de la misma, evalúa el cumplimiento de los objetivos institucionales, emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de cumplimiento de dichos objetivos.

La auditoría tiene como propósito principal proporcionar la base informativa que justifica la implementación de recomendaciones que posibiliten mejoras administrativas por parte de la dirección de la entidad auditada, quien además se encuentra obligada a aplicar, cuando sea necesario, las sanciones pertinentes. Para la ejecución de la auditoría deben diseñarse acciones y procedimientos que ofrezcan la garantía razonable para la detección de los errores, irregularidades y los actos ilícitos que pudieran repercutir directa o sustancialmente sobre los valores que figuran en los estados financieros o sobre los objetivos de la auditoría, así como debe prestarse atención a las situaciones o transacciones susceptibles de entrañar actos ilícitos que puedan afectar indirectamente los resultados de la auditoría. Cualquier elemento que

permita al auditor advertir la existencia de irregularidades, fraude o algún error que pueda tener efectos materiales sobre la auditoría en curso debe motivar su revelación suficiente y adecuar los procedimientos para verificar o disipar tal situación. La auditoría es una fuerza positiva que busca mejorar la administración, dirigiéndose a encontrar medidas más efectivas, eficientes y económicas que eleven el desempeño (rendimiento) y la calidad de los servicios, evitando la reiteración d circunstancias adversas reveladas por la auditoría. Con respecto a la auditoría gubernamental se dirige a la mejora de las operaciones futuras, más que a exclusiva crítica del pasado, a la sola revelación de irregularidades o a la aplicación de sanciones. Los auditores gubernamentales desarrollan un servicio útil para el público, congreso de la república, gobierno como un conjunto y alta dirección de la entidad sujeta a examen, a través de la evaluación y verificación de las operaciones, actividades y contratos gubernamentales, dando fe de su grado de conformidad con criterios establecidos y formulando recomendaciones para mejoras futuras.

A continuación daremos un concepto de auditoría con respecto a las tecnologías de la información y comunicación (TIC):

La auditoría de TIC consiste en un examen objetivo, critico, sistemático, eminentemente posterior y selectivo de las políticas, normas, practicas, procedimientos y procesos con el fin de emitir una opinión respecto a la eficiencia en la utilización de los recursos informáticos: la confiabilidad, consistencia, integridad y oportunidad de la información y la efectividad de los controles en los sistemas de información computarizados.

Los amplios y profundos conocimientos requeridos para la auditoría de TIC, implica:

- Enfoque de auditoría orientado a los riesgos de las aplicaciones.
- Uso del computador como herramienta de auditoría.
- Aplicación de normas nacionales e internacionales para probar e implementar sistemas de calidad de sistemas en desarrollo de software.
- Comprensión de las reglas y expectativas de negocios en la auditoría de sistemas bajo desarrollo para la compra de paquetes de software y administración de proyectos.
- Evaluación de la seguridad y privacidad de la información, que pueden poner en riesgo a la organización.
- Examinar y verificar el cumplimiento con las normas legales que podrían afectar o colocar en riesgo a la organización.
- Evaluación del ciclo de vida de desarrollo de sistemas (SDLC) o nuevas técnicas de desarrollo (ejemplo.: prototipos, desarrollo rápido de sistemas, etc.).
- Informes para la administración y seguimientos para asegurar que las acciones tomadas están operando adecuadamente.

Los objetivos de la auditoría de TIC están enmarcados en uno o más de los siguientes puntos:

- Cumplimiento de las políticas, normas y procedimientos de orden gubernamental e institucional (adquisición, contratación e instalación de servicios para el desarrollo de la función informática).

- Comprobar el adecuado uso y resguardo de los recursos informáticos de la entidad.
- Verificar que se efectúa el mantenimiento preventivo y correctivo de los recursos informáticos, para obtener la confiabilidad e integridad de los sistemas.
- Grado de confiabilidad y privacidad del ambiente informático.

Entre los principales motivos de una auditoría de TIC encontramos:

- Aumento del presupuesto del departamento de procesamiento de datos.
- Desconocimiento de la situación informática de la empresa.
- Falta total o parcial de seguridad lógica y física que garanticen la integridad del personal, equipo e información.
- Descubrimiento de fraudes efectuados con el uso del computador.
- Falta de una planificación informática. Falta de visión.
- Organización que no funciona correctamente, debido a falta de política, objetivos, normas, metodología, estándares, delegación de autoridad, asignación de tareas y adecuada administración del recurso humano.
- Descontento general de los usuarios, motivados generalmente, por incumplimiento de plazos y mala calidad de resultados.
- Falta de documentación o documentación incompleta de sistemas.

Si se tiene en cuenta que el objetivo básico que se busca con la adquisición y utilización del cómputo es de entregar información confiable, útil y oportuna, el

ámbito del auditor debe abarcar áreas donde hace presencia el computador y aquéllas que puedan afectar el cumplimiento de dicho objetivo, tales como:

- La gerencia de sistema.
- La organización y el personal.
- El área del computador.
- Las aplicaciones.
- Los estándares de documentación y desarrollo.
- La operación del computador.
- La gerencia financiera.
- Los planes de desarrollo informático.
- Los controles y la seguridad en general.
- Los archivos maestros y de transacciones.
- La red de comunicaciones y de datos.
- La Internet / Intranet.
- La transferencia electrónica de documentos.

3.2 TÉCNICA DE AUDITORÍA.

Las normas de auditoría establecen que se debe obtener evidencia suficiente y competente en relación a la información (o sistema) que se está auditando. Para operacionalizar lo anterior, se puede definir evidencia como cualquier información que utiliza el auditor para determinar si el objeto auditado cumple con los criterios establecidos (principios, normas, estándares, etc. según sea la materia sometida a escrutinio).

La evidencia se obtiene por el auditor aplicando ciertas técnicas, cuya calidad o competencia difiere una de otra, pero que en conjunto debe permitirle formarse y expresar una opinión respecto de la materia examinada. Existen casos que por limitaciones inherentes, no pueda aplicar todas las técnicas necesarias, y dependiendo de lo significativo del caso, puede obligarle a abstenerse de opinar, señalando el motivo de ello.

Las técnicas para obtener evidencia son las siguientes:

- **Examen Físico**. Es la inspección de un objeto tangible que hace el auditor para cerciorarse de su existencia y volumen o valor, dependiendo del elemento.
- **Confirmación**. Está constituida por las afirmaciones orales o escritas de una tercera parte independiente que permite verificar la información o hechos examinados por el auditor. Aquella de carácter escrito, se evalúa como de mayor calidad, puesto que identificar al responsable de ella y permanece en el tiempo.
- **Examen de documentos**. Se realiza para verificar la precisión de la información o de las operaciones institucionales. Asimismo, es muy importante para establecer la validez de ellas, esto es si fueron procesadas conforme a las normas o procedimientos establecidos en la estructura de control interno.
- **Observación**. Es el uso de los sentidos para evaluar ciertas actividades. De este modo, se puede establecer por ejemplo el estado de conservación de objetos físicos, si se cumplen o no determinadas controles al ejecutar

operaciones de interés, etc. Es decir, una experiencia sensible directa. Su calidad está limitada a la concurrencia de otras técnicas complementarias.

- **Entrevistas o indagación**. Es obtener evidencia oral del auditado o de un tercero independiente. Su calidad obviamente es limitada, y también requiere la concurrencia de evidencia adicional obtenida con otras técnicas.
- **Recálculo o recómputo**. Implica reprocesar por el auditor cálculos relativos a la información sometida a examen, a fin de verificar la precisión aritmética.
- **Procedimientos analíticos**. Es el uso de razones y relaciones, provenientes de estados financieros y/o estadísticas, para determinar si los valores acumulados son razonables. Debido a su importancia y potencia, se utilizan tanto en la etapa de planificación como de terminación de la auditoría, puesto que proporcionan una medida de coherencia de los valores examinados.

3.3 ENFOQUE DE AUDITORÍA.

Las normas de auditoría, el proceso, sus técnicas, procedimientos, etc. son cuerpos ya normativos, orientadores, etc. según su caso. Sin embargo, la forma de articular el trabajo en forma sistematizada y eficiente, de acuerdo a dichas normativas, es propio de cada entidad auditora. Corresponde a su visión acerca de cómo enfrentar la actividad. Es así como nacen los enfoques particulares, y que en muchos casos realimentan el desarrollo de la profesión. Existen grandes empresas mundiales de auditoría, tienen cuerpos investigadores encargados de perfeccionar constantemente dichos enfoques o metodologías. Por otra parte, también entidades especializadas sin fines de lucro, universidades y asociaciones profesionales hacen lo propio, sin dejar de mencionar a autores independientes destacados.

3.4 ALCANCE DE LA AUDITORÍA.

Identifica con claridad cuál es la responsabilidad del auditor, respecto a la realización de su trabajo. Al inicio, este concepto se refiere a los contenidos o límites temáticos bajo los cuales se desarrollarán las actividades. Aquí se deben identificar las áreas funcionales, el período que cubre la auditoría, los sistemas de información, aplicaciones y ambientes de procesamiento auditados. En la etapa del informe, describe la naturaleza, oportunidad y profundidad del trabajo ejecutado, haciendo presente cualquier restricción o limitación material que se haya suscitado, y que por lo tanto, lo eximen de expresar una opinión con todo el grado de certeza que fuera deseable.

3.5 TECNICAS DE AUDITORÍA ASISTIDAS POR COMPUTADORA (TAAC´S).

Esta se relaciona con el medio utilizado para obtener evidencia, más que por el tipo de acción realizado. Así, se denominan TAAC's a aquellas operaciones realizadas por el auditor para obtener evidencia, que están apoyadas por el uso de tecnologías de la información.

La técnica de auditoría facilitada por el uso de las computadoras, es lo que da forma al concepto de TAAC´s. El auditor en el desarrollo de su labor profesional aplica técnicas de control tales como:

- Observación.
- Inspección.
- Verificación o confirmación.

- Cálculo.
- Etc.

En cada una de ellas puede hacerse uso de las tecnologías de la información, por ejemplo:

- La presencia de cámaras permite que se pueda observar el comportamiento de las personas y de los procesos, sin tener que estar en el mismo sitio.
- El uso de lectora de barras o de bandas magnéticas facilita una revisión de inventarios, de bienes o de acciones que estén debidamente identificados. Esto mismo puede hacerse a través de logs que se construyen en los procesos y van dejando pistas sobre el desempeño del sistema.
- La posibilidad de obtener datos, documentos y especies en forma electrónica, facilita cualquier proceso de confirmación o verificación de los resultados obtenidos.
- El hecho de que los computadores, independiente del tamaño y de la plataforma en que se encuentre, no deja de ser una máquina definida para procesar y calcular en la forma más precisa posible, cantidades o valores, obteniendo en forma rápida, los resultados que permiten comparaciones reales en examen.

De allí que, en nuestros días, las posibilidades de ser asistidos por las computadoras es mucho más expedito que hace unos años atrás. Antes, todo tenía que definirse como requerimientos y en muchos casos no existía una gran conciencia de la

necesidad de control. Hoy, las exigencias de calidad, los estándares de operación y las necesidades de satisfacer un ambiente cada vez más exigente y competitivo, permite disponer de mejores tecnologías para asistirse en la labor de auditoría.

3.6 OBJETIVOS DE CONTROL.

Control de define como:

Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos y de aquí el objetivo de control se puede definir como:

Es el resultado o propósito que se desea alcanzar mediante la implementación de procedimientos de control en los procesos de trabajo de una empresa. Los estándares proveen o de ellos se derivan, con frecuencia objetivos de control. Cuando estos no existan o no estén declarados, el auditor sobre la base de su conocimiento y criterio profesional debe identificarlos y desarrollarlos.

Un objetivo de control apoya el cumplimiento de un factor crítico de éxito, siendo esto algo que se necesita cumplir para poder alcanzar un objetivo institucional. En consecuencia, se tiene toda una jerarquía de criterios que orientan el quehacer corporativo partiendo de la misión hasta llegar a los procedimientos operativos.

Los objetivos de control muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoría.

Los objetivos de control están definitivos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. se proporcionan consideraciones y guías para definir e implementar el objetivo de control de TIC.

La clasificación de los dominios a los que aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los recursos de TIC que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el marco referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 procesos de alto nivel y 318 objetivos detallados de control (anexo A). El marco referencial fue mostrado a la industria de TIC y a los profesionales dedicados a la auditoría para abrir la posibilidad a revisión, dudas y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

3.7 NORMAS DE AUDITORÍA.

Uno de los elementos del concepto de auditoría es la disciplina, es decir, un conjunto de especificaciones que regulan la actuación auditora, y que garantizan la confiabilidad de sus resultados. Entre éstas, se encuentran en forma muy relevante, las normas de auditoría y que para obtener credibilidad en el ambiente de negocios, se someten al escrutinio público de la comunidad de profesionales durante un tiempo de prueba apropiado, luego de lo cual, si no se manifiestan problemas en su aplicación, son promulgados como generalmente aceptados.

Dentro de las normas de auditoria podemos citar:

- **Las normas de auditoría gubernamental (NAGU).** Son los criterios que determinan los requisitos de orden personal y profesional del auditor, orientados a uniformar el trabajo de la auditoría gubernamental y obtener resultados de calidad. Constituyen un medio técnico para fortalecer y uniformar el ejercicio profesional del auditor gubernamental y permiten la evaluación del desarrollo y resultados de su trabajo, promoviendo el grado de economía, eficiencia, eficacia en la gestión de la entidad auditada. Se fundamentan en la ley del sistema nacional de control, su reglamento y en las normas de auditoría generalmente aceptadas(NAGA). La NAGA son aplicables en su totalidad cuando se trata de una auditoría financiera, y en lo aplicable, en una auditoría de asuntos financieros en particular y otros exámenes especiales. La auditoría de gestión requiere, sin embargo, normas complementarias y específicas para satisfacer las necesidades propias de los citados exámenes. Los auditores deben seleccionar y aplicar las pruebas y demás procedimientos de auditoría que, según su criterio profesional, sean apropiadas en las circunstancias para cumplir los objetivos de cada auditoría. Esas pruebas y procedimientos deben planearse de tal modo que permitan obtener evidencia suficiente, competente y relevante para fundamentar razonablemente las opiniones y conclusiones que se formulen en relación con los objetivos de la auditoría. Las normas de auditoría gubernamental son de cumplimiento obligatorio, bajo responsabilidad, por los auditores de la contraloría general de la república (CGR), de los órganos de auditoría interna de las entidades sujetas al sistema y de las sociedades de auditoría designadas por el organismo superior de control. Asimismo, son de observancia, por los

profesionales y/o especialistas de otras disciplinas que participen en el proceso de la auditoría gubernamental. Se caracterizan por ser flexibles, permitiendo su adaptabilidad y actualización, de ser necesario; así como servir de estándares para ponderar la eficiencia y efectividad de la auditoría.

- **Normas ISACA**. Se ha convertido actualmente en una organización global que establece las pautas para los profesionales de auditoria, control y seguridad de sistemas de información. Sus normas de auditoria, control y seguridad de sistemas de información son respetadas por profesionales de todo el mundo. Sus investigaciones resaltan temas profesionales que desafían a sus constituyentes.

3.8 ASPECTOS JURIDICOS DE TIC.

Los sistemas de información como la mayoría de las cosas, se encuentran sujetos a las normas legales que imperan en los diversos países, más aquellas de carácter internacional, en virtud de los acuerdos suscritos en los diversos foros regionales o mundiales.

Orientado a evitar o mitigar riesgos innecesarios originados en infracciones legales que hagan peligrar el logro de los objetivos institucionales, se debe considerar esta variable. Los temas más frecuentes dentro del contexto legal relacionado con los sistemas de información, están en el ámbito del derecho de propiedad intelectual de la información y de software. Asimismo, se incluyen los registros de información de la entidad, la protección de datos y privacidad de información personal, acceso a los controles criptográficos o al uso de ellos, y el uso inadecuado de los recursos de procesamiento de la información. De todo lo anterior, cabe entonces señalar que se

debe procurar asesoramiento jurídico para garantizar el cumplimiento de las leyes nacionales e internacionales. Esto implica que las entidades deben velar porque sus actuaciones estén enmarcadas dentro de las oportunidades que brindan las leyes, reglamentos, etc., a fin de evitar infracciones y violaciones que signifiquen sufrir multas, suspensión de actividades, etc, que hagan peligrar el logro de los objetivos institucionales. Los requisitos legales varían según el país y en relación con la información que se genera en un país y se transmite a otro (por ejemplo flujo de datos a través de fronteras).

Así, toda la actuación puede estar sujeta a normas específicas. El diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos legales, normativos y contractuales.

Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información.

Los temas más frecuentes dentro del contexto legal relacionado con los sistemas de información son los siguientes:

- **Derecho de propiedad intelectual de información y software**.

  Estos derechos protegen el software, contra usos no autorizados o no licenciados. Si no se tiene del debido cuidado, se puede caer en infringir el derecho de terceras partes, del gobierno, etc. Esto podría significar tener que pagar daños o devolver todos los beneficios obtenidos sobre la base de la infracción.

- **Registros de información de la entidad.**

  Estos derechos protegen trabajos, bases de datos contra usos no autorizados, etc.

- **Protección de datos y privacidad de información personal.**

  Dependiendo del tipo de legislación, se identifican como datos personales aquella relacionada con la identificación de las personas naturales, e incluyen lo relacionado con aspectos tales como nombre, dirección, cuentas bancarias, e-mail, teléfonos, tarjetas de créditos, registros médicos, etc. Las personas pueden estar caracterizadas genéricamente como clientes, estudiantes, contribuyentes, empleados, pacientes, etc.

  Con frecuencia las legislaciones, no protegen los datos personales de las personas jurídicas.

  Los datos personales deben ser procesados con apego a las normas legales, coleccionados para fines específicos, explícitamente declarados y para propósitos legítimos; los datos deben estar actualizados y no deben conservarse más allá del tiempo necesario, teniendo consideración a los propósitos con los cuales fueron procesados; no procesar más datos que los necesarios para dichos objetivos.

- **Acceso a los controles criptográficos o el uso de los mismos.**

  Están referidos a los documentos electrónicos (e-document), en los cuales, en principio, no debieran existir discriminación entre un documento digital y otro que no lo es, para propósitos de escribirlos, retenerlos, etc. Estos son accesibles y utilizables, generan confianza, pues están hechos para asegurar integridad, es decir, la información es completa e inalterada. Sin estos

requisitos, no se está obligado a utilizarlo. Para esto se utiliza técnicas criptográficas tales como la firma electrónica, la cual, puede ser un sonido digitalizado, símbolo, proceso, anexado o lógicamente asociado a un contrato o registro, ejecutado o adoptado por una persona con la intención de firmar el registro o documento.

Los actos ilegales que pueden ocurrir con dispositivos criptográficos tienen que ver con copiar, acceder o recrear la firma de otra persona, alterarla o revelarla sin autorización. Crear, alterar, publicar o usar una firma digital para propósitos ilegales o fraudulentos. Usar técnicas criptográficas para propósitos ilegales.

- **Uso inadecuado de los recursos de procesamiento de información.**

  Uso de los computadores u otros dispositivos relacionados para acceder a datos, software, obtener documentación, usarlos, copiarlos o modificarlos. Sacar información o datos de alguna manera. Impedir el acceso a datos. Dañar la integridad de datos. Tomar posesión del uso de datos o de marcas. Alterar, destruir o ingresar datos. Revelación de password o facilitar el acceso a otras personas no autorizadas. Uso de password o nombre de usuarios de otras personas, correo electrónico, u otras formas de acceder a la información. Revelación de datos, a menos que sea requerido por tribunales para dichos efectos, o por alguna ley. Daño o destrucción de un computador, sistema, redes de computadores, o elementos accesorios a estos, impedir o afectar la operación de estos equipamientos.

3.9 FASES DE PROCESO DE AUDITORÍA.

Toda acción de auditoría sigue ciertas fases específicas mediante las cuales se desarrolla el trabajo. Se deben seguir básicamente las siguientes fases:

- Planeamiento.
- Ejecución.
- Informe.
- Seguimiento.

3.9.1 PLANEAMIENTO DE LA AUDITORÍA TIC.

Esta fase siempre es la que reviste mayor relevancia, puesto que se inicia desde el momento en que se conoce el interés de efectuar la auditoría y termina cuando se ha entregado el informe y se efectúa el proceso de seguimiento de las recomendaciones efectuadas.

En esta fase de define adecuadamente los objetivos y el alcance del trabajo, las técnicas y herramientas a utilizar, los recursos humanos y técnicos que se emplearán, así como los plazos para realizar la auditoría.

Provee conocimiento sobre la importancia de los sistemas de información en la organización, una evaluación preliminar de sus fortalezas y debilidades y una lista de materias relacionadas con el área, que sean de potencial significancía y que deberán ser examinadas en la fase de ejecución.

La fase de planeación se compone de actividades importantes tales como:

- **Conocimiento general de la entidad**. Conocer y estudiar en forma general la entidad y la función informática: información relacionada con la

organización, sus objetivos, reglamentos, normas, funciones, estructura del área de sistema, sus equipos, aplicaciones, etc.

- **Evaluación del sistema de control interno del área de sistema**. Son los métodos y procedimientos de administración y protección de recursos informáticos, la confiabilidad de los registros, la eficiencia de las operaciones y la adhesión a las políticas informáticas establecidas por la organización entre las cuales se puede mencionar:
  a) Controles de carácter general; controles de adquisición, organización, desarrollo, administración física y lógica, documentación y seguridad.
  b) Controles de carácter específico; controles de aplicación (entrada, proceso y salida), bases de datos, de procesamiento distribución y de microcomputadores.

- **Programa de auditoría**. Aspectos a cubrir en la fase de ejecución de la auditoría y la disposición en tiempo, modo y lugar de los recursos necesarios para llevar a cabo:
  a) Programa para la evaluación de organización en el área de sistemas.
  b) Programa para la evaluación de la seguridad física y planes de contingencia de la oficina de sistemas.
  c) Programa para la evaluación de la base de datos, archivos y datos.
  d) Programa para evaluación de operaciones en el centro de procesamiento y área de atención a usuarios.
  e) Programa para evaluación de desarrollo y mantenimiento de sistemas.
  f) Programa para evaluación de redes de comunicación.

3.9.2 FASE DE EJECUCIÓN.

El auditor prueba la existencia, de que si son adecuados, si funcionan consistentemente y efectividad de operación de los controles claves que reducen la exposición a los riesgos identificados seleccionados en la fase de planificación. Para ello, aplica diferentes técnicas de auditoría, tales como revisión de evidencia documental, observación, reprocesos, entrevistas, etc.

En esta fase se orienta probar la calidad o veracidad de los productos finales de los sistemas, así como también verificar que los controles que soportan los procesos sean adecuados para garantizar la producción de buenos output o productos.

La evidencia se puede obtener de dos maneras:

- **Pruebas de cumplimiento**. Se usa para determinar si un procedimiento de control prescrito esta funcionando efectivamente y consiste en verificar:
    a) La aplicación de leyes o reglamentos y de los procedimientos establecidos en los manuales que éstos se encuentren actualizados.
    b) El conocimiento por parte del personal, de los manuales y de las políticas del ambiente informático.
    c) La existencia de informe o memorandos preparados por el departamento de informática.
    d) Si han sido implantadas las recomendaciones emitidas por auditoria anteriores.

- **Pruebas sustantivas**. Son para proveer una seguridad razonable sobre la validez de la información producida. El desarrollo de las pruebas es logrado

mediante las aplicaciones de una o varias técnicas de auditoría, ya sea simultánea o secuencial tales como:

a) Analizar registros.

b) Hacer operaciones.

c) Comparar archivos.

d) Estratificar archivos.

e) Seleccionar una muestra aleatoria.

f) Resumir información.

g) Generar reportes.

h) Construir archivos de prueba.

i) Extraer información de un archivo.

j) Realizar análisis estadísticos.

k) Simular parte del sistema o el sistema completo.

3.9.3 INFORME.

Durante las distintas fases del trabajo, el equipo puede hacer comentarios positivos como también hacer presente otros puntos que deberían ser establecidos o respecto de aquellos en que se ha mejorado. Al terminar la ejecución del programa, el gerente de auditoría revisará una lista de aspectos significativos con el gerente del centro de cómputo. Esos puntos no significan necesariamente que serán eliminados, pero son sugerencias útiles para mejorar las operaciones y proteger la función de servicios de información contra fraudes o pérdidas.

Esas sugerencias serán discutidas completamente. El gerente del centro de cómputo esperará expectante para preparar las respuestas a cada uno de los puntos. Lo

corriente es que éstas sean en una forma que se ratifique lo informado para corregir o eliminar las deficiencias observadas El informe incluirá comentarios positivos acerca de las cosas que se encuentran particularmente bien o que son efectivas para lograr buenos controles y proteger los intereses de la administración.

3.9.4 SEGUIMIENTO.

El informe de auditoria contiene regularmente hallazgos y recomendaciones orientadas a superar dichas deficiencias, las que se convierten a su vez en un compromiso para la entidad auditada. En consecuencia, el auditor efectúa revisiones posteriores para evaluar el grado de cumplimiento de las recomendaciones, determinando si éstas han dado los resultados esperados, todo lo cual debe ser reportado en la forma acordada con la administración.

3.10 RIESGO DE AUDITORÍA.

La norma de auditoría sobre planeación indica que una evaluación de riesgo debe efectuarse para proveer una razonable seguridad de que los aspectos importantes han sido considerados y adecuadamente cubiertos. Esta evaluación debería identificar las áreas de alto, mediano y bajo riesgo de existencia de problemas significativos.

La evaluación de riesgos es un proceso subjetivo y especulativo, basado en la información que recaba el auditor, y que en último término, conduce a un juicio de carácter profesional.

Así, el riesgo de auditoría es la probabilidad de que el auditor inadvertidamente pueda llegar a una conclusión incorrecta basado en los hallazgos de auditoría. Esto

puede deberse a errores o irregularidades existentes y que aquél no logró detectar con la aplicación de sus procedimientos de auditoría.

Los tipos de riesgos que se pueden presentar son:

- **Riesgo inherente**. Es la susceptibilidad de que puedan ocurrir errores o irregularidades importantes, suponiendo inicialmente, que no existen controles relacionados. Se hace esta abstracción inicial respecto de los controles existentes, puesto que con posterioridad se consideran conjuntamente con los otros factores.
- **Riesgo de control**. Es la probabilidad de que un error o irregularidad material pueda ocurrir, sin que el sistema de control interno pueda prevenirlo, detectarlo o corregirlo oportunamente.
- **Riesgo de detección**. Es la probabilidad de que el auditor no detecte un error o irregularidad material existente en el área auditada.

CAPÍTULO IV

4 DESARROLLO DE UN CASO PRÁCTICO A LA AUDITORÍA SOBRE SEGURIDAD DE REDES A UNA ENTIDAD.

4. 1 INTRODUCCIÓN.

El presente informe es el resultado de la evaluación realizada a la gerencia de sistemas y tecnologías de información de la contraloría general de la republica (CGR).

La CGR es el órgano superior del sistema nacional de control, que cautela el uso eficiente, eficaz y económico de los recursos del estado, su oficina principal se encuentra ubicada en Lima y sus oficinas regionales en diversos departamentos del Perú.

Actualmente la CGR esta en proceso de descentralización para lo cual, se esta llevando a cabo un proceso de interconexión entre la sede central y sus sedes regionales; el cual se esta implementando de manera progresiva, ya que para esta primera etapa se han considerado los aplicativos más relevantes: sistema de auditoría gubernamental (SAGU), trámite documentario (SICGR), programa de vaso de leche, sistema de tareas y tiempos, sistema de denuncias, sistema de costos, intranet y correo electrónico.

Dentro de los diferentes procesos que realiza la gerencia de TIC se revisó los principales procesos relacionados con la seguridad de la red para al cumplimiento de la misión de la institución, dentro de estos procesos podemos destacar los siguientes:

- Determinar la dirección tecnológica.
- Aseguramiento de servicio continúo.
- Garantizar la seguridad de sistema.

4.2 METODOLOGÍA Y ALCANCE.

Para la auditoría aplicada a la gerencia de TIC de la CGR, se utilizó la metodología COBIT, que es una metodología que posee estándares y regulaciones, basado en una revisión critica de tareas y actividades en tecnología de información, cuya finalidad es la de suministrar a la gerencia de normas generalmente aceptadas basadas en buenas prácticas para el control de TIC, y está sujeta a las exigencias del control interno solicitadas por la alta dirección, considerando en su ejecución las acciones siguientes:

- Elaboración de cuestionarios para ser resueltos por el jefe de la gerencia de sistemas sobre las acciones previstas en los procesos.
- Levantamiento de la información sobre la situación actual de los procesos analizados.
- Elaboración de programas de trabajo, cuestionarios de control interno y formatos de análisis de riesgo.
- Desarrollo de la matriz de procesos de control aplicables a cada uno de los procesos.
- Identificación de observaciones.
- Elaboración del informe final.

Procesos de TIC a considerar:

- Determinar la dirección tecnológica.
- Garantizar la seguridad de sistemas.
- Aseguramiento de servicio continúo.

Para la elaboración de este informe se seleccionaron los siguientes procesos y objetivos COBIT:

1. PLANIFICACIÓN Y ORGANIZACIÓN.

PO3 Determinar la dirección tecnológica.

3.1 Planeamiento de la infraestructura tecnológica.

La función de servicios de información deberá crear y actualizar regularmente un plan de infraestructura tecnológica que concuerde con los planes a largo y corto plazo de tecnología de información.

Dicho plan deberá abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

3.3 Contingencias en la infraestructura tecnológica.

El plan de infraestructura tecnológica deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de infraestructura).

3.4 Planes de adquisición de hardware y software.

La gerencia de TIC deberá asegurar que los planes de adquisición de hardware y software sean establecidos y que reflejen las necesidades identificadas en el plan de infraestructura tecnológica.

3.5 Estándares de tecnología.

La gerencia de TIC deberá definir normas de tecnología con la finalidad de fomentar la estandarización.

2. ENTREGA Y SOPORTE.

DS4 Aseguramiento de servicio continúo.

4.1 Marco de referencia para continuidad de TIC.

La gerencia de la función de servicios de información deberá, crear un marco de referencia de continuidad que defina los roles, responsabilidades, el enfoque basado en riesgos, la metodología a seguir así como las reglas y la estructura para documentar el plan y los procedimientos de aprobación.

4.2 Estrategia y filosofía del plan de continuidad de TIC.

La gerencia deberá garantizar que el plan de continuidad de tecnología de información se encuentra en línea con el plan general de continuidad de la empresa para asegurar consistencia.

4.3 Contenido del plan de continuidad de TIC.

La gerencia de la función de servicios de información deberá asegurar que se desarrolle un plan escrito conteniendo entre otros:

- Guía sobre la utilización del plan de continuidad.
- Procedimiento emergencia para asegurar la integridad de todo el personal afectado.
- Procedimiento para salvaguardar y reconstruir la instalación.
- Procedimiento de comunicación con los interesados: empleados, clientes, proveedores críticos, accionistas y gerencia.

4.6 Prueba del plan de continuidad de TIC.

Para contar con un plan efectivo de continuidad, la gerencia necesita evaluar de manera regular; esto requiere de una preparación cuidadosa, documentación, reportes de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.

4.7 Capacitación para el plan de continuidad de TIC.

La metodología de continuidad para desastres deberá asegurar que todas las partes interesadas reciban sesiones de entrenamiento regulares con respecto a los procedimientos a ser seguidos en caso de un incidente o un desastre.

4.8 Distribución del plan de continuidad de TIC.

Debido a la naturaleza sensitiva de la información del plan de continuidad, dicha información deberá ser distribuida solo a personal autorizado y mantenerse bajo adecuado medida de seguridad para evitar su divulgación.

4.9 Procedimientos de respaldo del procesamiento alterno en el departamento usuario.

La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que los servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.

4.11 Respaldo del sitio y hardware.

La gerencia deberá asegurar que la metodología de continuidad incorpora la identificación de alternativas relativas al centro de cómputo y al hardware de respaldo, así como una selección alternativa final.

DS5 Garantizar la seguridad de los sistemas.

5.1 Manejo de las medidas de seguridad.

La seguridad en tecnología de información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio, tales como:

- Traducir información sobre la evaluación de riesgo a los planes de seguridad de tecnología.

- implementar el plan de seguridad de tecnología de información.
- Monitorear la implementación del plan de seguridad de tecnología de información.

5.2 Identificación, autenticación y acceso.

El acceso lógico y el uso de los recursos de TIC deberán restringirse a través de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Así mismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso como cambio periódico de contraseñas o passwords.

5.3 Seguridad de acceso a datos en línea.

La gerencia de la función de servicios de información deberá implementar procedimientos acorde con la política de seguridad que garantice el control de la seguridad de acceso, tomando como base las necesidades individuales como visualizar, agregar, modificar o eliminar datos.

5.4 Administración de cuentas de usuario.

La gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la adquisición, establecimiento, emisión y suspensión de cuentas de usuario.

5.5 Control de las cuentas de usuario.

La gerencia deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

5.9 Administración centralizada de identificación y derechos de acceso.

Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

5.10 Reportes de actividades de violación y seguridad.

La administración de la función de los servicios de información deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas.

5.11 Manejo de incidentes.

La gerencia deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizadas con suficiente experiencia y equipada con instalaciones de computación rápida y segura.

5.19 Prevención, detección y corrección del software dañino.

Con respecto al software malicioso, tal como los virus informáticos o caballos de troya, la gerencia deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas.

5.20 Arquitectura de firewalls y conexiones con las redes públicas.

Si existe conexión con internet o redes publicas en la organización, se deberá contar con sistemas firewall adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones como también deberá proteger en contra de negación o ataques de servicio.

4.3 OBJETIVOS.

Objetivo principal.

El presente trabajo de auditoría tiene como objetivo principal verificar los procedimientos empleados para salvaguardar la información contra uso no autorizado, así como el servicio disponible de acuerdo con los requerimientos en el periodo enero-diciembre del 2004.

Objetivos específicos.

- Evaluar el planeamiento de la infraestructura tecnológica.
- Evaluar la contingencia de la infraestructura tecnológica.

- Planes de adquisición de software y hardware con relación a la seguridad y continuidad de la red.
- Estándar tecnológico.
- Evaluar los criterios y especificaciones de seguridad vigentes.
- Determinar el grado de efectividad de los sistemas en cuanto a la satisfacción de los requerimientos del usuario y de performance.
- Identificar el nivel de confiabilidad, integridad y disponibilidad de la información; así como también los adecuados procedimientos de autenticación y autorización, copias de respaldo y restauración.

4.4 DESCRIPCIÓN DE LOS PROCESOS EVALUADOS.

La gerencia de TIC asesora, planifica, organiza y dirige las actividades relacionadas con la TIC, equipos de procesamiento de información y la red de transmisión de datos. Asimismo, apoya las acciones de control en temas relacionados con la informática de acuerdo a los lineamientos impartidos por la alta dirección.

A partir de lo antes mencionado y la coyuntura actual de la organización se han identificado los procesos críticos del área de TIC en el ámbito de la seguridad de la red, los cuales se describen a continuación.

- **Determinar la dirección tecnológica**.

  A pesar que no se cuenta formalmente con una política y procedimiento para la evaluación, creación y la actualización del plan de infraestructura tecnológico, se ha establecido una política de supervisión de los servicios de

información, pero que no cuentan con un marco de referencia para la evaluación de la dirección tecnológica alineada a la entidad.

De lo anterior se puede deducir que existe una inadecuada planificación de los servicios de TIC relacionada con la seguridad y la continuidad de los servicios riesgos que pueden convertirse en amenazas y afectar de manera significativa los objetivos y metas de la organización

- **Aseguramiento de servicios continuos.**

  Los procesos de recuperación ante la caída de la red se realiza utilizando procedimientos adquiridos con la practica, las cuales no se encuentran dentro de un marco de referencia así como la responsabilidad de los servicios continuos recae en una sola persona no existiendo segregación de funciones.

  La entidad no presenta una política muy clara respecto a recuperación y contingencia de los servicios informáticos ante una eventual caída de red.

- **Garantizar la seguridad de los sistemas.**

  Con el fin de contar con información confiable y segura la gerencia de TIC establece los mecanismos para la prevención, identificación, análisis de los riesgos de seguridad de los sistemas.

  Actualmente se cuenta con procedimientos de autorización y autentificación para el control de acceso a las aplicaciones tanto cliente/servidor y web. Asimismo, los temas de antivirus y actualización automática de software son administrados en forma centralizada.

Aún no se han definido criterios y/o especificaciones claras de seguridad para algunas de las aplicaciones, sobre todo para las aplicaciones web que son las que más se encuentran en riesgo. No se cuenta con un reporte automatizado de los incidentes de seguridad, revisiones y solución de problemas.

4.5 CUADROS DE EVALUACIÓN.

Los siguientes cuadros representan la evaluación al área de TIC.

RUBRO	Planificación y Organización PO 3 Determinar la Dirección Tecnológica			
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
1	La administración de la función de servicios de información comprende y utiliza el plan de infraestructura tecnológica.	3	2	1.3.1
2	Se ha realizado cambios al plan de infraestructura tecnológica para identificar los costos y riesgos inherentes, y que dichos cambios reflejen las modificaciones a los planes a largo y corto plazo de tecnología de información.	3	2	1.3.1, 1.3.4

Análisis de proceso

RUBRO	Planificación y Organización PO 3 Determinar la Dirección Tecnológica		
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
3	La administración de la función de servicios de información comprende el proceso de monitoreo y evaluación de nuevas tecnologías, y que incorpora tecnologías apropiadas a la infraestructura de servicios de información actual.	3	1	1.3.4
4	La administración de la función de servicios de información comprende el proceso de evaluar sistemáticamente el plan de tecnología en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).	4	2	1.3.3
5	La existencia de un ambiente físico de la función de servicios de información adecuado para alojar el hardware / software actualmente instalado, así como nuevo hardware / software a ser añadido según el plan de adquisiciones actual aprobado.	4	2	1.3.4
6	El plan de adquisición de hardware y software cumple con los planes a largo y corto plazo de tecnología de información, reflejando las necesidades identificadas en el plan de infraestructura tecnológica.	4	2	1.3.4, 1.3.5
7	El plan de infraestructura tecnológica dirige la utilización de tecnología actual y futura.	3	2	1.3.4
8	Se debe cumplir con los estándares de tecnología y que éstos sean agregados e incorporados como parte del proceso de desarrollo.	3	2	1.3.5
9	El acceso permitido debe ser consistente con los niveles de seguridad definidos en las políticas y procedimientos de la función de servicios de información, y que se haya obtenido la autorización apropiada para el acceso.	3	2	1.3.1

PROMEDIO	**3.3**	**1.8**

Análisis de proceso

RUBRO	Entrega de Servicios y Soporte DS 4 Aseguramiento de Servicio Continuo			
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
1	Existen planes de recuperación de desastre/contingencia, que éste es actual y que es comprendido por todas las partes afectadas	**4**	**1**	3.4.1
2	Se ha proporcionado a todas las partes involucradas un plan regular de entrenamiento de contingencia y recuperación en caso de desastre	**4**	**1**	3.4.3, 3.4.7
3	Se han seguido todas las políticas y procedimientos relacionados con el desarrollo del plan.	**4**	**1**	3.4.6, 3.4.8
4	El contenido del plan tiene como base el contenido descrito anteriormente, y que: • Los objetivos del plan de contingencia han sido alcanzados. • Se ha seleccionado a las personas apropiadas para llevar a cabo funciones de liderazgo. • El plan ha recibido las revisiones y aprobaciones apropiadas por parte de la administración. • El plan ha sido probado recientemente y que éste trabajó de acuerdo con lo esperado, o que cualquier deficiencia encontrada trajo como resultado la aplicación de correcciones al plan. • Existe un vínculo entre el plan de recuperación en caso de desastres y el plan de negocios de la organización. • Los procedimientos manuales alternativos son documentados y probados como parte de la prueba global.	**4**	**1**	3.4.1, 3.4.2, 3.4.6, 3.4.7, 3.4.8.
5	Se han dado el entrenamiento, la conciencia y el conocimiento de los usuarios y del personal de la función de servicios de información en cuanto a funciones, tareas y responsabilidades específicas dentro del plan	**3**	**1**	3.4.7, 3.4.8

Análisis de proceso

RUBRO	Entrega de Servicios y Soporte DS 4 Aseguramiento de Servicio Continuo			
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
6	Las relaciones y tiempos del proveedor contratado son consistentes con las expectativas y necesidades del usuario	**3**	**1**	3.4.1
7	El contenido del centro de cómputo de respaldo está actualizado y es suficiente con respecto a los procedimientos normales de rotación fuera del centro de cómputo	**3**	**2**	3.4.9, 3.4.11
	PROMEDIO	**3.5**	**1.1**	

Análisis de proceso

RUBRO	Entrega de Servicios y Soporte DS 5 Garantizar la Seguridad de Sistemas			
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
1	La función de servicios de información cumple con los estándares de seguridad relacionados con: • Autenticación y acceso. • Administración de clasificación de perfiles de usuario y seguridad de datos. • Reportes y revisión gerencial de la violación e incidentes de seguridad. • Estándares criptográficos administrativos clave. • Detección de virus, solución y comunicación. • Clasificación y propiedad de datos.	**2**	**3**	3.5.1, 3.5.2, 3.5.3, 3.5.4, .5.10, 3.5.19
2	Existen procedimientos para la adquisición, establecimiento y mantenimiento del acceso de usuarios al sistema.	**2**	**3**	3.5.4, 3.5.6
3	Existen procedimientos para el acceso externo o remoto de recursos del sistema, por ejemplo, "logon", "ID", "password" o contraseña y "dial back".	**2**	**3**	3.5.2, 3.5.4
4	Se lleva un inventario de los dispositivos del sistema para verificar su suficiencia	**2**	**2**	3.5.20
5	Las prácticas de administración de seguridad de la red son comunicadas, comprendidas e impuestas.	**3**	**2**	3.5.6
6	Existen procedimientos de "logon" reales para sistemas, usuarios y para el acceso de proveedores externos.	**2**	**2**	3.5.2, 3.5.9
7	Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes.	**4**	**2**	3.5.10, 3.5.11

Análisis de proceso

RUBRO	Entrega de Servicios y Soporte DS 5 Garantizar la Seguridad de Sistemas			
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
8	Los firewalls poseen por lo menos las siguientes propiedades: • Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles digitales, debe reforzarse fisicamente). • Sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local. • Los firewalls por sí mismos son inmunes a la penetración. • El tráfico se intercambia en firewalls a la capa de aplicación únicamente. • La arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación. • La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte. • La arquitectura del firewall debe estar configurada de acuerdo a la "filosofía de arte mínima". • La arquitectura del firewall debe desplegar sólida autentificación para la administración y sus componentes. • La arquitectura del firewall oculta la estructura de la red interna. • La arquitectura del firewall provee una auditoria de todas las comunicaciones hacia o a través del sistema del firewall y activará alarmas cuando se detecte alguna actividad sospechosa. • El host de la organización, que provee el soporte para las solicitudes de entrada al servicio de las redes públicas, permanece fuera del firewall. • La arquitectura del firewall se defiende de los ataques directos (ej., a través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico). • Todo código ejecutable se explora en busca de códigos malignos ej., virus, applets dañinos) antes de introducirse a la red interna.	**2**	**3**	3.5.20

Análisis de proceso

RUBRO	ENTREGA DE SERVICIOS Y SOPORTE DS 5 Garantizar la Seguridad de Sistemas			
Tarea N°.	**Descripción**	**Nivel de Riesgo**	**Nivel de Madurez**	**Objetivo de Control**
9	Los procedimientos para la protección contra software maligno incluyen:• Todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso.• Existe una política por escrito para bajar archivos (downloads), aceptación o uso de aplicaciones gratuitas y compartidas y esta política está vigente.• El software para aplicaciones altamente sensibles está protegido por MAC (Messsage Authentication Code - Código de Autentificación de Mensajes) o firma digital, y fallas de verificación para evitar el uso del software.• Los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos.• Existe una política y un procedimiento vigente para la verificación de disquetes externos al programa de compra normal de la organización.	**2**	**3**	3.5.19
	PROMEDIO	**2.3**	**2.5**	

Análisis de proceso

ANÁLISIS DE RIESGO DEL AREA INFORMATICA DE ENERO A DICIEMBRE DEL 2004			
Objetivo Control de Riesgo	**Código**	**Nivel de Riesgo**	**Nivel de Madurez**
Planificación y Organización			
Determinar la Dirección Tecnológica	PO-3	**3.3**	**1.8**
Definición de la Organización y de las Relaciones de TIC	PO-4		
Evaluar los Riesgos	PO-9		
Administrar los Proyectos	PO-10		
Administrar la Calidad	PO-11		
Definir un Plan Estratégico de TIC	PO-1		
Definir la Arquitectura de la Información	PO-2		
Determinar el Rumbo Tecnológico	PO-3		
Definir la Organización y las Relaciones de TIC	PO-4		
Administrar los Recursos Humanos	PO-7		
Asegurar el Cumplimiento de los Requerimientos Externos	PO-8		
Administrar la Inversión de TIC	PO-5		
TOTAL DOMINIO		**3.3**	**1.8**
Adquisición e Implementación			
Identificar las Soluciones	AI-1		
Adquirir y Dar Mantenimiento al Software de Aplicación	AI-2		
Adquisición y Mantenimiento de Arquitectura de Tecnología	AI-3		
Desarrollar y Mantener Procedimientos de TIC	AI-4		
Instalar y Acreditar los Sistemas	AI-5		
Manejar los Cambios	AI-6		
Adquirir y Dar Mantenimiento a la Arquitectura Tecnológica	AI-3		
TOTAL DOMINIO		**0.0**	**0.0**
Entrega y Soporte			
Identificar y Atribuir los Costos	DS-6		
Educar y Capacitar a los Usuarios	DS-7		
Manejar los Problemas e Incidentes	DS-10		
Asegurar el Servicio Continuo	DS-4		
Definir los Niveles de Servicio	DS-1		
Ayudar y Aconsejar a los Clientes de TIC	DS-8		
Manejar la Configuración	DS-9		
Manejar los Servicios de Terceros	DS-2		
Administrar el Desempeño y la Capacidad	DS-3		
Aseguramiento de Servicio Continuo	DS-4	3.5	1.1
Asegurar la Seguridad de los Sistemas	DS-5	2.3	2.5
Manejar las Instalaciones	DS-12		
Manejar los Datos	DS-11		
Manejar las Operaciones	DS-13		
TOTAL DOMINIO		**2.9**	**1.8**
Riesgo determinado para el área tecnológica		**3.1**	**1.8**

4.6 RESUMEN EJECUTIVO.

Aspectos favorables	Aspectos mejorables
Existe una política básica para la evaluación, creación y la actualización del plan de infraestructura tecnológico.	El proceso de planificación de la dirección tecnológica se puede mejorar utilizando políticas bajo una metodología de referencia estándar.
La existencia de procedimientos de recuperación de desastres / contingencias para la función de servicios de información se presenta como un proceso adquirido en la practica.	Los procedimientos de recuperación de desastres / contingencias para la función de servicios de información se podrían fortalecer utilizando una política acorde con los lineamientos de la entidad y que este estandarizado.
La política de backup de la base de datos de los servidores que se realiza a diario	Dentro de la política diaria de backup de la base de datos se podría adicionar software que permita la correcta copia a la cinta (libre de información corrupta).
Se cuenta con un manejo centralizado de los accesos a la red y correo electrónico, actualizaciones de software y control de versiones.	Es necesario poner énfasis a la seguridad de los sistemas ya sea control de accesos y configuración de servidores, de la interacción con usuarios externos así como también el monitoreo del trafico de la información a través de la red, creando políticas que permitan una administración alineada a la entidad.

4.7 DETALLE DE OBSERVACIONES.

- **Observación 1.**

La gerencia de TIC en la parte que corresponde a planificación y organización, específicamente en los procesos que corresponden a determinar la dirección tecnológica poseen niveles de administración medio-bajo, encontrándose los siguientes problemas:

- No se encuentra establecida formalmente una política clara del planeamiento de la infraestructura tecnológica.
- La contingencia de infraestructura tecnológica presenta debilidades ante la falta de procedimientos de planificación.
- No existe un plan de infraestructura tecnológica que se compare contra los planes de largo y corto plazo de tecnología de información.
- Falta de un proceso de evaluación de tecnología de vanguardia, que incorpore tecnologías apropiadas a la infraestructura de servicios de información actual.
- No se encuentran establecidos los estándares de tecnología para los componentes informáticos en el ámbito de software para la red.

Riesgo.

- La entidad puede llegar a una situación de riesgo alto, ya que no podrá actuar adecuadamente ante la inexistencia de un plan estratégico de la dirección tecnológica.
- La falta de políticas y procedimientos para evaluar y monitorear la tecnología traen consigo una mala administración de TIC.

- La mala planificación de largo o corto plazo trae la insatisfacción de los usuarios en los plazos establecidos inicialmente.
- Proyectos no concluidos que son de vital importancia para toda la entidad.

Recomendación.

Se recomienda que la gerencia de TIC, inicie un plan de evaluación de su política de planificación con relación a la dirección de tecnología, utilizando un marco de referencia.

La entidad debe tener una perspectiva diferente respecto de la tecnología de información dentro de la institución, que beneficios positivos como negativos pueden traer sino se planifica dentro de un marco referencial para lo cual se puede utilizar diferentes estándares que se presentan en el mercado.

Las políticas dadas deben ser de conocimiento tanto de los gerentes como de todo el personal de la institución de acuerdo a la actividad con que se realizan (ya sea anual o semestral).

- **Observación 2.**

La administración y mantenimiento de la red a nivel de arquitectura física, presenta ciertas falencias de las cuales podemos citar:

- No existe una bitácora documentada de los sucesos presentados ante la caída de la red y de las áreas que son más propensas a presentar fallas.
- No existe procedimientos documentados de plan de contingencia ante la falla de la red.

- No existe una priorización de las aplicaciones con respecto a los tiempos de recuperación y regreso.
- No existe una filosofía y un marco referencial consistente en relación con el desarrollo de un plan de recuperación y regreso.

Riesgo.

Los sistemas desarrollados por la gerencia de TIC se ven en ocasiones frente al riesgo de que los usuarios muestren su insatisfacción respecto al desempeño y performance de los sistemas ya que esto es inaccesible ante una falla en la red lo cual se ve reflejado en el retrazo de sus actividades.

Recomendaciones.

Se recomienda a la gerencia de TIC, capacitar al personal de TIC y establecer políticas, procedimientos y funciones dirigidos a mejorar el plan administración y mantenimiento de la red entre los cuales están:

- Administración y monitoreo permanente de la red.
- Llevar un reporte documentado de los sucesos como el tráfico de información y fallas en la red.
- Revisión periódica de los equipos de red como hubs, switchs y las conexiones de cableado estructurado.
- Procedimientos de emergencia para garantizar la continuidad del funcionamiento de la red.

- **Observación 3.**

Si bien existe un control sobre los accesos a los diferentes ambientes de la gerencia de TIC y la administración de las claves para el personal de la institución, no se presenta el mismo esquema para la prevención, detección, control y monitoreo del software dañino. Se han detectado los siguientes problemas:

- El personal de la entidad no está bien informado sobre los virus de computadora.
- No se tiene un concepto claro sobre los programas maliciosos (los que se descargan a través de internet).
- No tienen un cuidado sobre el control de la verificación de los diskettes que ingresan a la institución.
- No hay un control para contrarrestar las instalaciones de software no autorizado.
- El personal de la entidad no tiene presente que las claves que se le entrega para el acceso a los diferentes módulos de los sistemas son responsabilidad del mismo.

Riesgo.

En caso de ingreso de un programa malicioso que no sea detectado por el antivirus es posible que quede inoperativo el equipo así como también la posible pérdida de la información del equipo. Esto trae como consecuencia de que el usuario se quede sin equipo por un periodo de aproximadamente de un día y medio, ya que la institución no cuenta con equipos suficientes para un reemplazo inmediato.

La divulgación de las claves para el acceso de los módulos por parte del personal de la entidad trae como riesgo la manipulación de los datos de la base de dato por usuarios no autorizados.

Recomendaciones.

Establecer políticas y directivas de seguridad dirigidas a todo el personal de la institución a fin de tomar acciones correctivas por parte del personal de soporte de la gerencia de TIC y concientizar sobre la importancia de prevenir riesgos de virus y código malicioso como también que las claves que se les entrega es de tipo personal.

- **Observación 4.**

Si bien existe una política de los backup de la información de la base de datos, del servidor de correo, del servidor web y otros, se pudo verificar las siguientes falencias:

- No existe un proceso de verificación de los backup, es decir si la información grabada o guardada en la cinta no esta corrupta.
- Las cintas de backup son guardadas en los escritorios de los administradores de base de datos, servidor de correo y servidor web.
- No se ha documentado los procesos de backup de los diferentes servidores para que lo realice otro personal en caso que el administrador del servidor falte por algún motivo.

Riesgo.

En caso de alguna catástrofe como incendio terremoto u otro tipo, podría existir el riesgo de perderse toda la información ya que los backups están guardados en la misma oficina de informática.

La no verificación de la información del backup en las cintas trae el riesgo de que la información este mal grabada.

Recomendaciones.

Establecer políticas y directivas de backup que incluyan revisión de la información en las cintas de backup, manual de procedimiento de backup así como también tener un local diferente donde se pueda guardar una copia de backup para su mayor seguridad.

RECOMENDACIONES Y CONCLUSIONES

1. Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la tecnología de información (TI), esto se debe a la creciente dependencia, el incremento de vulnerabilidad, la escala y el costo de las inversiones actuales y futuras así como el potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio.

2. La información que puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación es un activo que, como otros activos importantes del negocio tiene un valor para la organización y requiere por lo tanto una política de control adecuada.

3. La auditoría de las tecnologías de la información se presenta como un examen objetivo, crítico, sistemático, eminentemente posterior y selectivo de las políticas, normas prácticas, procedimientos y procesos con el fin de emitir una opinión respecto a la eficiencia en la utilización de los recursos informáticos; la confiabilidad, consistencia, integridad y oportunidad de la información y de la efectividad de los controles en los sistemas de información computarizados.

4. Ante la necesidad de una política clara y una buena práctica de tecnología de información que proporcione a la organización, a la auditoría y a los usuarios se

presenta COBIT (objetivos de control para tecnología de información y tecnologías relacionadas). COBIT se desarrolla como un estándar generalmente aplicable y aceptado para las buenas practicas de seguridad y control de tecnología de información.

5. Al aplicar COBIT en el ámbito de auditoría provee las directrices de auditoría, el cual es una estructura sencilla para auditar y evaluar controles.

6. En la auditoría de la seguridad de redes para la organización, se utilizan los procesos de TIC: determinación de la dirección tecnológica, garantizar la seguridad de los sistemas y aseguramiento de servicio continúo, así como sus objetivos de control detallados; los cuales no necesariamente son los mismos para la evaluación de otras organizaciones, ya que estos dependen de muchos factores (función, misión, visión, organización, etc).

7. Finalmente diremos, para el desarrollo de la auditaría a la tecnología de información se pueden usar diferentes herramientas, pero COBIT se presenta como un marco referencial orientado al negocio, manteniendo una independencia con respecto a las plataformas técnicas de TIC y utilizando los diferentes estándares existentes en el campo de control de los sistemas de información.

ANEXO A:

RELACIONES DE OBJETIVOS DE CONTROL:

DOMINIOS, PROCESOS Y OBJETIVOS DE CONTROL

Planeación y organización.

1.0 Definición de un plan estratégico de tecnología de información.

1.1 Tecnología de información como parte del plan de la organización a corto y largo plazo.

1.2 Plan a largo plazo de tecnología de información.

1.3 Plan a largo plazo de tecnología de información – enfoque y escritura.

1.4 Cambios al plan a largo plazo de tecnología de información.

1.5 Planeación a corto plazo para la función de servicios de información.

1.6 Comunicación de los planes de TI.

1.7 Evaluación y monitoreo de los planes de TI.

1.8 Valoración de los sistemas existentes.

2.0 Definición de la arquitectura de información.

2.1 Modelo de la arquitectura de información.

2.2 Diccionario de datos y reglas de sintaxis de datos corporativos.

2.3 Esquema de clasificación de datos.

2.4 Niveles de seguridad.

3.0 Determinación de la organización y de las relaciones de TI.

3.1 Planeación de la estructura tecnológica.

3.2 Monitoreo de tendencias y regulaciones futuras.

3.3 Adquisición de hardware y software.

3.4 Estándares de tecnología.

3.5 Contingencias en la infraestructura tecnológica.

4.0 Definición de la organización y de las relaciones de TI.

4.1 Planeación de TI comité de plantación / dirección de la función de los servicios de información.

4.2 Ubicación de los servicios de información en la organización.

4.3 Revisión de logros organizacional.

4.4 Funciones y responsabilidades.

4.5 Responsabilidad del aseguramiento de calidad.

4.6 Responsabilidad por seguridad lógica y física.

4.7 Propiedad y custodia.

4.8 Propiedad de datos y sistemas.

4.9 Supervisión.

4.10 Segregación de funciones.

4.11 Asignación de personal para tecnología de información.

4.12 Descripción de puestos para el personal de la función de TI.

4.13 Personal clave de TI.

4.14 Procedimientos y política para el personal contratado.

4.15 Relaciones.

5.0 Manejo de la inversión en tecnología de información.

5.1 Presupuesto operativo anual para la función de servicio de información.

5.2 Monitoreo de costo – beneficio.

5.3 Justificación de costo – beneficio.

6.0 Comunicación de los objetivos y aspiraciones de la gerencia.

6.1 Ambiente positivo de control de la información.

6.2 Responsabilidad de la gerencia en cuanto a políticas.

6.3 Comunicación de las políticas de la organización.

6.4 Recursos para la implementación de políticas.

6.5 Mantenimiento de políticas.

6.6 Cumplimiento de políticas, procedimientos y estándares.

6.7 Compromiso con la calidad.

6.8 Política sobre el marco referencial para la seguridad y el control interno.

6.9 Derechos de propiedad intelectual.

6.10 Políticas específicas.

6.11 Comunicación de conciencia de seguridad en TI.

7.0 Administración de recursos humanos.

7.1 Reclutamiento y promoción de personal.

7.2 Clasificación de personal.

7.3 Roles y responsabilidades.

7.4 Entrenamiento del personal.

7.5 Entrenamiento cruzado o respaldado de personal.

7.6 Procedimientos para la acreditación del personal.

7.7 Evaluación de desempeño de los empleados.

7.8 Cambios de puesto y terminación de contrato de trabajo.

8.0 Aseguramiento del cumplimiento con requerimientos externos.

8.1 Revisión de requerimientos externos.

8.2 Prácticas y procedimientos para el cumplimiento de requerimientos externos.

8.3 Cumplimiento de los estándares de seguridad y ergonomía.

8.4 Privacidad, propiedad intelectual y flujo de datos.

8.5 Comercio electrónico.

8.6 Cumplimiento con contratos de seguros.

9.0 Análisis de riesgos.

9.1 Análisis de riesgo del negocio.

9.2 Enfoque de análisis de riesgos.

9.3 Identificación de riesgos.

9.4 Medición de riesgos.

9.5 Plan de acción para mitigar los riesgos.

9.6 Aceptación de riesgos.

9.7 Selección de protección.

9.8 Compromiso de análisis de riesgos.

10.0 Administración de proyectos.

10.1 Marco referencial para la administración de proyectos.

10.2 Participación del departamento usuario en la iniciación de proyectos.

10.3 Miembros y responsabilidades del equipo del proyecto.

10.4 Definición del proyecto.

10.5 Aprobación del proyecto.

10.6 Aprobación de las fases del proyecto.

10.7 Plan maestro del proyecto.

10.8 Plan aseguramiento de calidad de sistemas.

10.9 Planeación de métodos de aseguramiento.

10.10Administración formal de riesgo de proyectos.

10.11 Plan de prueba.

10.12 Plan de entrenamiento.

10.13 Plan de revisión post implementación.

11.0 Administración de calidad.

11.1 Plan general de calidad.

11.2 Enfoque de aseguramiento de calidad.

11.3 Planeación de aseguramiento de calidad.

11.4 Revisión de aseguramiento de calidad sobre el cumplimiento de estándares y procedimientos de TI.

11.5 Metodología de ciclo de vida de desarrollo de sistemas.

11.6 Metodología de ciclo de vida de desarrollo de sistemas para cambios mayores a la tecnología actual.

11.7 Actualización de la metodología del ciclo de vida de desarrollo de sistemas.

11.8 Coordinación y comunicación.

11.9 Marco referencial para la adquisición y mantenimiento de la infraestructura de tecnología.

11.10 Relaciones con terceras partes en su rol de implementadores.

11.11 Estándares para la documentación de programas.

11.12 Estándares para pruebas de programas.

11.13 Estándares para pruebas de sistemas.

11.14 Pruebas piloto en paralelo.

11.15 Documentación de las pruebas del sistema.

11.16 Evaluación del aseguramiento de la calidad sobre el cumplimiento de estándares de desarrollo.

11.17 Revisión del aseguramiento de calidad sobre el logro de los objetivos de la función de servicios de información.

11.18 Métricas de calidad.

11.19 Reportes de revisiones de aseguramiento de la calidad.

Adquisición e implementación.

1.0 Identificación de soluciones.

1.1 Definición de requerimientos de información.

1.2 Formulación de acciones alternativas.

1.3 Formulación.

1.4 Requerimientos de servicios de terceros.

1.5 Estudio de factibilidad tecnológica.

1.6 Estudio de factibilidad económica.

1.7 Arquitectura de información.

1.8 Reporte de análisis de riesgos.

1.9 Controles de seguridad costo-efectivo.

1.10 Diseño de pistas de auditoria.

1.11 Ergonomía.

1.12 Selección de software del sistema.

1.13 Control de abastecimiento.

1.14 Adquisición de productos de software.

1.15 Mantenimiento de software de terceras partes.

1.16 Contratos para la programación de aplicaciones.

1.17 Aceptación de instalaciones.

1.18 Aceptación de tecnología.

2.0 Adquisición y mantenimiento de software de aplicación.

2.1 Métodos de diseño.

2.2 Cambios significativos a sistemas actuales.

2.3 Aprobación de diseño.

2.4 Definición y documentación de requerimientos y archivos.

2.5 Especificaciones de programas.

2.6 Diseños para la recopilación de datos fuente.

2.7 Definición y documentación de requerimiento de entrada de datos.

2.8 Definición de interfaces.

2.9 Interfaces usuario-máquina.

2.10 Definición y documentación de requerimientos de procesamiento.

2.11 Definición y documentación de requerimientos de salida de datos.

2.12 Controlabilidad.

2.13 Disponibilidad como factor clave de diseño.

2.14 Consideración de integridad TI en programas de software de aplicaciones.

2.15 Pruebas de software de aplicación.

2.16 Materiales de consulta y soporte para usuario.

2.17 Reevaluación del diseño del sistema.

3.0 Adquisición y mantenimiento de la arquitectura de tecnología.

3.1 Evaluación de nuevo hardware y software.

3.2 Mantenimiento preventivo para hardware.

3.3 Seguridad del software del sistema.

3.4 Instalación del software del sistema.

3.5 Mantenimiento del software del sistema.

3.6 Controles para cambios del software del sistema.

3.7 Uso y monitoreo de utilidades/utilitarios del sistema.

4.0 Procedimiento de desarrollo y mantenimiento de TI.

4.1 Requerimientos operacionales y niveles de servicio.

4.2 Manual de procedimientos para usuarios.

4.3 Manual de operaciones.

4.4 Material de entrenamiento.

5.0 Instalación y acreditación de sistemas.

5.1 Entrenamiento.

5.2 Medición del desempeño del software de aplicación.

5.3 Plan de implementación.

5.4 Conversión del sistema.

5.5 Conversión de datos.

5.6 Planes y estrategias de pruebas.

5.7 Pruebas a cambios.

5.8 Criterios y desempeño de pruebas e paralelos/piloto.

5.9 Pruebas de aceptación final.

5.10 Pruebas de acreditación de la seguridad.

5.11 Prueba operacional.

5.12 Promoción a producción.

5.13 Evaluación de la satisfacción de los requerimientos del usuario.

5.14 Revisión general post-implementación.

6.0 Administración de cambios.

6.1 Inicio y control de solicitudes de cambio.

6.2 Análisis de impacto.

6.3 Control de cambio.

6.4 Cambios de emergencia.

6.5 Documentación y procedimientos.

6.6 Mantenimiento autorizado.

6.7 Política de liberación de software.

6.8 Distribución de software.

Entrega de servicios y soporte.

1.0 Definición de niveles de servicio.

1.1 Marco de referencia para acuerdos de nivel de servicio.

1.2 Aspectos sobre los acuerdos de nivel de servicio.

1.3 Procedimiento de desempeño.

1.4 Monitorio y soporte.

1.5 Revisión de contratos y acuerdos de nivel de servicio.

1.6 Elementos sujetos a cargo.

1.7 Programa de mejoramiento del servicio.

2.0 Administración de servicios presentados por terceros.

2.1 Interfaces con proveedores.

2.2 Relaciones con los diseños.

2.3 Contratos con terceros.

2.4 Calificaciones de terceros.

2.5 Contratos con outsourcing.

2.6 Continuidad del servicio.

2.7 Relaciones de seguridad.

2.8 Monitoreo.

3.0 Administración de desempeño y capacidad.

3.1 Requerimientos de disponibilidad y desempeño.

3.2 Plan de disponibilidad.

3.3 Monitoreo y reporte.

3.4 Herramientas de modelado.

3.5 Administración de desempeño proactivo.

3.6 Pronostico de carga de trabajo.

3.7 Administración de capacidad de recursos.

3.8 Disponibilidad de recursos.

3.9 Calendarización/programación de recursos.

4.0 Aseguramiento de servicio continúo.

4.1 Marco de referencia de continuidad de tecnología de información.

4.2 Estrategia y filosofía del plan de continuidad tecnología de información.

4.3 Contenido del plan de continuidad de tecnología de información.

4.4 Minimización de requerimientos de continuidad de tecnología de información.

4.5 Mantenimiento del plan de continuidad de tecnología de información.

4.6 Pruebas del plan de continuidad de tecnología de información.

4.7 Entrenamiento sobre el plan de continuidad de tecnología de información.

4.8 Distribución del plan de continuidad de tecnología de información.

4.9 Procedimientos de respaldo de procesamiento para departamentos usuarios.

4.10 Recursos críticos de tecnología de información.

4.11 Centro de cómputo y hardware de respaldo.

4.12 Almacenamiento de copias de respaldo fuera del sitio.

4.13 Procedimientos de refinamiento del plan de continuidad de TI.

5.0 Garantizar la seguridad de sistemas.

5.1 Administrar medidas de seguridad.

5.2 Identificación, autenticación y acceso.

5.3 Seguridad de acceso a datos en línea.

5.4 Administración de cuentas de usuario.

5.5 Revisión gerencial de cuentas de usuario.

5.6 Control de usuarios sobre cuentas de usuarios.

5.7 Vigilancia de seguridad.

5.8 Clasificación de datos.

5.9 Administración centralizada de identificación y derechos de acceso.

5.10 Reportes de violación de actividades de seguridad.

5.11 Manejo de incidentes.

5.12 Re-acreditación.

5.13 Confianza en las contrapartes.

5.14 Autorización de transacciones.

5.15 No rechazo.

5.16 Sendero seguro.

5.17 Protección de las funciones de seguridad.

5.18 Administración de las llaves criptográficas.

5.19 Prevención, detención y corrección de software "malicioso".

5.20 Arquitecturas de firewall y conexión a redes públicas.

5.21 Protección de valores electrónicos.

6.0 Identificación y asignación de costos.

6.1 Elementos sujetos a cargo.

6.2 Procedimientos de costeo.

6.3 Procedimientos de cargos de facturación a usuarios.

7.0 Educación y entrenamiento de usuarios.

7.1 Identificación de necesidades de entrenamiento.

7.2 Organización de entrenamiento.

7.3 Entrenamiento sobre principios y conciencias de seguridad.

8.0 Apoyo y asistencia a los clientes de tecnología de información.

8.1 Help desk.

8.2 Registro de consultas del cliente.

8.3 Escalamiento de consultas del cliente.

8.4 Monitoreo de atención a clientes.

8.5 Análisis y reporte de tendencias.

9.0 Administración de la configuración.

9.1 Registro de la configuración.

9.2 Base de la configuración.

9.3 Registro de status.

9.4 Control de la configuración.

9.5 Software no autorizado.

9.6 Almacenamiento de software.

9.7 Procedimientos para la administración de la configuración.

9.8 Contabilidad y registro del software.

10.0 Administración de problemas e incidentes.

10.1 Sistema de administración de problemas.

10.2 Escalamiento de problemas.

10.3 Seguimiento de problemas y pista de auditoria.

10.4 Autorizaciones de acceso temporal y de emergencia.

10.5 Prioridades en proceso de emergencia.

11.0 Administración de datos.

11.1 Procedimientos de preparación de datos.

11.2 Procedimientos de autorización de documentos fuente.

11.3 Recopilación de datos de documentos fuente.

11.4 Manejo de errores de documentos fuente.

11.5 Retención de documentos fuente.

11.6 Procedimientos para la autorización de entrada de datos.

11.7 Chequeos de exactitud, suficiencia y autorización.

11.8 Manejo de errores en la entrada de datos.

11.9 Integridad de procesamiento de datos.

11.10 Validación y edición de procesamiento de datos.

11.11 Manejo de errores en el procesamiento de datos.

11.12 Manejo y retención de datos de salida.

11.13 Distribución de datos de salida.

11.14 Balanceo y conciliación de datos de salida

11.15 Revisión de salidas de datos y manejo de errores.

11.16 Provisiones de seguridad para reportes de salida.

11.17 Protección de información sensitiva durante transmisión y transporte.

11.18 Protección de información sensitiva a ser desechada.

11.19 Administración de almacenamiento.

11.20 Periodos de retención en términos de almacenamiento.

11.21 Sistema de administración de la librería de medios.

11.22 Responsabilidades de la administración de la librería de medios.

11.23 Respaldo y restauración.

11.24 Funciones de respaldo.

11.25 Almacenamiento de respaldo.

11.26 Archivo.

11.27 Protección de mensajes sensitivos.

11.28 Autenticación e integridad.

11.29 Integridad de transacciones electrónicas.

11.30 Integridad continúa de datos almacenados.

12.0 Administración de instalaciones.

12.1 Seguridad física.

12.2 Discreción (bajo perfil) de las instalaciones de tecnología de información.

12.3 Escolta de visitantes.

12.4 Salud y seguridad del personal.

12.5 Protección contra factores ambientales.

12.6 Suministro ininterrumpido de energía.

13.0 Administración de operaciones.

13.1 Manual de instrucciones y procedimientos de operaciones de procesamiento.

13.2 Documentación del proceso de inicio y de otras operaciones.

13.3 Calendarizacion /programación de trabajos.

13.4 Ejecución de los trabajos estándar programados.

13.5 Continuidad de procesamiento.

13.6 Bitácoras de operación.

13.7 Protección de formas especiales y dispositivos de salida.

13.8 Operaciones remotas.

Monitoreo.

1.0 Monitoreo del proceso.

1.1 Recolección de datos de monitoreo.

1.2 Análisis del desempeño.

1.3 Evaluación de la satisfacción de clientes.

1.4 Reportes gerenciales.

2.0 Evaluar lo adecuado del control interno.

2.1 Monitoreo de control interno.

2.2 Operación oportuna del control interno.

2.3 Reporte sobre el nivel del control interno.

2.4 Seguridad en las operaciones y aseguramiento del control interno.

3.0 Obtención de aseguramiento independiente.

3.1 Certificación, acreditación, independencia de control interno y seguridad de los servicios de TI.

3.2 Certificación, acreditación, independencia de control interno y seguridad de proveedores externos de servicios.

3.3 Evaluación independiente de efectividad de los servicios de TI.

3.4 Evaluación independiente de efectividad de proveedores externos de servicios.

3.5 Aseguramiento independiente del cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales.

3.6 Aseguramiento independiente del cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales con proveedores externos de servicios.

3.7 Competencia de la función de aseguramiento independiente.

3.8 Participación proactiva de auditoría.

4.0 Proveer auditoría independiente.

4.1 Estatutos de auditoría.

4.2 Independencia.

4.3 Ética y estándares profesionales.

4.4 Competencia.

4.5 Planeación.

4.6 Desempeño del trabajo de auditoría.

4.7 Reporte.

4.8 Actividades de seguimiento.

ANEXO B: GLOSARIO.

1. **TI:** Tecnología de información.
2. **TIC:** Tecnologías de información y comunicación.
3. **COBIT:** Objetivos de control para tecnología de información y tecnologías relacionadas.
4. **CMM:** Modelo de madurez de capacidad.
5. **TAAC`S:** Técnica de auditoría asistida por computadora.
6. **ISO:** Organización internacional de estándares.
7. **OSI:** Interconexión de sistemas abiertos.
8. **NAGU:** Normas de auditoría gubernamental.
9. **NAGA:** Normas de auditoría generalmente aceptadas.
10. **MAGU:** Manual de auditoría gubernamental.
11. **COSO:** Comité de organizaciones patrocinantes de la comisión treadway.
12. **ITSEC**: Criterios de evaluación de la seguridad de la tecnología de Información.
13. **TCSEC:** Criterios de evaluación de la seguridad de los sistemas de Computación.
14. **ISACA:** Asociación de auditoría y control de sistemas de información.

BIBLIOGRAFÍA

1 Manual de Auditoría Gubernamental (MAGU).

2 Norma de Auditoría Gubernamental (NAGU).

3 Information Systems audit. And Control Association (ISACA).
www.isaca.org

4 International Organization of Supreme Audit Institutions (INTOSAI)
www.intosai.org

5 Objetivo de Control para Tecnología de Información y Tecnologías Relacionadas (COBIT).

6 Separatas de Auditoría de Sistemas.