UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TÍTULO DE LA TESIS:

Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa

Previa la obtención del Grado Académico de Magíster en Telecomunicaciones

ELABORADO POR:

ING. CESAR ANDRES SANDOVAL VARGAS

DIRIGIDO POR:

MSc. LUIS CÓRDOVA RIVADENEIRA

Guayaquil, Abril de 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Ing. Cesar Andrés Sandoval Vargas como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, Abril de 2014

DIRECTOR DE TESIS

_____

Ing. Luis Córdova Rivadeneira, MSc.

REVISORES:

_____

Ing. Orlando Philco Asqui, MSc.

_____

Ing. Edwin Palacios Meléndez, MSc.

DIRECTOR DEL PROGRAMA

_____

Ing. Manuel Romero Paz, MSc.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, CESAR ANDRES SANDOVAL VARGAS

DECLARO QUE:

La tesis “Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa”, previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, Abril de 2014

EL AUTOR

_____

ING. CESAR ANDRES SANDOVAL VARGAS

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

YO, ING. CESAR ANDRES SANDOVAL VARGAS

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución de la Tesis de Maestría titulada: "Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, Abril de 2014

EL AUTOR

_____

ING. CESAR ANDRES SANDOVAL VARGAS

DEDICATORIA

A Dios, que me regala los dones de la sabiduría y entendimiento que me permiten alcanzar otro logro en mi vida profesional, por los triunfos y momentos difíciles que me han enseñado a valorarlo cada día más.

A mis padres por su inmenso amor y apoyo constante quienes me han acompañado a llegar a estas instancias, me han convertido en una persona de bien, inculcándome valores, principios, carácter, empeño, perseverancia y deseos de superación.

AGRADECIMIENTO

Me complace exteriorizar mi sincero agradecimiento a la Universidad Católica de Santiago de Guayaquil y en ella a sus docentes quienes con su profesionalismo y ética imparten sus conocimientos que me servirán para ser útil en el desarrollo de la sociedad.

A mis padres, que creyeron en mí, dándome ejemplos de superación y entrega, gracias por haber fomentado el deseo de superación y el anhelo de triunfo en mi vida.

A cada una de las personas que de una u otra manera han sido claves en mi vida personal y profesional, me brindaron su amistad y su apoyo para la culminación de este objetivo.

A todos gracias y que Dios los bendiga.

Resumen

Durante el proceso de esta investigación se aborda el tema relacionado con la seguridad informática, haciendo énfasis en el análisis de la norma ISO/IEC (*International Organization for Standardization*/ *International Electrotechnical Commission*)27001 y su puesta en práctica en una empresa o institución. El trabajo se encuentra dividido en tres capítulos. En el primero se efectúa un estudio de la seguridad informática. Durante el segundo capítulo se lleva a cabo una caracterización general de las normas ISO/IEC 27000, profundizando en la ISO/IEC 27001 que abarca lo concerniente a las técnicas de seguridad, los Sistemas de Gestión de Seguridad de la Información y los requerimientos a tener en cuenta. Por último, durante el tercer capítulo se implementa el Plan de Seguridad Informática de la empresa, con los análisis de riesgos, basado en el estándar mencionado.Este trabajo se desarrolla teniendo en cuenta la necesidad de que la seguridad en la empresa cumplacabalmentecon los parámetros internacionales establecidos,contribuyendo así al mejoramiento de la misma y al propósito de obtener su certificación.

Palabras claves

Normas de Seguridad Informática, Plan de Seguridad Informática, Sistema de Gestión de Seguridad de la Información (SGSI).

Abstract

This research deals with the subject of computer security, with emphasis on the analysis of ISO / IEC (International Organization for Standardization / International Electrotechnical Commission) 27001 and its implementation in an organization. The report is divided into three chapters. The first one makes a study of computer security. In the second chapter conducts a general description of the ISO / IEC 27000, delving into the ISO / IEC 27001 covering techniques regarding security, Systems Management and Information Security requirements have into account. Finally, in the third chapter implements the Information Security Plan of the entity, risk analysis, based on the aforementioned standard. This work is developed taking into account the need for security in the entity complies fully with international standards established, contributing to the improvement of the same and the purpose of obtaining certification.

Keywords

Norms of Computer Security, Plan of Computer Security, System of Administration of Security of the Information (SGSI).

Índice

INDICE FIGURAS

INDICE DE TABLAS

Introducción

En los inicios del presente siglo, llamado de la información por algunos, la dependencia de las TIC (Tecnologías de la Información y las Comunicaciones) para el desarrollo de las actividades de cualquier organización, sea económica, política, social u otras es tal que el no poder contar con estas en un momento determinado pudiera provocar una verdadera catástrofe, que en función de su magnitud, acarrearía inclusive la desaparición de la propia organización. Debido a la existencia de este peligro, garantizar la seguridad de la información se ha convertido en un aspecto estratégico vital de toda política que se ponga en práctica. (ECURED, s.f.) Indica que llevar a cabo la prevención, evaluación, aviso, investigación y respuesta a las acciones, tanto internas como externas, que afecten el normal funcionamiento de dichastecnologías resulta primordial para lograr el éxito en cualquier empeño.

Además, no sólo el volumen si no la importancia de esta información, para el desarrollo en general, no tiene parangón con la que tuvo en cualquier otra época que consideremos. De hecho, en la actualidad se estima que la información es un bien más de los activos y, en muchos casos, prevalece sobre los restantes.

Aparejado a ello, las redes de computadoras se han transformado con este vertiginoso ascenso de las tecnologías informáticas en uno de los pilares fundamentales de las comunicaciones, permitiendomoverse diariamente innumerables cantidades de información desde un extremo del mundo al otro, haciendo que la confidencialidad, integridad y disponibilidad de la red de conexión sea un punto esencial para obtenerun determinado propósito.

Cada vez son más los intrusos que pretenden penetrar los niveles de seguridad de las redes, creando el llamado hueco de seguridad que contribuye al desvío del flujo de información de un punto de transmisión a su debido destino. Estas condiciones antes mencionadas favorecen a que los esfuerzos por lograr una menor vulnerabilidad sea bastante difícil y en ocasiones engorrosa. A estose debe añadir que generalmente no se cuenta, o simplemente no se emplean cabalmente las normas o estándares que facilitan o

viabilizan las estrategias a tomar en pos de poder tener una mejor seguridad en cualquier empresay que la misma sea certificada internacionalmente.

Es imprescindible encontrar la manera con la cual se pueda brindar una adecuada solución a los inconvenientes señalados, específicamente en una empresa,siendo esta la misión esencial del presente trabajo, además de continuar aportando de una manera u otra a que la red informática, pueda tener la protección necesaria, y le continúe permitiendo comunicarse sin grandes repercusiones.

Problema

Insuficiencias en las medidas y procedimientos recogidas en los planes de seguridad informática de entidades que no se rigen por los estándares internacionales que norman los sistemas de gestión de seguridad informática tanto en la prevención como recuperación ante desastres o ataques.

Hipótesis

Un análisis de aplicación de la norma ISO/IEC 27001 (*International Organization for Standardization / International Electrotechnical Commission*) en el Plan de Seguridad Informática de unaentidad permitirá proponer un Plan de Seguridad Informática que responda a un sistema de gestiónacorde con un estándar internacional de reconocida eficiencia que elevará los niveles de seguridad en dicha entidad.

Objetivo general

Proponer un enfoque de análisis que facilite la elaboración de un Plan de Seguridad Informática de una entidad basado en la norma ISO/IEC 27001.

Objetivos específicos

- Realizar un estudio de Planes de Seguridad Informática existentes en entidades, empresas o instituciones..
- Analizar la norma de Seguridad Informática ISO/IEC 27001.
- Proponer un nuevo Plan de Seguridad Informática a partir de las indicaciones recogidas en la norma ISO/IEC 27001.

METODOLOGÍA DEL PROYECTO

Esta tesis pretende realizar el análisis de la norma ISO/IEC 27001 y el diseño para la implementación en la red de una empresa. Para lo cual se realiza un análisis del sistema, el flujo de datos, estableciendo toda la información a enviar para determinar la capacidad del mismo.

Es una investigación explicativa, donde se valora la técnica de análisis de una norma y su aplicación a la red de una empresa para transmisión en banda ancha.

Se aplica el paradigma Empírico-Analítico, por tratarse de un enfoque cuantitativo y no experimental pues no se manipularán las variables y se observará directamente el fenómeno para su análisis.

A continuación en el capítulo 1 se desarrolla el tema de la Seguridad Informática presentando sus objetivos, aspectos de la seguridad física y lógica, un análisis de riesgos, políticas de seguridad, amenazas, técnicas, entre otros aspectos fundamentales que aportarán al objetivo de este trabajo.

Capítulo 1. Seguridad informática.

En este capítulo se presentará de manera detallada un estudio de la seguridad informática.

1.1 Introducción a la seguridad informática.

La **seguridad informática**actualmente es uno de los temas más analizadospor su impacto en el desarrollo global. Su objetivo escuidar a bien recaudo todos los componentes del sistema de informático de una organización,que se cumplan estándares de seguridad planificadasy que el acceso a la información y su modificación pueda efectuarse solamente por usuarios autorizados y dentro de los límites permitidos a ellos. Se puede entender entonces como seguridad cuando la información de un sistemano corra peligro de sufrir algún daño o riesgoque pueda afectar su funcionamiento o los resultados obtenidos del mismo. La mayoría de los expertos consideran que es imposible tener un sistema informático totalmente seguro.

Para que se pueda definir como seguro debe cumplir con condiciones tales como: la integralidad, donde la información sólo puede ser modificada por quien está autorizado, la confidencialidad, la cual refleja que la información sólo puede ser legible para los autorizados, la disponibilidad de cuando se le necesite, y la irrefutabilidad, es decir que no se pueda negar la autoría. De acuerdo a las fuentes de amenaza la seguridad puede ser lógica o física.

En la actualidad la seguridad informática es un tema de dominio obligado por cualquier usuario de internet u otra red de computadoras, haciendo difícil con su dominio que su información sea robada.

Es necesario que la organización del sistema funcione correctamente y alcance los objetivos propuestos, para que no sucedan incidentes que produzcan daños materiales o pérdidas inmateriales en los activos, según con ello es vital medir las consecuencias al materializarse una amenaza, debido a la posibilidad de un impacto determinado en un activo, en un dominio o en toda la organización. Según información disponible en http://suriramirez.blogspot.com/, se dice, que, un sistema será más vulnerable o no en dependencia de la capacidad que tenga de rechazar las amenazas, manteniendo así su correcto funcionamiento.

1.2 Objetivos de protección de la seguridad informática.

El objetivo de la seguridad informática es la protección de los activos, los cuales están formados por tres elementos:

Información: Es lo más importante para una entidad y su protección es el objetivo primordial, independientemente de donde esté almacenada, en medios electrónicos o físicos.

Equipos que la soportan: Dentro de los equipos que soportan la información se encuentran: software, hardware y la organización.

Usuarios: se denomina así a quienes utilizan la infraestructura tecnológica y de comunicaciones en que se manipula la información.

1.3 Análisis de riesgos.

Como ya se indicó anteriormente, la información es considerada el activo más importante y, por lo tanto, es necesaria la aplicación de técnicas que garanticen su seguridad, siendo más importante que la **seguridad física**implementada para proteger los equipos de almacenamiento, la **seguridad lógica**de la misma, mediante técnicas que aplicanbarreras y procedimientospara resguardar el acceso a los datos, permitiéndoloúnicamente a los usuarios autorizados.Suele indicarse en la seguridad informática que *"lo que no está permitido debe estar prohibido"* y ese debe ser el objetivo a alcanzarse.

Entre los medios para conseguir dicho objetivo pueden mencionarse los siguientes:

- Limitar el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.

- Establecerlimitaciones para que los usuarios puedan operar pero sinalterar los programas o archivos que no conciernan.
- Garantizar que los datos, archivos y programas correctos sean utilizados de acuerdo al procedimiento seleccionado.
- Certificar que la información que se envía sea la misma que llegaal receptor al que se envía y no a un destino diferente.
- Garantizar la existencia de sistemas y caminos emergentesalternospara transmitir entre diferentes puntos.
- Dotar a cada usuario de acuerdo a su jerarquía informática, de una clave y autorizacionescorrespondientes para los sistemas o programas que utilice.
- Cambiar continuamente las claves de acceso a los sistemas informáticos.

1.4 Seguridad físicaen las redes de computadoras.

La **seguridad física**se refiere a las medidas externas aplicadas para proteger al computadory su entorno de amenazas físicas. Para este fin, por lo general se utilizan dispositivos eléctricos, electrónicos, etc., y son las primeras medidas de protección que se implementan en las instalaciones para sistemas informáticos, por dos causas: la primera es la posibilidad de que ocurra un incendio, inundación u otro tipo de catástrofe que produzca la pérdida total de la infraestructura. La segunda, es que las medidas de seguridad física son usualmente las más fáciles de tomar,su costo no es excesivo (con la excepción de los sistemas de continuidad eléctrica) y su mantenimiento no ofrece especiales problemas.

En el caso de los CPD (Centros de Procesamiento de Datos), la protección para todas las amenazas que puedan presentarse,parte de su apropiada ubicación geográfica y la adecuada construcción de la mismaen el sitiocorrecto dentro dela edificación. Existen además medidas específicas para cada tipo de amenaza. En resumen, la correcta ubicación de los equipos en edificios alejados de zonas potencialmente peligrosas es la mejor medida para la protección del sistema.

A continuación se detalla brevemente algunas amenazas físicas que pueden presentarse:

Inundaciones internas: A más de las medidas constructivas (no deben pasar tuberías de agua por techos ni paredes, debe haber desagües en el piso real, el cual debe presentar una inclinación hacia estos, etc.), existen detectores de humedad para alertar de la inundación. Además, se recomienda tapar con forros plásticos los equipos cuando no se usen, sobre todo los PC's (*Personal Computer,* Computadora Personal).

Fuego: Los sistemas de detección/extinción de incendios son suficientemente conocidos. Hoy en día, el halón es el elemento más utilizado para combatir incendios, es un gas anticatalítico de la reacción química que causa el fuego y no es tóxico en pequeñas proporciones, sin embargo en Convención de Montrealpor el daño que produce a la capa de ozono se acordó su total eliminación, por lo cual se investigan sustitutos para este elemento.

Caídas de tensión: Aquí se consideran los cortes de más de unos pocos milisegundos, microcortes, transitorios, etc. Lo más eficaz contra estas anomalías del suministro es un UPS (*Uninterrupted Power System)* o SAI (Sistema de Alimentación Ininterrumpida) preferiblemente en línea puesto que los fuera de línea precisan de unos microsegundos, tiempo de conmutación, para actuar. En casos de cortes más prolongados se necesitaría un equipo electrógeno de respaldo.

Calor: La protección contra el calor depende de la instalación de alarmas que se dispararían en caso de subir o bajar la temperatura del lugar seleccionado por encima o debajo de los límites permitidos.

Interferencias electromagnéticas: Para esta amenaza la solución óptima es el apantallamiento de la sala de computadoras y el uso de terminalescon certificación TEMPEST (Enmascaramiento de Pulsos Electromagnéticos Transientes). En razón de que las líneas de comunicación son las más expuestas a estas amenazas, deben usarse cables apantallados o de fibra óptica.

Atentados: Es posible evitar estos casos aplicando estrictos controles de ingreso a las ubicaciones de los computadores. Si se trata de instalaciones informáticas de mayor jerarquía, pueden implementarse controles biométricostales como: reconocimiento de

huellas digitales, fondo de ojo, forma de la mano, voz, etc., inclusive se puede controlar los materiales que ingresan a estos sitios mediante dispositivos de reconocimiento.

Hurtos: Son más susceptibles a estos riesgos las computadoras portátiles y sus dispositivos periféricos, para prevenirlos es posible implementar técnicas de anclaje. Las pérdidas anuales estimadas por hurto de partes de PCs sobrepasan los 5 billones de dólares, sin considerar el valor de la información robada. A continuación, en la figura 1.1, se muestran los riesgos físicos que pudieran atentar contra una determinada red de computadoras.

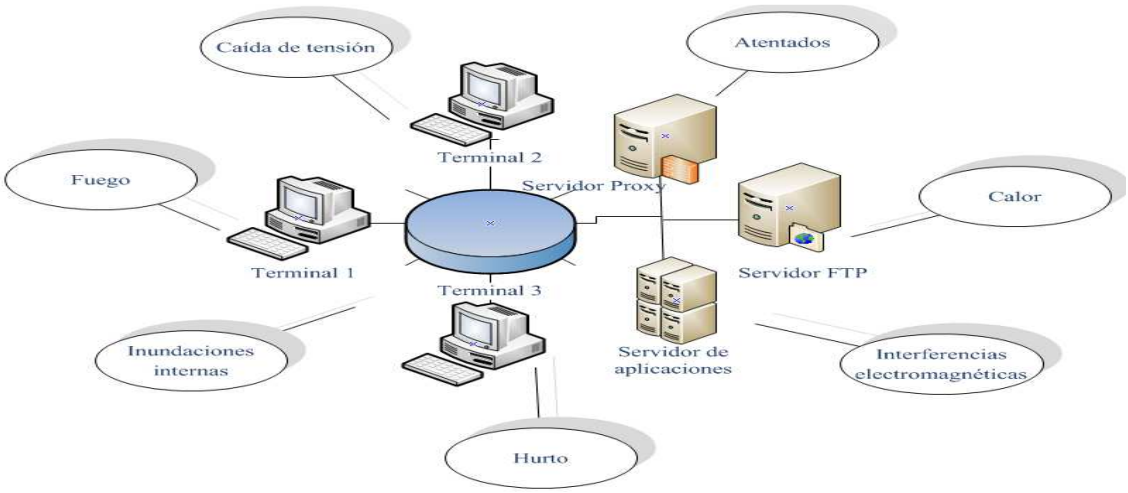

Figura 1.1 Riesgos en la seguridad física de una red de computadoras

Elaborada por el autor

1.5 Seguridad lógica en las redes de computadoras.

Ahora se tratará acerca de la seguridad lógica para los sistemas informáticos.

Defensa perimetral: La seguridad perimetral es uno de los métodos posibles de defensa de una red, se basa en la implementación de recursos para asegurar el perímetro externo y a diferentes niveles. Es necesario proteger todos los elementos de la red interna, esto es*hardware, software*, datos, etc., no solo de cualquier intento externo de acceso no autorizado, sino también de ataques desde dentro que se pueden prevenir. Sin embargo, se pueden definir niveles de confianza, permitiendo el acceso de determinados usuarios externos a ciertos servicios o denegando cualquier tipo de acceso a otros.La

implementación de una defensa perimetral podría basarse en dos paradigmas de seguridad:

- Todo lo que no se prohíbe expresamente está permitido.
- Todo lo que no se permite expresamente está prohibido.

De aquí que se puedan implementar estrategias “paranoicas”, “prudentes”, “permisivas” o “promiscuas”, siempre cumpliendo las políticas impuestas en la red. Dichas estrategias podrían dejar a un sistema sin servicio o alojar intrusos en la red. Esto permitiría decidir qué métodos de defensa es posible establecer:

- En profundidad
- Perimetral

De las dos aproximaciones tradicionales antes mencionadas como métodos de defensa, se podría optar por implementar un esquema de seguridad perimetral para el cumplimiento de las políticas definidas por la institución. A su vez se podría optar por una estrategia "prudente", sin caer en lo "paranoico" ni en lo "permisivo"(técnicamente hablando). Comúnmente, una institución preferiría adoptar esta solución al darse cuenta de la dificultad de mantener un sistema de seguridad del nivel paranoico con los medios tanto técnicos como humanos de los que pudiera disponerse. Por el contrario, en caso de querer forzar el cumplimiento obligado de las medidas adoptadas, se podría optar por un modelo "todo lo que no se permite expresamente está prohibido", especialmente en el punto único de entrada y salida del perímetro interior. Otros aspectos importantes que deberían incorporarse en la política de seguridad dentro de este plan perimetral son:

- Procedimientos para reconocer actividades no autorizadas.
- Definir acciones a tomar en caso de incidentes.
- Definir acciones a tomar cuando se sospeche de actividades no autorizadas.
- Conseguir que la política sea refrendada por el sector más alto posible dentro de la organización.

- Divulgar la política de forma eficiente entre los usuarios y administradores.
- Implementar auditorías del sistema de seguridad.
- Establecer plazos de revisión de la política en función de resultados obtenidos.

Una vez definido el modelo de seguridad a utilizar, resultaría necesario definir las herramientas con las que se contará para su implementación.

Estructura del método de seguridad perimetral: Las directivas marcadas dentro de la política de seguridad definida por una institución, fuerzan a diseñar su propia red en dos perímetros bien definidos: Uno interior, en el que se ubicarán los recursos sensibles a un posible ataque, y el exterior donde se situarán los recursos menos sensibles, o que inevitablemente por motivos funcionales deban estar en contacto con el mundo exterior de forma menos rígida. Es necesario aislar el perímetro interior del exterior y además del resto de Internet, mediante un dispositivo en el que se centralizarán la mayoría de las medidas: los cortafuegos. Un ejemplo podría ser el de una institución educativa en cuyo perímetro interior o red de servidores necesitara ubicar dos servidores para usuarios no confiables en la red externa de estudiantes, servicios de FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos), correo electrónico y aulas virtuales como se muestra en la figura 1.2:

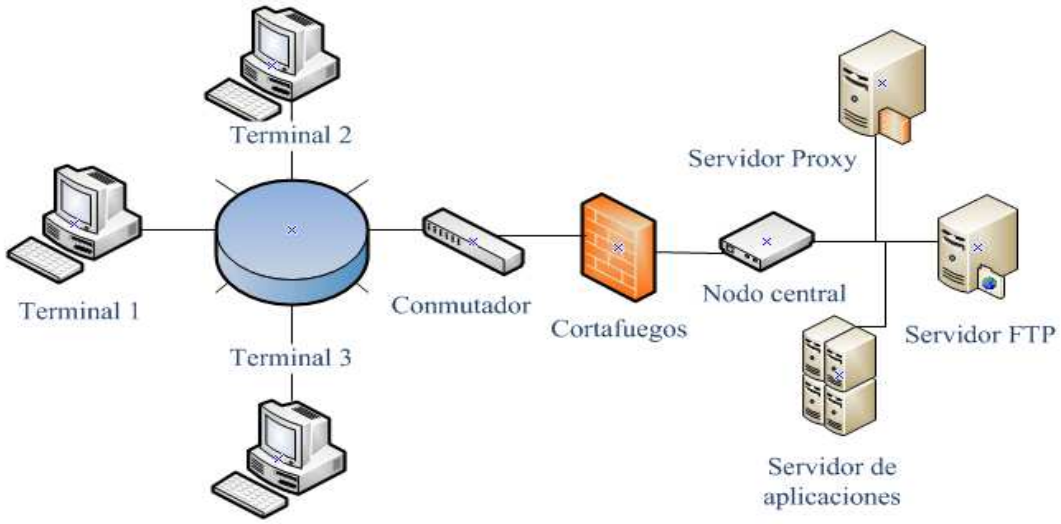

Figura1.2 Conexión de dos redes a través de un cortafuegos

Elaborada por el autor

De acuerdo a lo expresado, es necesario aplicar medidas diferentes a los servidores internos ya que estarían expuestos más directamente a los ataques externos, siendo necesario utilizar sobre ellos, medidas típicas de "seguridad en profundidad" tales como:

Protección del Cortafuegos: Mientras solo se permite el ingreso como usuario del administrador a los cortafuegos, los demás usuarios no tienen ningún tipo de acceso al mismo, pudiendo hacer iniciar una sesión únicamente, dentro de la red de servidores. Cualquier programa o utilidad innecesaria o potencialmente peligrosa será desinstalada. Algunas de las acciones que activarían la notificación de alarma serían:

- Intento de acceso a puertos restringidos.
- Intento de acceso a cualquier puerto superior al 1024.

Algunas de las acciones motivo de examen o inspección serían:

- Registro de todos los paquetes rechazados.
- Registro de todos los procesos de inicio de sesión que han sido incorrectos.

Restricción de acceso al Cortafuegos

- Cuentas de usuario en ningún sistema que ejerza de cortafuegos.
- No se permite inicio de sesión al cortafuego desde el exterior.
- Las cuentas con privilegios de administrador solo se pueden activar desde la consola del sistema.
- Un programa se encarga de manera regular de chequear la integridad del sistema.
- Para efectuar un cambio de configuración del sistema se requiere reiniciar el sistema.

Algunos modelos también tienen protecciones físicas como:

Protección de la red interior: son sistemas dedicados a una misión, utilizan *hardware* y *software* para implementar un cortafuegos que tiene como única función la seguridad y como misión la protección de la red interior (servidores). En lugar de conformarse con una aplicación de *software*, se intenta elevar el nivel de protección con un "sistema dedicado". Esta solución de tener un cliente dedicado es desestimada por algunas entidades por el costo económico que supone dedicar un sistema (bastante caro en algunos casos) a la tarea exclusiva de proteger la red perimetral interna.Es evidente que el nivel de protección de las redes que no cuentan con un equipo de estas características es sensiblemente menor.

Construcciones de Muro Doble: Algunos cortafuegos se construyen con la técnica de "muro doble", en este caso el cortafuegos consta de dos sistemas separados físicamente (muro exterior e interior) conectados por una red privada como por ejemplo tipo DMZ (*Demilitarizaded Zone,* ZonaDesmilitarizada). Si alguien es capaz de comprometer el muro exterior, el muro interior protege la red cortando su red DMZ y aislando la red interior. El muro interior se rige por el "pesimismo", de forma que solo acepta paquetes si responden a una petición originada en el interior de la red o provienen de uno de sus servidores (por defecto guarda toda la información sobre las transacciones). De no llegar de estas dos fuentes, se pone a la defensiva de manera inmediata cortando la red privada que lo une al muro exterior y alerta sobre una posible violación de seguridad crítica.

Realmente, la lógica de esta alternativa es bastante dudosa pues en un sistema con unos únicos cortafuegos, si se lograra comprometer al mismo, el atacante ganaría el acceso a toda la red. Este caso específico de "muro doble", lo único que lograría el presunto atacante es aislar la red (aunque puede que este sea el verdadero objetivo del atacante).

Los cortafuegos, además, poseen otras propiedades:

Acceso transparente a la red: Los cortafuegos ofrecen acceso transparente a la red a las aplicaciones TCP/IP (*Transmission Control Protocol/Internet Protocol,* Protocolo de Control de Transmisión/Protocolo de Internet)de los servidores, siempre y cuando estén

habilitadas. Esto significa que tanto las computadoras comunes con sistemas operativos como Windows y Linux, operan normalmente a través del cortafuegos. Las aplicaciones IP (*Internet Protocol*, Protocolo de Internet)comunes tales como Telnet, FTP, servicio *web*, etc., se pueden utilizar sin modificaciones.

Ocultación de Dominios: El cortafuegos oculta el dominio interno de la red protegida; si se posee un “muro doble” la única parte que expone de su dominio es el “muro exterior”, no interfiriendo servicios permitidos, por ejemplo, correo electrónico, FTP u otros servicios aprobados para la red externa. De manera adicional, el correo enviado desde la red de servidores será "despojado" de la información comprometedora con respecto al servidor y DNS (*Domain Name System*, Sistema de Nombres de Dominio) que podría dar a un potencial atacante una idea de la configuración interior de la red.

NAT (*Network Address Translation,* Traducción de Dirección de Red): Todas las direcciones IP son traducidas a la del cortafuegos expuesto, lo que significa que todos los paquetes de datos que se originan dentro de la red aparecen como provenientes del cortafuegos. En la red LAN(*Local Area Network,* Red de Área Local) las computadoras de los clientes de las redes de estudiantes tendrán como puerta de enlace la interfaz donde se localiza el cortafuego. Cuando se solicita un servicio de la red interna de servidores, esta interfaz traducirá de nuevo la dirección a la de destino en la red de los servidores.

Filtrado Inteligente de Paquetes: Todos los paquetes dirigidos hacia el cortafuego son "inteligentemente filtrados" para impedir el acceso a puertos no autorizados. Se permite la conexión únicamente a los clientes autorizados y el administrador puede conceder o denegar acceso de manera amplia, valiéndose hasta de combinaciones específicas de cliente/puerto (por ejemplo puede prohibir a todas las subredes usar el puerto "x", o solo al cliente "x", o solo el cliente "x" puede usar el puerto "z").La defensa perimetral basa su accionar en un conjunto de recursos de aseguramiento establecidos en el perímetro externo de la red, tales como cortafuegos y enrutadores asegurados.

Seguridadenlosencaminadores: Dentro de la amplia gama de soluciones que se pueden encontrar para incrementar la seguridad de la red, una de ellas la constituyen los encaminadores que filtran paquetes los cuales realizan el reenvíoo unasupresión de los mismos, basados en un conjunto de reglas configuradas por el administrador de la red.La configuración de estos encaminadores debe contemplar:

- Qué servicios se ofrecerán y en qué dirección.
- Las limitaciones respecto a la cantidad de computadoras que tendrán acceso a los servicios y su posible agrupamiento.
- La existencia de equipos en Internet o redes externas que deban autenticarse con los equipos internos.

Los parámetros a considerar para crear las reglas o políticas son:

- Dirección IP origen y destino.
- Protocolo de capa 3 (IP).
- Protocolo de capa 4 TCP/UDP(*Transmission Control Protocol /User Datagram Protocol*, Protocolo de Control de Transmisión/ Protocolo de Datagrama de Usuario).
- En los segmentos TCP (*Transmission Control Protocol*, Protocolo de Control de Transmisión), el *bit* de ACK (*Acknowledgement*, Acuse de Recibo o Asentimiento).
- Tipo de mensaje para el caso de protocolo ICMP (*Internet Control Message Protocol,* Protocolo de Mensajes de Control de Internet)
- Puertos origen/destino de TCP y UDP (*User Datagram Protocol*, Protocolo de Datagrama de Usuario).

Encaminadoresque filtranpaquetes: Previo al análisis de una implementación con encaminadores que filtran paquetes, hay que recordar que el encaminamiento ordinario solamente tiene en cuenta hacia dónde se dirige cada paquete de información, y selecciona cuál es la mejor vía para llegar a su destino. Este tipo de encaminamiento no tiene en cuenta las políticas de seguridad o si la ruta es potencialmente segura o insegura. Únicamente su objetivo es el de llevar la información a su destino. El encaminador que filtra paquetes en cambio, analiza el paquete de información al detalle y establece si puede ser enviado a su destino en función de las políticas de seguridad del sistema. En el supuesto caso de que fuera el único sistema de protección, y ante su posible falla, la red o el equipo puede verse expuesto a las amenazas del exterior. Este

encaminador puede dar acceso a un servicio o denegarlo. Pero, de haberse producido el acceso no autorizado, no puede realizar protecciones individuales dentro del mismo.

Al igual que un cortafuegos, este filtro encaminador discrimina paquetes de información o de datos que va redirigiendo entre los clientes internos y externos del sistema, gracias a una selección que realiza siguiendo las políticas de seguridad establecidas. Seguidamente en la figura 1.3 se representa una topología de red implementada con un encaminador que filtra paquetes.

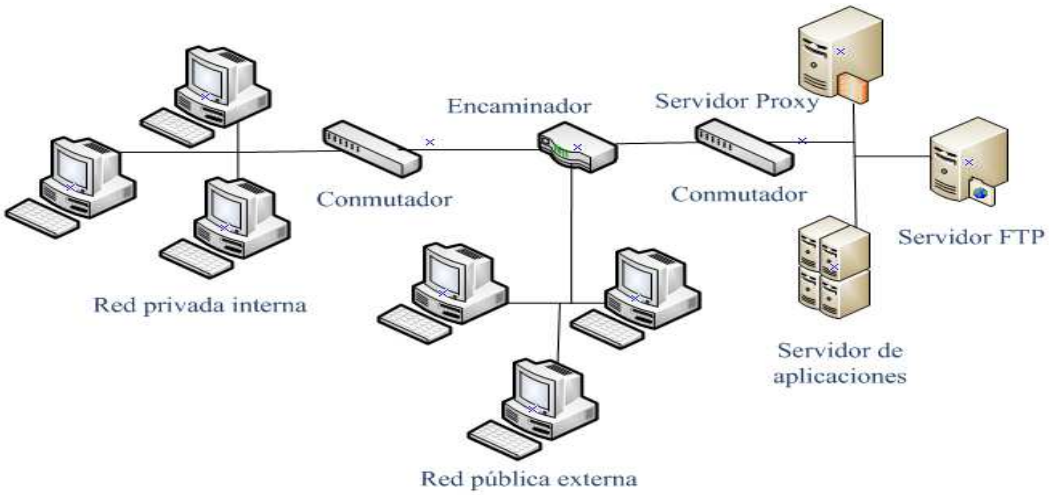

Figura1.3 Topología de red implementada con encaminador que filtra paquetesElaborada por el autor

Para entender la finalidad de dicho encaminador pueden considerar algunos de los siguientes elementos:

- Bloqueo de todas las conexiones externas, salvo aquellas que trabajen bajo SMTP(*Simple Mail Transfer Protocol*, Protocolo para la Transferencia Simple de Correo Electrónico), para permitir la recepción de correo electrónico.
- Bloqueo de todas las conexiones que puedan considerarse potencialmente inseguras.
- Permisión del servicio de correo electrónico y de FTP, aunque manteniendo el bloqueo a servicios potencialmente peligrosos como TFTP (*Trivial File Transfer Protocol,* Protocolo de Transferencia de Archivos Triviales), RPC (*Remote*

Procedure Call, Llamada de Procedimiento Remoto), servicios del tipo "r": *rlogin* (Acceso por Clave no Verificado), etc.

- Políticas de seguridad en los encaminadores que filtran información.

Existen una serie de elementos de seguridad que son similares a todos los cortafuegos:

- Un criterio de filtro de paquetes que se establece para los puertos del dispositivo.
- Cuando un paquete de información llega al puerto establecido, cada uno de sus encabezados se analiza. Generalmente ocurre en los de tipo IP, TCP o UDP.
- Las reglas de filtro de paquetes se guardan en un orden preciso para que cada una de ellas se ejecute en ese mismo orden, en función del tipo de paquete de información que llegue al sistema de red o al equipo.
- En el caso de que una regla (o parte de ella) se vea vulnerada, o no cumpla los requisitos establecidos, el paquete de información podrá recibirse en el sistema, pero, éste avisará mediante alertas de cuáles han sido los protocolos y normas que no cumple.
- Si la política de seguridad lo permite, la transmisión de los datos continúa y se recibe el paquete.
- Si un paquete no cumple ninguna de las reglas, se manda un aviso al sistema, que impide su acceso. En función de lo explicado anteriormente, quedaría definida la importancia del mantenimiento adecuado del orden de las reglas de este encaminador, ya que la aplicación las va leyendo una a una. Al igual que un cortafuegos, un encaminador que filtra paquetes no es un sistema autónomo que pueda ir de una regla a otra sino que las va procesando según el orden marcado por el administrador del sistema.
- Si las reglas se establecieran en un orden equivocado, podría no permitir el acceso de servicios que serían válidos, y permitir el acceso a otros servicios nocivos. Un encaminador que filtra paquetes puede ser un encaminador comercial o un nodo con capacidad de encaminamiento que posee aptitudes de filtrado de paquetes, teniendo la funcionalidad de bloquear o permitir el tráfico entre redes o nodos basados en direcciones, puertos, protocolos e interfaces, etc.

Arquitecturade clienteencaminador: Un cliente encaminador (llamado también *PC-router)*cuando se configura como cliente bastión, como se observa en la figura 1.4 es una computadora que encamina paquetes y también posee la capacidad de filtrarlos (cortafuegos). Este cliente encaminador es la única computadora de la red interna por la que los clientes externos pueden abrir conexiones, donde solo cierto tipo de conexiones son permitidas. Por lo tanto, cualquier sistema externo que intente acceder al sistema interno, deberá conectarse con este cliente, el cual se requiere que tenga un alto nivel de seguridad. El filtrado de paquetes, también, debe permitirle al cliente encaminador abrir conexiones a subredes exteriores. La configuración del filtrado de paquetes en este cliente debería contemplar las siguientes reglas:

1. Permitir que clientes internos se conecten con clientes externos para ciertos servicios (servicios permitidos por medio de paquetes filtrados)

2. No permitir todas las conexiones desde los clientes internos (forzar a esos clientes a usar el servicio vía cliente encaminador).

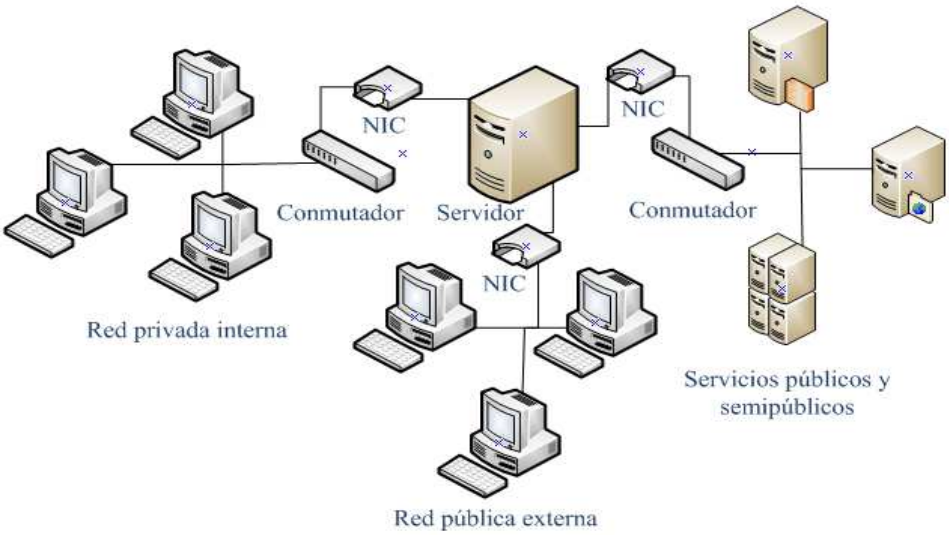

Figura1.4 Comunicación a una red externa a través de un cliente encaminador

Elaborada por el autor

Existen algunas desventajas en una implementación de este tipo; la principal es que si un ataque vulnera al cliente encaminador, esto no es notado por la red interna. Asimismo, el encaminador también presenta un punto de falla, porque si es comprometido, la red entera está disponible para ser atacada. El encaminador puede ser

el primer elemento a utilizar en la estrategia de defensa perimetral, si bien éste debe contar con recursos de seguridad e inspección para mejorar su rendimiento. A continuación se explicará cómo esta instancia se potencia con los cortafuegos.

Cortafuegos: El cortafuegos constituye una segunda línea dentro de la defensa perimetral, ya que la primera fue el encaminador que filtra paquetes o su variante cliente encaminador. Un cortafuegos es un equipo que inspecciona el tráfico y realiza un control de acceso a los recursos de la red basado en políticas predefinidas, de las que se distinguen dos tipos básicos, impidiendo que atacantes o personal no autorizado acceda a recursos o servicios de la red interna. Estos principios son:

- Aceptar todo servicio, excepto lo denegado por las reglas.
- Filtrar todo servicio, excepto lo permitido por las reglas.

De este modo, un cortafuego "sí" puede permitir servicios *web*, correo y FTP desde una la red interna hacia la red externa, pero "no" permitir el *chat* que puede o no ser necesario para el trabajo. También, se puede configurar los accesos que se hagan desde la red externa hacia la red interna y es posible denegar todos, o permitir algunos servicios como el de FTP.Siendo un dispositivo con un único propósito (prohibir el acceso no-autorizado a terceras personas) se conecta entre el encaminador y la red interna como se muestra en la figura 1.5, y actúa como un guardia vigilando y controlando el tráfico de los datos, previniendo actos sospechosos de atacantes y otras personas. Sólo los empleados o personas con autorización pueden tener el acceso a los datos más relevantes y el administrador de seguridad será el único que lo permitirá. Además, en algunos casos hay que implementarlos internamente (en diferentes sectores de la red interna) para proteger a los departamentos que poseen información particularmente sensitiva.

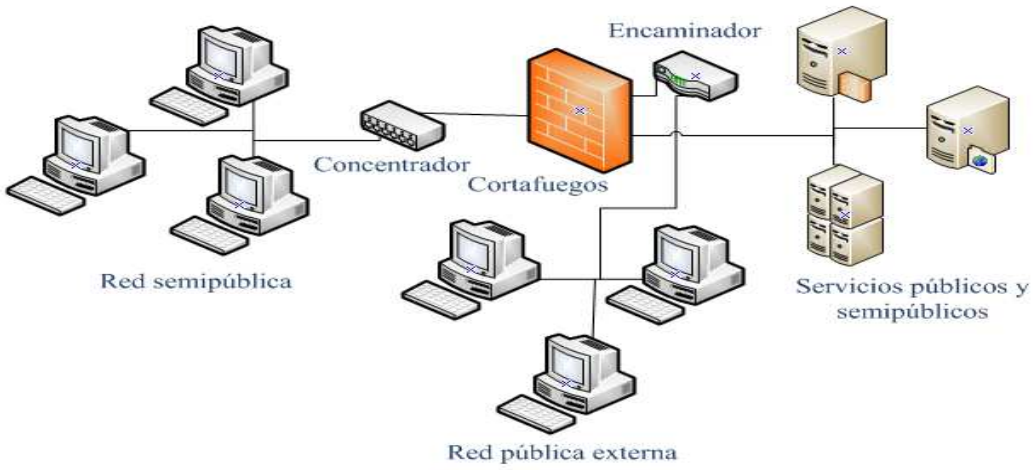

Figura1.5 Topología de red usando encaminador- cortafuegos

Elaborada por el autor

El cortafuego registra todos los accesos a la red interna y desde ella, y acepta o rechaza conexiones basadas en reglas prefijadas.

Conocer la diversidad de los modelos de algunos cortafuegos que existen actualmente, ayuda a clarificar qué tipo o tipos implementar. Su clasificación básica es:

- Filtros de paquetes
- Cliente Bastión
- Proxies

Los cortafuegos basados en *proxies*, poseen una serie de ventajas tendientes a incrementar la seguridad, pero no se tratan explícitamente en este trabajo porque no son de gran aplicación en la investigación.

Filtros de paquetes: Son aquellos dispositivos que estando conectados a ambos perímetros (interior y exterior), dejan pasar (a través de ellos) paquetes IP en función de reglas predeterminadas. Estos cortafuegos conceptualmente trabajan a nivel de red, y son capaces de filtrar tráfico en función de direcciones IP, protocolos, y números de puerto de TCP o UDP. Normalmente, esta misión la pueden desempeñar tanto clientes con dos o más tarjetas de red, como encaminadores. En el caso de cortafuegos basados en filtrado de paquetes, los dispositivos de la red interna se configuran con la ruta por

defecto apuntando a este dispositivo, que en función de sus reglas, dejará pasar estos paquetes o los rechazará. El principal problema de este tipo de cortafuegos es la limitación a la hora de configurar reglas complejas y la falta de flexibilidad en la capacidad de *log* o registro de actividad. Otra limitación fundamental es la imposibilidad de filtrar tráfico en función de información contenida en niveles superiores, tales como URLs(*UniformResourceLocator,* Localizador de Recursos Uniforme), o esquemas de autenticación fuertes.

Cualquier encaminador IP utiliza reglas de filtrado para reducir la carga de la red, por ejemplo, se descartan paquetes cuyo TTL (*TimetoLive,* Tiempo de Vida) ha llegado a cero, paquetes con un control de errores erróneos, o simplemente tramas de difusión.Además de estas aplicaciones, el filtrado de paquetes se puede utilizar para implementar diferentes políticas de seguridad en una red; el objetivo principal de todas ellas suele ser evitar el acceso no autorizado entre dos redes, pero manteniendo intactos los accesos autorizados. Su funcionamiento es habitualmente muy simple: se analiza la cabecera de cada paquete, y en función de una serie de reglas establecidas previamente, la trama es bloqueada o se le permite seguir su camino. Estas reglas suelen contemplar campos como el protocolo utilizado (TCP, UDP, ICMP, etc.), las direcciones fuente y destino y el puerto de destino. Además de la información de cabecera de las tramas, algunas implementaciones de filtrado permiten especificar reglas basadas en la interfaz del encaminador por donde se reenvía el paquete, y también en la interfaz por donde ha llegado hasta el usuario.

Bastión: Un cliente bastión, como se ve en la figura 1.6, es un servidor asegurado, a tal punto, que no es viable en circunstancias normales. Este tipo de dispositivo hace uso de los recursos internos de seguridad del sistema operativo, la auditoría y la autenticación al máximo. Los servicios no autorizados son desestimados, al igual que toda cuenta de usuario, excepto la de administración. Usualmente, funciona en forma conjunta con el filtro de paquetes instalado en el encaminador que conecta la red LAN a Internet.

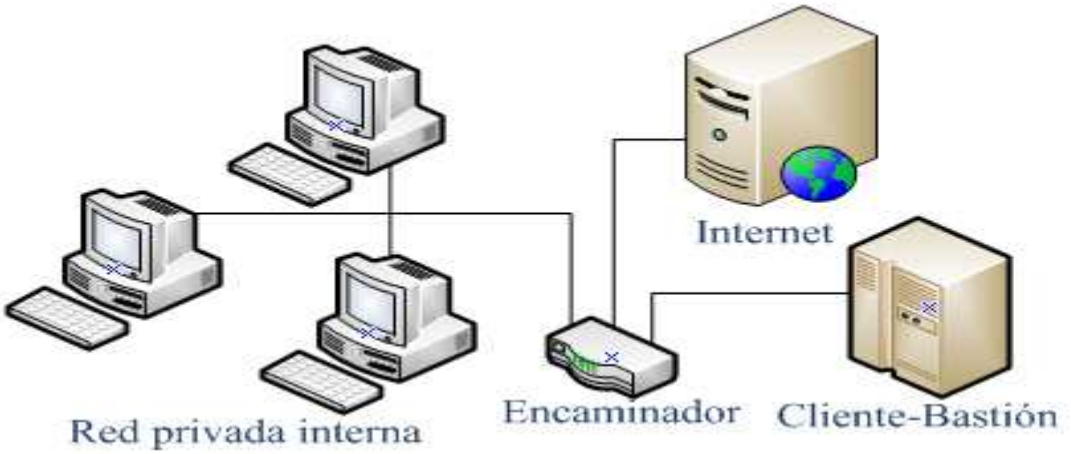

Figura1.6 Topología cliente bastión y encaminador con filtro de paquetes

Elaborada por el autor

TopologíaDMZ: Es posible implementar diferentes arquitecturas de seguridad basándose en cortafuegos, y armar con ellas un diseño de red perimetral segura que comprenda diferentes áreas, dependiendo de los niveles de seguridad requeridos. DMZ es la zona donde residen los servidores que contienen aplicaciones semipúblicas, como el servidor de correo, *web*, etc. A este sector de la red es posible acceder desde el exterior, previo filtrado del encaminador y cortafuegos perimetral. Los servidores de aplicaciones están protegidos por medio de otro cortafuegoque forma un segundo circuito de defensa, con direcciones no direccionales desde Internet.Existen determinadas situaciones en las que sería necesario dejar entrar a cualquier persona a alguna parte determinada de la red. Por ejemplo, si se estuviera operando un portal de Internet en un servidor *web* conectado a la red interna de la entidad, seguramente será preciso que los visitantes potenciales tengan acceso en cualquier momento a determinadas áreas de la red. En este caso, sería necesario disponer de un cortafuego que contenga un puerto desmilitarizado.

Este puerto no provee notorias funciones de seguridad, por lo que cualquier usuario podría acceder al recurso en cuestión. Por ejemplo, se podría conectar el servidor *web* al puerto DMZ y el resto de la red interna a los demás puertos que sí estarían provistos de seguridad. De esta manera, la red sería privada, mientras que el sitio *web* de la entidad (servidor *web*) no.Entonces, podría decirse que una DMZ es una red entre una red protegida y una red externa, cuyo objetivo es proveer de un nivel de seguridad adicional

a los recursos (o servicios) que necesiten ser publicados a la comunidad de Internet, redes o subredes. En esta red adicional, podrían ubicarse los servidores que no estarían totalmente protegidos por el cortafuego, como por ejemplo, un servidor de correo. Se muestra en la figura 1.7 un ejemplo de DMZ donde al tráfico proveniente de Internet se le aplica un filtrado ligero y cuando ingresa a la red privada se filtra más rigurosamente.

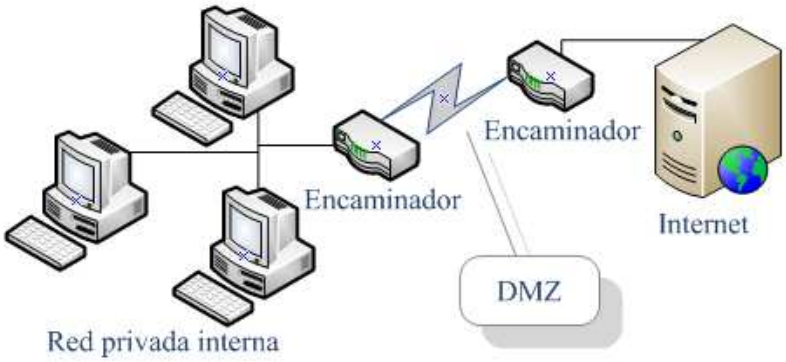

Figura 1.7 Topología DMZ

Elaborada por el autor

Subredprotegida: La arquitectura de subred protegida, también conocida como red perimétrica o DMZ añade un nivel de seguridad en las arquitecturas de cortafuegos, situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al cliente bastión. En otros modelos, toda la seguridad se centra en el bastión de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como el sistema bastión es un objetivo codiciado por muchos piratas, la arquitectura DMZ intenta aislarla en una red perimétrica, de forma tal que, si un intruso lograra acceder a este sistema, no consiga un acceso total a la subred protegida. Subred protegida es la arquitectura más segura, pero también la más compleja.Se utilizan dos sistemas (pueden ser dos encaminadores) denominados exterior e interior, conectados ambos a la red perimétrica (que constituye el sistema cortafuegos) en que se incluye el cliente bastión; y también, se podrían incluir otros sistemas que requieran un acceso controlado, como por ejemplo el servidor de correo o el de servicios *web*, que serían los únicos elementos visibles desde fuera de la red.El encaminador exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica.

De esta forma, un atacante tendría que romper la seguridad de ambos encaminadores para acceder a la red protegida. Incluso es posible; si se desean mayores niveles de seguridad, definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas; así, el atacante habrá de saltar por todas y cada una de ellas para acceder a todos los sistemas de la entidad. Evidentemente, si en cada red perimétrica se siguen las mismas reglas de filtrado, estos niveles adicionales no proporcionarían mayor seguridad.

Aunque la arquitectura DMZ es la que mayores niveles de seguridad puede proporcionar, no se trata del ideal de los sistemas cortafuegos. Existen algunos problemas relacionados con este modelo: por ejemplo, se puede utilizar el cortafuegos para que los servicios fiables pasen directamente sin acceder al cliente bastión, lo que puede dar lugar a un incumplimiento de la política de la organización. Un segundo problema, quizás más grave, es que la mayor parte de la seguridad reside en los encaminadores utilizados. Como se ha dicho antes las reglas de filtrado de estos elementos pueden ser complicadas de configurar y comprobar, lo que puede dar lugar a errores que abran importantes brechas de seguridad en toda la infraestructura de la entidad. Seguidamente se observa en la figura 1.8 la topología de subred protegida.

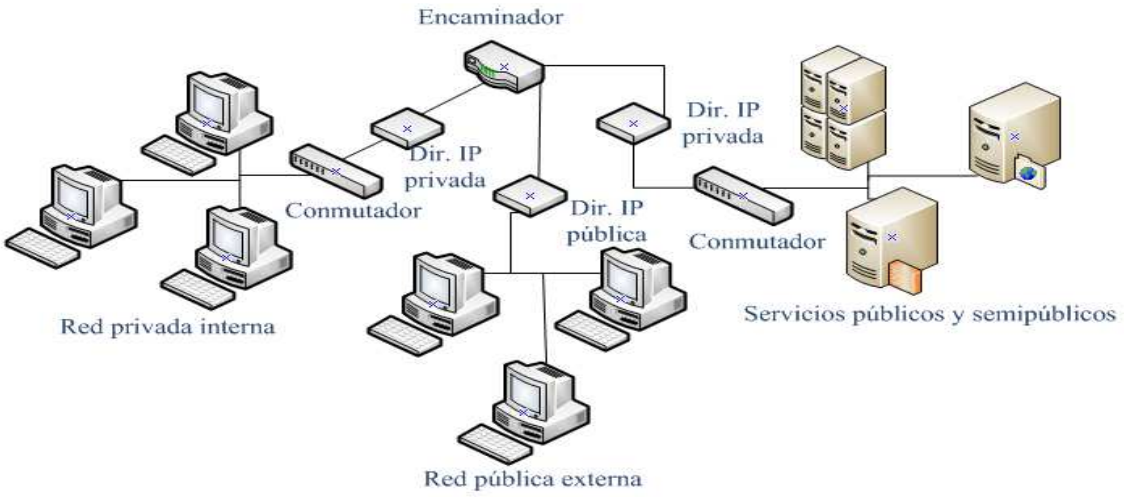

Figura1.8 Topología de subred protegida

Elaborada por el autor

También pueden existir variantes en las que se utiliza un *PC-router* (combinación cliente ruteador y bastión) en el mismo sistema, como se representa en la figura 1.9, donde este cliente es el encargado de filtrar, denegar servicios, gestionar el tráfico, proteger contra intrusos y encaminar. Según el tráfico que este maneje incluso podría llegar a prestar algunos servicios como DNS, DHCP (*Dynamic Host Configuration Protocol*, Protocolo de Configuración Dinámica de Host), correo electrónico, etc.

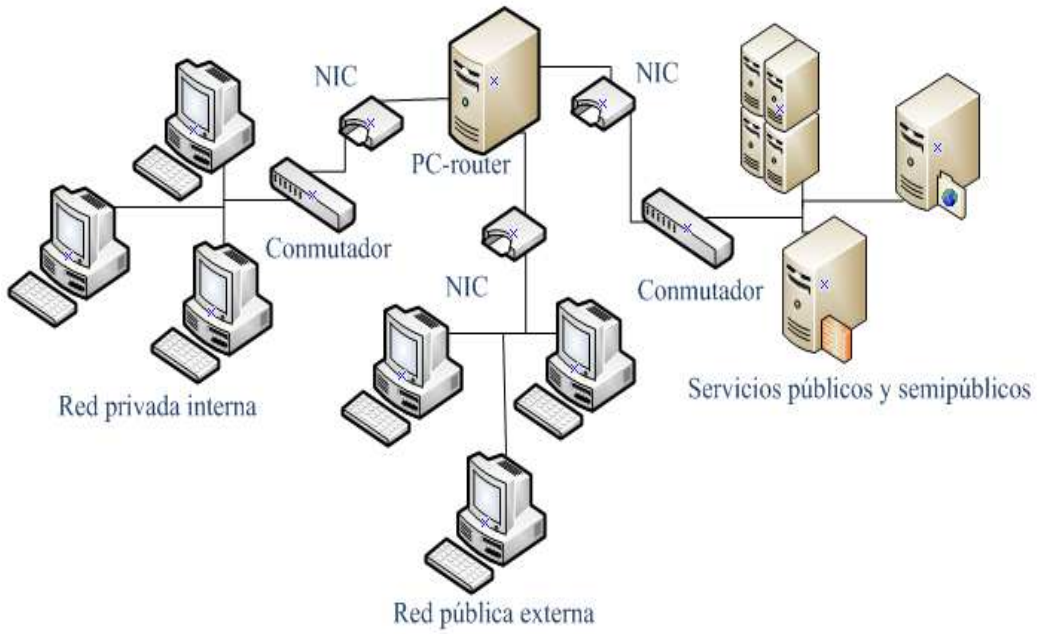

Figura1.9 Topología de subred protegida usando un PC-router

Elaborada por el autor

En los dos últimos ejemplos, al segmentar la red mejora su rendimiento y se divide tanto el dominio de colisiones como el de difusión, una gran red se segmenta por las necesidades de rendimiento y seguridad como se expone seguidamente en la figura 1.10.

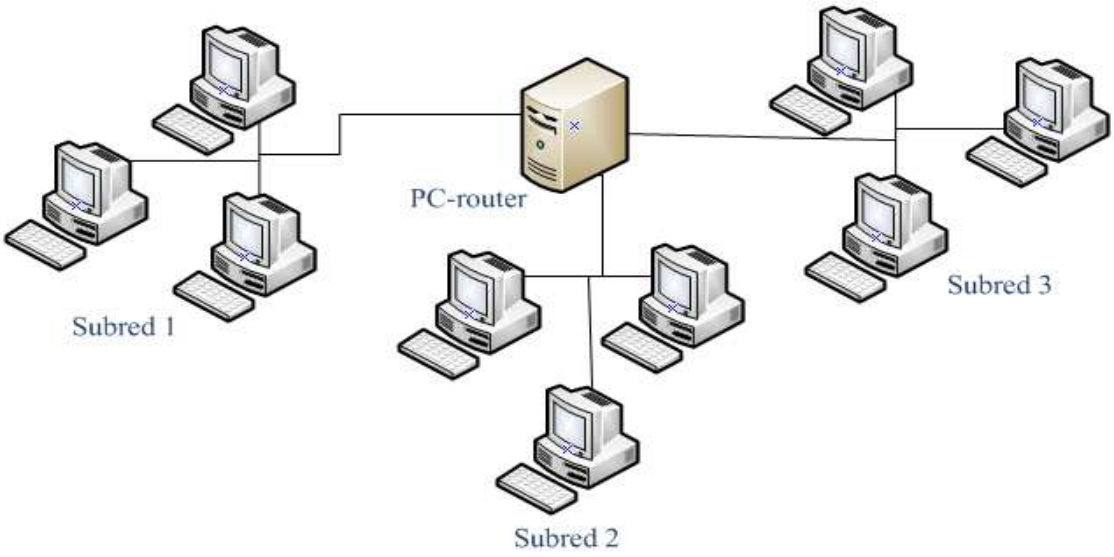

Figura1.10 Segmentación de una red por medio de un PC-router

Elaborada por el autor

El DMZ no es más que un diseño de red posible para constituir la defensa perimetral de la red. Como las capas de una cebolla, los niveles de seguridad y acceso a servicios y sistemas de información más seguros están en las zonas más profundas de la red donde los controles exigidos a los cortafuegos son muy estrictos.(Stallings, 2003)(Tanenbaum, 1997)(Segu-info)

1.6Modo deiniciar políticaspara seguridad.

Según (Orejuela, 2012) señala que habitualmentese asegura los derechos de acceso a los datos y recursos con los instrumentos de control y componentes de identificación. Estos componentesadmiten saber que los operarios o empleados de una organización, tengan sólo lasautorizaciones que se les facilitó.

La confianza en un sistema de información debe ser diseñada para noparalizar lalabor de los operadores. Por aquello, se debe integrar estándares y política de seguridad, como los siguientes objetivos:

- Crearnormas y procedimientos para cada prestación de la organización.
- Delimitar las operaciones a promover y preferir las personas a contactar en caso de descubrir una posible intromisión
- Capacitar a los operadores con lasdificultadesde riesgo en sistemas informáticos.

(Orejuela, 2012) Comenta al respecto, los derechos de acceso de los operadores deben ser determinados por los responsables jerárquicos y no por los directivos informáticos, los cuales tienen que lograr que los recursos y derechos de acceso sean relacionados con la actitud de seguridad determinada. Además, como el administrador es el único en conocer todo el sistema de la organización, tiene que comunicar a la directiva o gerencia cualquier problema e información valiosa sobre la seguridad, y siempre actualizarse en estrategias de seguridad y siempre socializando dicho conocimiento con los trabajadores de la organización.

1.7 Los riesgos de amenaza.

Tomando como referencia un estudio de (Belduma, 2013) a una institución educativa, se orienta que una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en el caso de los datos) y la descentralización por ejemplo mediante distribución de redes, en el caso de las comunicaciones. Estos fenómenos pueden ser causados por:

- **El usuario:** causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).
- **Programas maliciosos:**aplicaciones informáticas, destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el computador abriendo una puerta a intrusos o bien modificando los

datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía.

- **Un intruso:** persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (*cracker*, *defacer*, *script kiddie* o *Script boy*, *viruxer*, etc.).
- **Un siniestro** (robo, incendio, por agua): una mala manipulación o una mala intención derivan a la pérdida del material o de los archivos.
- **El personal interno de Sistemas:** Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

1.8 Técnicas de aseguramiento del sistema.

Según información en la web y cuyo autor es desconocido (http://seguridadeninternet-rosi.blogspot.com/) se indica que, entre las técnicas para asegurar el sistema se pueden mencionar las siguientes:

- **Codificar la información:** Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red.
- **Tecnologías repelentes o protectoras:** cortafuegos, sistema de detección de intrusos,*antispyware*, antivirus, llaves para protección de *software*, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

1.9 Consideraciones de software.

Tener instalado en la máquina únicamente el *software* necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el *software* pirata o sin garantías aumenta los riesgos). En todo caso un inventario de *software* proporciona un método correcto de asegurar la reinstalación en caso de

desastre. El *software* con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Hay*software* que son conocidos por la cantidad de agujeros de seguridad que introducen. Se pueden buscar alternativas que proporcionen iguales funcionalidades pero permitiendo una seguridad extra.

1.10 Consideraciones de red.

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de archivos desde discos, o de computadoras ajenas, así como portátiles. Por eso según el trabajo disponible en el link: http://seguridadeninternet-rosi.blogspot.com/. Se recomienda mantener al máximo el número de recursos de red sólo en modo lectura, esto impide que computadoras infectadas propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo. También se pueden centralizar los datos de forma que detectores de virus en modo *batch* puedan trabajar durante el tiempo inactivo de las máquinas. Además es importante controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.(Tanenbaum, 1997)(Security)

1.11 Conceptos erróneos acerca de la seguridad informática.

A continuación se detallan algunos conceptos erróneos acerca de los aspectos de la seguridad informática:

- Un sistema determinado no es importante para un *cracker*. Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una entidad no entraña riesgos pues ¿quién va a querer obtenerla información? Sin embargo, dado que los métodos de contagio se realizan por medio de programas automáticos, desde unas máquinas a otras, estos no distinguen buenos de malos,

interesantes de no interesantes, etc. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.

- No abrir archivos que se desconocen es seguro. Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.
- Tener un antivirus brinda completa seguridad. En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.
- Disponer de un cortafuegosprotege contra contagios. Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un cortafuegos) y otras de conexiones que se realizan (de las que no protegen). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los cortafuegos de aplicación (los más usados) no brindan protección suficiente contra el *spoofing*.
- Un servidor web cuyo sistema operativo es un unix actualizado es invulnerable. Puede que esté protegido contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web, tales como PHP(*Hypertext Preprocessor*), Perl, Cpanel, etc., está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra un *Shell* y por ende ejecutar comandos en unix.

1.12 Organismos oficiales de seguridad informática.

(Elías, 2010)en su trabajo “Resguardo de información” señala que, existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el CERT/CC (*Computer Emergency Response Team Coordination Center*) del SEI*(Software Engineering Institute)* de la *Carnegie Mellon University*, el cual es un centro de alerta y reacción frente a los ataques

informáticos, destinados a las entidades o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

1.13Aspectos primordiales a tener en cuenta para la seguridad.

Algunos aspectos importantes que se deben tener en cuenta en este campo son los siguientes:

Conoceralenemigo: Este punto se refiere a los atacantes y a los intrusos. Considera quien querría engañar la seguridad, mide e identifica las motivaciones. Determina lo que ellos querrán hacer y el daño que podrían causar a la red. Las medidas de seguridad nunca pueden hacer posible que un usuario realice tareas no autorizadas en el sistema.

Calcularelcosto: La seguridad puede demorar el trabajo, crear una costosa administración y gastos educacionales. Esta puede usar significativos recursos computacionales y requerir *hardware* especializado. Cuando se diseñan las medidas de seguridad se deben tener en cuenta los costos y los beneficios pese a este costo. Para ello, se tiene que entender los costos de las medidas y las probabilidades de brechas de seguridad. Si se incurre en que los costos de seguridad estén fuera de la proporción de los peligros reales, se estará haciendo un perjuicio.

Identificarlasasunciones: Todo sistema de seguridad tiene como base las asunciones. Por ejemplo, se podría asumir que la red no puede ser vulnerada, que los atacantes conocen menos que los que los que administran el sistema de seguridad, que están usando software estándares, o que un cuarto cerrado con llave está seguro. Hay que estar seguro de examinar y justificar las asunciones. Cualquier asunción oculta es un agujero potencial de seguridad.

Controlarlossecretos: La mayoría de los sistemas de seguridad se basan en secretos. Por ejemplo: contraseñas y claves encriptadas. Sin embargo frecuentemente los secretos no son tan “secretos”. Lo más importante para mantener secretos es conocer las áreas que se necesita proteger. Hay que saber que conocimiento permitiría a alguien engañar al sistema, para guardarlo celosamente y asumir que todo lo demás es conocido por los

adversarios. Los sistemas de seguridad deben diseñarse para que solo un número limitado de secretos necesiten ser guardados.

Factoreshumanos: Muchos sistemas de seguridad fallan porque los diseñadores no consideran como los usuarios reaccionarán a este. Si las medidas de seguridad interfieren con el uso esencial del sistema, esas medidas se resistirán y quizás se engañarán. Para ganar la complacencia, se debe asegurar que los usuarios pueden conseguir su trabajo hecho. Los usuarios deben entender y deben aceptar la necesidad de la seguridad. Algunas organizaciones llevan a cabo entrenamiento de seguridad de redes para sus usuarios; es decir, no se les permiten el acceso al Internet hasta que ellos hayan completado un programa de entrenamiento formal.

Conocerlasvulnerabilidadesdel sistema: Todo sistema de seguridad tiene vulnerabilidades. Hay que entender los puntos débiles del sistema y conocer como ellos pueden ser explotados. Se debe también conocer las áreas que presentan el peligro más grande y prevenir el acceso inmediatamente a ellas. Entender los puntos débiles es el primer paso para convertirlas en áreas seguras.

Limitar elalcance deacceso: Se deben crear las barreras apropiadas dentro del sistema para que si los intrusos acceden a una parte del mismo, no tengan el acceso automáticamente al resto del sistema. La seguridad de un sistema sólo es tan buena como el nivel de seguridad más débil de cualquier *host* en el sistema.

Entenderelentorno: Entendiendo cómo funciona normalmente el sistema, sabiendo lo que se espera y lo que es inesperado y estando familiarizado con cómo normalmente se usan los dispositivos instalados, ayuda a que se descubra los problemas de seguridad. Notar los eventos raros puede ayudar a capturar a los intrusos antes de que ellos puedan dañar el sistema. Las herramientas de auditoria pueden ayudar a que se descubran esos eventos raros.

Limitar laconfianza: Se debe saber con qué*software* se cuenta exactamente y se debe tener en cuenta en el sistema de seguridad que todo *software* no está libre de errores.

Recordarla seguridadfísica: El acceso físico a una computadora (o un encaminador) normalmente le da el mando total a un usuario suficientemente sofisticado sobre esa computadora. El acceso físico a un eslabón de la red normalmente le permite a una persona taladrar ese eslabón, lo bloquea, o inyecta el tráfico en él. No tiene ningún

sentido instalar un *software* de seguridad complejo mientras el acceso al *hardware* no se controla.

La seguridad espenetrante: Casi cualquier cambio que se hace en un sistema puede tener efectos de seguridad. Esto es especialmente verdad cuando nuevos servicios son creados. Administradores, programadores y usuarios deben considerar las implicaciones de seguridad de cada cambio que ellos hacen. Entender las implicaciones de seguridad de un cambio es algo que se aprende con la práctica. Exige una buena gana de explorar cada manera en que un servicio podría ser potencialmente manipulado.

1.14Estudio de los peligros principales.

Dos aspectos fundamentales en cuanto a riesgos son:

1. La identificación de los activos.
2. La identificación de las amenazas.

Identificación de los activos: Un paso importante en el análisis de riesgo, es identificar todo lo que se necesita proteger. Algunas cosas son obvias, pero algunas son pasadas por alto, tales como el personal que realmente usa el sistema. El punto esencial es listar todas las cosas que podrían afectarse por un problema de seguridad, por ejemplo:

El hardware: el CPU (*Central Processing Unit*, Unidad Central de Procesamiento), tarjetas, teclados, terminales, estaciones de trabajo, las computadoras personales, impresoras, discos, líneas de comunicación, servidores de terminales, ruteadores.

El software: programas fuentes, programas orientados a objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación.

Los datos: en ejecución, en línea, fuera de línea, salvas del sistema, *logs* de auditoria, bases de datos, en el tránsito sobre medios de comunicación.

Las personas: los usuarios, las personas que necesitan ejecutar sistemas.

La documentación: de los programas, *hardware*, los sistemas, los procedimientos de administrativos locales.

Los suministros: el papel, los formularios, las cintas, los medios de comunicación magnéticos

Identificación de las amenazas: Una vez que los recursos que requieren protección se identifican, es necesario identificar las amenazas a estos recursos. Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) según información en un trabajo sobre "tipos de ataques contra sistemas de información" y cuyo autor es desconocido, sugiere que, dada una circunstancia, 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 creador del sistema de seguridad especificar los servicios y componentes de seguridad necesarios. Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción:según información disponible en la web; http://cufminformaticos.blogspot.com/2011/02/clasificacion-y-tipos-de-ataques-contra.html, la interrupción es un recurso del sistema es derribado o se torna no disponible. Este es un embate contra la disponibilidad. Ejemplos de este ataque son la destrucción de un dispositivo*hardware*, como el disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Intercepción:un pirata informáticologra acceso a un recurso. Este es un ataque contra la confidencialidad. Se establece que puede ser una persona, un programa o un computador. Ejemplos de este ataque son "pinchar" una línea para hacerse con datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para descubrir la identidad de uno o más de los usuarios implicados en la comunicación observada ilegítimamente (intercepción de identidad)

Modificación: un pirata informático o *hacker* no ético, no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es el cambio de transacciones en un archivo de datos, alterar un programa para que actúe de forma desigual y altere el contenido de mensajes que están siendo transferidos por la red.

Fabricación:el hacker no ético, 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 en dos tipos de ataques.

1. Ataques pasivos: En los ataques pasivos el atracador no altera la comunicación, sino que únicamente la escucha o monitorea, 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:

- **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitoreados.
- **Control del volumen de tráfico** intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- **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.

2. Ataques activos: Estos ataques envuelven algún tipo de alteración del flujo de datos transferido o la creación de un artificial flujo de datos, la página en línea de delitos informáticos.com (http://delitosinformaticos.com/seguridad/clasificacion.shtml), en el tema, seguridad, clasifica en cuatro categorías los ataques contra sistemas de información:

- **Suplantación de identidad**: el hacker no ético, se hace pasar por una entidad diferente. Por ejemplo, sucesiones de autentificación 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.
- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar una cantidad repetidas veces en una cuenta dada.
- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa unacantidad determinada en la cuenta A" podría ser modificado para decir "Ingresa una cantidad determinada en la cuenta B".
- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o 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.A continuación se muestran en la figura 1.11, los tipos de ataques a una red de computadoras. (William & Cheswick, 1994)(ISO/IEC) (ups)

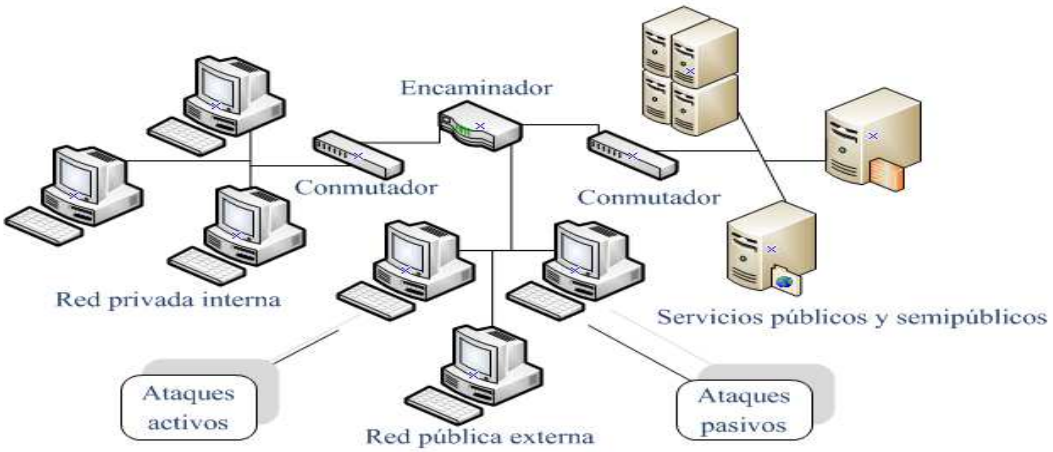

Figura1.11 Tipos de ataques a una red de computadoras

Elab**o**rada por el autor

1.15SGSI(Sistema de Gestión de la seguridad de la Información).

Un **SGSI** esun conjunto de políticas de administración de la información. El término es utilizado principalmente por la norma(ISO/IEC207001, s.f.).Se denomina en inglésISMS (*Information Security Management System*).El concepto clave de un SGSI es para una organización el diseño, la implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de la información y minimizando a la vez los riesgos de seguridad. Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo, adaptándose a los cambios internos de la organización así como a los externos del entorno.

PDCA (Plan-Do-Check-Act) o PHVA (Planificar-Hacer-Verificar-Actuar)

Las normas de seguridad de la información incorporan el típico PDCA o PHVA, el cual se muestra en la figura 1.12, siendo este un enfoque de mejora continua:

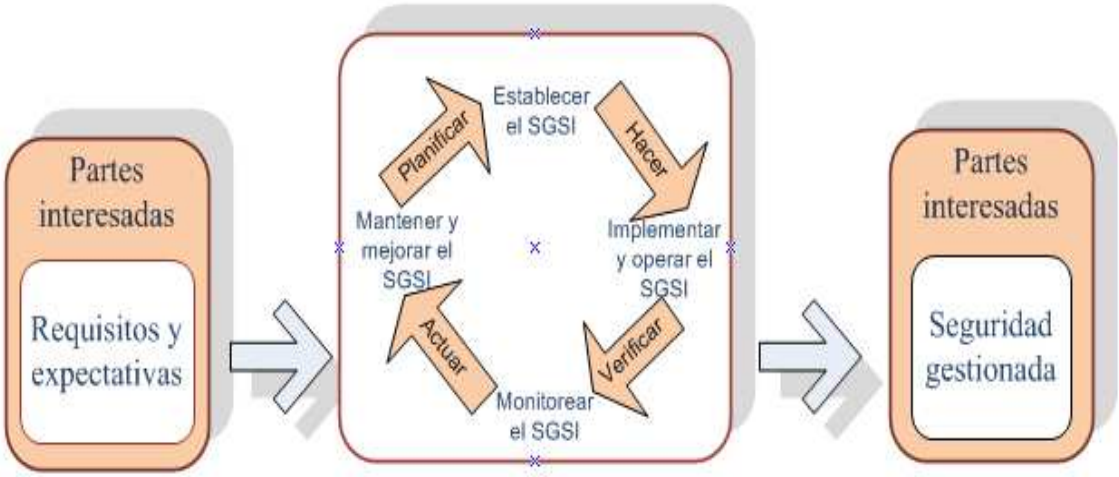

Figura 1.12 Ciclo del PHVA

Elaborada por el autor

- **Plan***(planificar)*: es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- **Do***(hacer)*: es una fase que envuelve la implantación y operación de los controles.

- **Check***(verificar)*: es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Act***(actuar)*: en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

La mejor definición del SGSI es descrito por la ISO/IEC 27001 y 27002y relaciona los estándares publicados por laISO (*International Organization for Standardization*, Organización Internacional de Normalización)y la IEC(*International Electrotechnical Commission*, Comisión Electrotécnica Internacional). (Ver anexo 2.) La documentación del SGSI se representa en la figura 1.13.

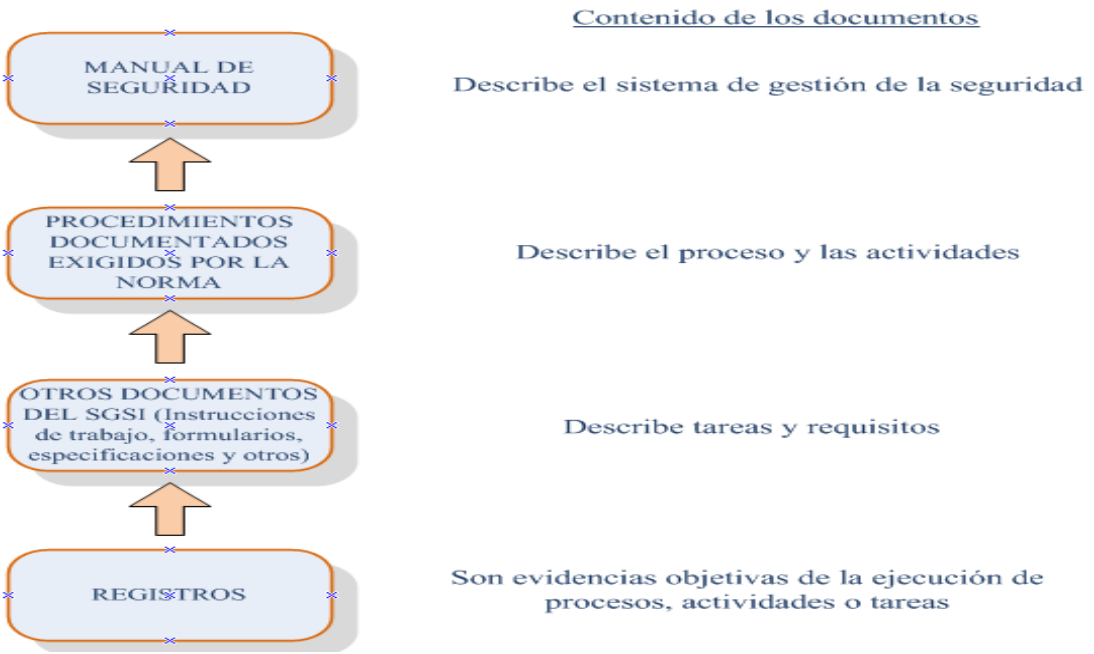

Figura 1.13 Documentación del SGSI

Elaborada por el autor

Otros SGSI: a continuación se mencionan otros SGSI:

SOGP: Otro SGSI que se empleainternacionalmente es SOGP (*Information Security Forum's Standard of Good Practice)*, el cual realiza "*best practice*" (las mejores prácticas), basado en las experiencias de implementación.

ISM3: *Information Security Management Maturity Model*o ISM-cubed, es otra forma de SGSI que está construido en estándares como ITIL (*Information Technology Infrastructure Library*, Biblioteca de Infraestructura de Tecnologías de Información), ISO 20000, ISO 9001, CMM (*Capability Maturity Model*, Modelo de Capacidad y Madurez), ISO/IEC 27001, e información general de conceptos de seguridad de los gobiernos ISM3 puede ser usado como plantilla para una ISO 9001,mientras que la ISO/IEC 27001 está basada en controles, ISM3 está basada en procesos e incluye métricas de proceso.

1.16 Seguridad de la información.

La **seguridad de la información** tiene como fin la protección de la misma y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada. El termino seguridad de lainformación, seguridad informática y garantía de la informaciónson usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger laConfidencialidad, Integridad y Disponibilidad de la información; Sin embargo entre ellos existen algunas diferencias sutiles que radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.La seguridad de la información se refiere a la Confidencialidad, Integridad y Disponibilidad de la información y datos, independientemente de la forma, los datos pueden ser: electrónicos, impresos, audio u otras formas.

Principios básicos: Los gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas, acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, la investigación y la situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes a otras computadoras.En caso de que la información confidencial de una empresa, sus usuarios, investigaciones, su estado actual o nueva línea de desarrollo caigan en manos indebidas,o se vuelva pública en forma no autorizada, podría causar la pérdida de credibilidad de sus investigaciones, pérdida de autenticidad, demandas legales o incluso el desplome de la misma.

Por lo que proteger la información confidencial es un requisito primordial, y en muchos casos también un imperativo ético y una obligación legal. Para el individuo común, la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. El campo de la seguridad de la información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad delaentidad, la ciencia forense digital y administración de sistemas de gestión de seguridad,entre otros.

Conceptos importantes: Por más de veinte años la seguridad de la información ha declarado que la CIA (Confidentiality, Integrity, Availability, Confidencialidad, Integridad y Disponibilidad) son los principios básicos de la seguridad de la información. La correcta gestión de la seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y del comerciante a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, una violación de la confidencialidad se ha producido.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras se tiene información confidencial en la pantalla, cuando se publica información privada, cuando una laptop con información sensible sobre una empresa es robada, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad: Para la seguridad de la información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas y no es lo mismo que

integridad referencial en bases de datos. La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.

Disponibilidad: La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad del sistema es el objetivo a seguir, estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema (SGSI). Garantizar la disponibilidad implica también la prevención de ataque odenegación de servicio.

Otros conceptos: a continuación se indican otros conceptos importantes:

Auditabilidad:permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Identificación:verificación de una entidad o cosa; reconocimiento.

Autenticación:proporcionar una prueba de identidad; puede ser algo que se sabe, que es, se tiene o una combinación de todas.

Autorización:lo que se permite cuando se ha otorgado acceso.

No repudio: no se puede negar un evento o una transacción.

Seguridad en capas:la defensa a profundidad que contenga la inestabilidad.

Control de Acceso: limitar el acceso autorizado solo a entidades autenticadas.

Métricas de seguridad ymonitoreo:medición de actividades de seguridad.

Gobierno:proporcionar control y dirección a las actividades.

Estrategia:los pasos que se requieren para alcanzar un objetivo.

Arquitectura:el diseño de la estructura y las relaciones de sus elementos.

Gerencia:vigilar las actividades para garantizar que se alcancen los objetivos.

Riesgo:la explosión de una vulnerabilidad por parte de una amenaza.

Exposiciones:áreas que son vulnerables a un impacto por parte de una amenaza.

Vulnerabilidades:deficiencias que se pueden convertir en amenazas.

Amenazas:cualquier acción o evento que puede ocasionar consecuencias adversas.

Riesgo residual:el riesgo que permanece después de que se han implementado medidas y controles.

Impacto:los resultados y consecuencias de que se materialice un riesgo.

Criticidad:la importancia que tiene un recurso para el negocio.

Sensibilidad:el nivel de impacto que tendría una divulgación no autorizada.

Análisis de impacto al sistema:evaluar los resultados y las consecuencias de la inestabilidad.

Controles: cualquier acción o proceso que se utiliza para mitigar el riesgo.

Contra medidas: cualquier acción o proceso que reduce la vulnerabilidad.

Políticas: declaración de alto nivel sobre la intención y la dirección de la dirección.

Ataques: tipo y naturaleza de inestabilidad en la seguridad.

Normas:establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

Clasificación de datos:el proceso de determinar la sensibilidad y criticidad de la información.

Tecnologías empleadas:

- Cortafuegos
- Administración de cuentas de usuarios
- Detección y prevención de intrusos
- Antivirus
- Infraestructura de llave publica

- SSL (*Secure Sockets Layer*, Capa de Conexión Segura)
- SSO (*Single Sign on*, Inicio de Sesión Único)
- Biometría
- Cifrado
- Cumplimiento de privacidad
- Acceso remoto
- Firma digital
- EDI (*Electronic Data Interchange*,Intercambio electrónico de Datos) y EFT (*Electronic. Funds Transfer*,Transferencia Electrónica de Fondos)
- VPN (*Virtual Private Network*,Red PrivadaVirtual)
- SET (*Secure Electronic Transaction*,Transacción Electrónica Segura)
- Informática Forense
- Recuperación de datos
- Tecnologías de monitoreo
- Estándares de seguridad de la información:

ISO/IEC 27000-series

ISO/IEC 27001

ISO/IEC 17799 actual ISO/IEC 27002

La figura 1.14 muestra un resumen del contenido de las normas ISO/IEC 27001 y 27002.

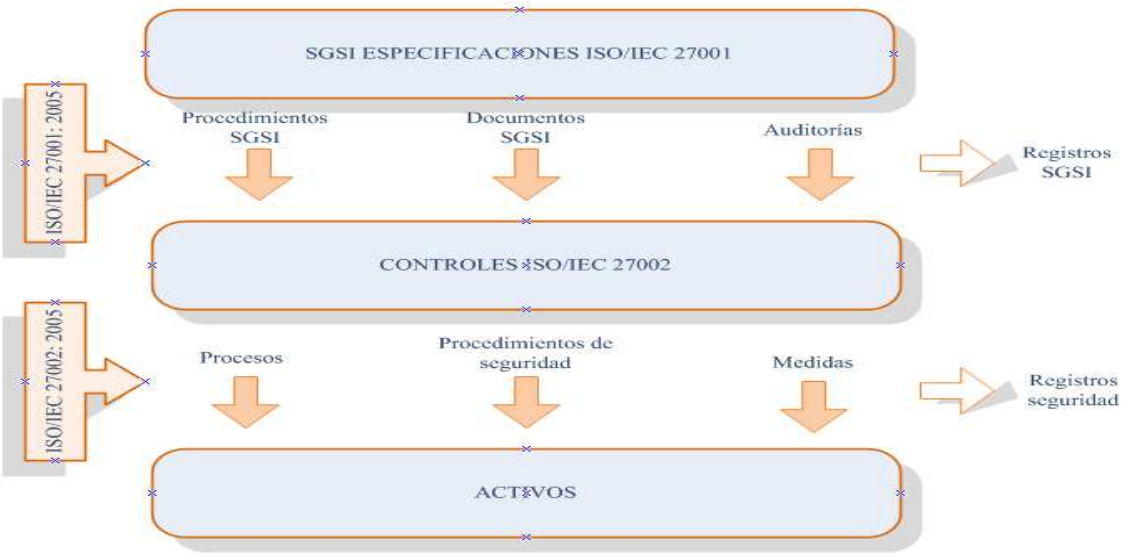

Figura1.14 Normas ISO/1EC 27001 y ISO/IEC 27002

Elaborada por el autor

Otros estándares relacionados:

- COBIT: *Control Objectives for Information and related Technology*, Objetivos de Control para Información y Tecnologías Relacionadas
- ISACA: *Information Systems Audit and Control Association*, Asociación de Auditoría y Control de Sistemas de Información
- ITIL:*Information Technology Infrastructure Library*, Biblioteca de Infraestructura de Tecnologías de Información.

Certificaciones:

- CISM: *Certified Information Security Manager*, Certificación para Administradores de Seguridad de la Información
- CISPP: Certified Information Systems Security Professional
- GIAC: Global Information Assurance Certification.
- Certificaciones independientes en seguridad de la información

- CISA- Certified Information Security Auditor, ISACA

- CISM- Certified Information Security Manager, ISACA
- Lead Auditor ISO27001- Lead Auditor ISO 27001, BSI (*British Standards Institution*)
- CISPP - Certified Information Systems Security Professional, ISC2 (*International Information Systems Security Certification Consortium*, Consorcio internacional de Certificación de Seguridad de Sistemas de Información)
- SECURITY++,COMPTia: Computing Technology Industry Association
- CEH - Certified Ethical Hacker
- PCI DSS - *Payment Card Industry Data Security Standard*, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

A modo de conclusión en este capítulo se tiene que:

- Como se analizó, la seguridad lógica y física, describen una serie de medidas internas y externas al ordenador que protegen a este y a su entorno de amenazas.
- Se evidencia que las medidas y políticas de seguridad a desarrollar en cualquier organización deben ser aspectos esenciales a conocer por todos los usuarios del sistema.
- La identificación de los activos y las amenazas que pudieran afectar a una determinada empresa permite conocer que se desea proteger y contribuye en el mantenimiento de la Confidencialidad, Integridad y Disponibilidad en la organización.
- La puesta en funcionamiento de un SGSI garantiza la ejecución de un conjunto de procesos que gestionen la accesibilidad de la información.

El siguiente capítulo se centrará en las Normas ISO/IEC 27000 (27001), sus generalidades, implantación, certificación y todos aquellos aspectos que en general permiten la caracterización de la norma indicada.

Capítulo 2. Normas ISO/IEC 27000 (27001).

En este capítulo se centrará la atención en las Normas ISO/IEC 27000 y en especial en su versión 27001.Esta es una serie de normas ISO/IEC 27000 que constituyen estándares de seguridad publicados por la ISO y la IEC. Esta serie de normas incluyen prácticas recomendadas para la Seguridad Informáticaque permiten el desarrollo, la implementación y el mantenimiento de lasespecificaciones para los SGSI.

2.1 Norma ISO/IEC 27001.

En el caso específico de la Norma ISO/IEC 27001(*Information technology - Security techniques - Information security management systems - Requirements*), puede afirmarse que es un estándar para la seguridad de la información que fue certificado y publicado en octubre de 2005 como estándar internacional por la ISO y por la IEC.

2.1.1 Introducción

El estándar para la seguridad de la información **ISO/IEC 27001,** como ya se indicó con anterioridadespecífica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI según el conocido “Ciclo de Deming”: PDCA, el cual fue analizado en el capítulo anterior. Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002.

2.1.2 Implantación

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a

estar sometida al SGSI elegido. En general, es recomendable la ayuda de consultores externos.Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001.

El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión.

2.1.3 Certificación

La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.Antes de la publicación del estándar ISO 27001, las organizaciones interesadas eran certificadas según el estándar británico BS 7799-2.Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su recertificación trienal, puesto que la certificación BS 7799-2 ha quedado reemplazada.El Anexo C de la norma muestra las correspondencias del SGSI con el Sistema de Gestión de la Calidad según ISO 9001:2000 y con el Sistema de Gestión Medio Ambiental según ISO 14001:2004, hasta el punto de poder llegar a certificar una organización en varias normas y en base a un sistema de gestión común.

(González, 2012) Indica que la información es un aspecto importante para el éxito y buen desempeño organizacional. Basado en la aportación de (ISO 27000, 2009) y la documentación en el link: http: //www.iso27000.es/download/doc_iso27000_all.pdf, se recomienda asegurarla información y los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para el adecuadocompromiso de la

seguridad de la información, es imperativoinstituir un sistema que enfrente esta tarea de unmodoordenado, que esté justificadaeinstaurada en unos objetivos concretosde seguridad y una valoración de riesgos y situaciones de peligro. La norma (ISO/IEC) 27000, es la acumulación de estándares perfeccionados o en fase de desarrollo por ISO e IEC, que suministran un cuadro de gestión de la seguridad de la información servible por una organización, pública o privada, grande o pequeña.

En el siguiente apartado se resumen las distintas normas que componen la serie ISO27000 y se indica cómo puede una organización implantar un SGSI basado en ISO 27001.

2.1.4 Origen

A partirde 1901, el BSI organización inglesa, es responsable de la divulgación de importantes políticas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS (*Occupational Health and Safety Assessment Series*, Sistemas de Gestión de Salud y Seguridad Laboral) 18001

(ISO 27000, 2009) Indica que, la norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica o no un conjunto de buenas prácticas para la gestión de la seguridad de su información. Un documento sin autor que trata sobre (ISO 27000, 2009) y que se puede descargar del link; www.freewebs.com/scc2008/ISO%2027000.doc, señala que laparteprimera, de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se funda un esquema de certificación. Es la segunda parte (BS 7799-2), divulgada en 1998, instituye las obligaciones de un SGSI para ser certificable por una entidad independiente.Las dos

partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión. La figura 2.1 refleja el período de evolución del estándar ISO/IEC 27001.En Marzo de 2006, consecutivamente a la divulgación de la (ISO/IEC207001) especificada en el 2005, la BSI divulgó la BS7799-3:2006, ajustada en la gestión del riesgo de los sistemas de información.(Certificación)(bsi).

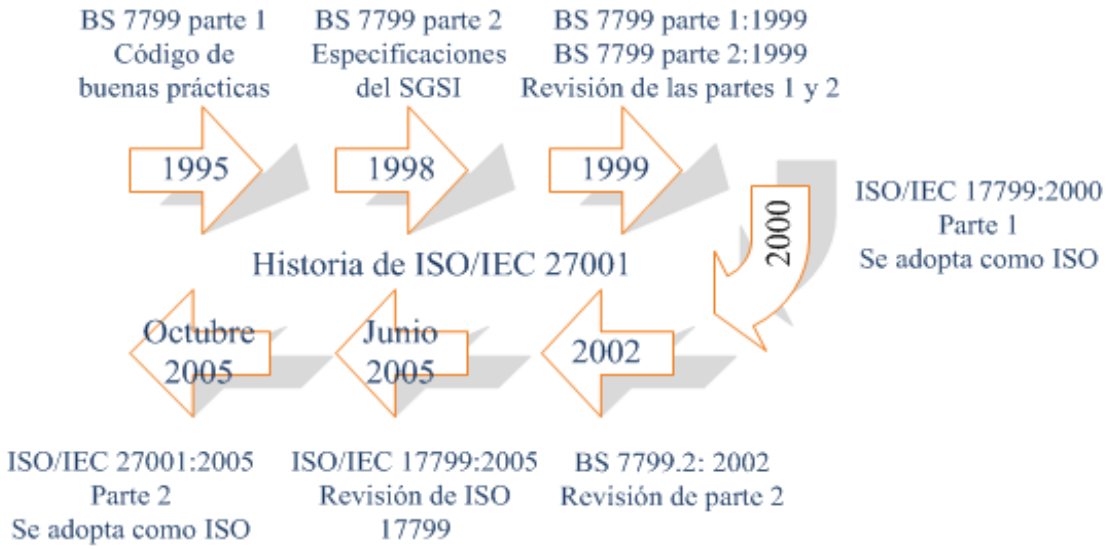

Figura2.1 Historia de ISO/IEC 27001

Fuente: (Certificación)

2.1.5 La especificación 27000

Según (Zambrano & Jannina Cerón, 2012) indican que asimilitud de otros estándares de la ISO, la especificación 27000 es verdaderamente una sucesión de patrones. Los niveles de notación reservados por ISO parten de 27000 a 27019 y de 27030 a 27044.

ISO 27000: En la etapapráctica; esta norma se publicó en el 2008. Comprende requisitos yaxiomas que se utilizan en 27000. La aplicación de cualquier estándar necesita de unaterminologíanotoriamenteespecífica, que impidadiferentes interpretaciones de concepciones técnicas y de gestión.

ISO 27001: Divulgada el 15 de octubre de 2005. Es elcriteriofundamental de la serie y contiene lasobligaciones del procedimiento de gestión de seguridad de la información. Se fundamenta en la BS 7799-2:2002 y es la política con ajustea certificación, por auditores externos (SGSI de las organizaciones). Reemplaza a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, detalla en sinopsis los objetivos de control eintervenciones que despliegaISO 27002:2005 (nueva notación de ISO 17799:2005 desde el 1 de Julio de 2007), para que esténescogidos por organizaciones en el progreso de sus SGSI; a pesar de no ser obligatoria la ejecución de todos los controles especificados en dicho anexo, la organización deberá refutartenazmente la no aplicabilidad de los revisiones no efectuados.

ISO 27002: Se referencia información el documento (ISO 27000, 2009) que también se encuentra en el link; http://www.slideshare.net/abc000123/doc-iso27000-all, A partir el 1 de julio de 2007, se denomina: ISO 17799:2005, conservando 2005 como año de edición. Detalla los objetivos de control eintervencionessugeridaspara seguridad de la información. No es certificable. Sujeta 39 objetivos de control y 133 controles, asociados en 11 dominios. Como se describió anteriormente, la ISO27001 define un anexo que resume los controles de ISO 27002:2005.

ISO 27003: En fase de puesta en práctica; se publicó enMayo de 2009. Se fundamentaen patrones de implementación de SGSI e información acerca del uso del modelo PDCA y de las exigencias de sus disparejasetapas. Tiene su principio en el anexo B de la norma BS7799-2 y en la serie de documentacionesdivulgadas por BSI.

ISO 27004: En fase de puesta en práctica; su fecha de publicación fuenoviembre de 2008. Define las métricas y las técnicas de medida adaptable para establecer la eficacia de un SGSI y de los controles afines. Estas métricas se empleanesencialmente para el cálculo de componentes de la etapa "*Do*" (Implementar y Utilizar) del período PDCA.

ISO 27005:la (ISO 27000, 2009) sobre este estándar indica que fue divulgada el 4 de junio de 2008. Esta especificación fundacriterios para la gestión del riesgo en la

seguridad de la información. Respaldaconcepciones generales descritas en ISO/IEC 27001 y está delineada para socorrer la diligencia satisfactoria de la seguridad de la información fundada en unaorientación de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR (*Technical Report*)13335-3:1998 y ISO/IEC TR 13335-4:2000.

ISO 27006: Divulgada el 13 de febrero de 2007. Según (Zambrano & Jannina Cerón, 2012)y la (ISO 27000, 2009) indican que, las obligaciones para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (*European Co-operation for Accreditation*, Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. En otras palabras, auxilia a descifrar los criterios de acreditación de ISO/IEC 17021 cuando se emplean a entidades de certificación de ISO 27001, pero no es una patrón de acreditación por sí misma.

ISO 27007: publicada enmayo de 2010. Consiste en una guía de auditoría de un SGSI.

ISO 27011: su fecha de publicación fue finales de 2008. Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (*International Telecommunication Union*,Unión Internacional de Telecomunicaciones).

ISO 27031: Se publicó enmayo de 2010. Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032: Publicada enfebrero de 2009. Consiste en una guía relativa a la ciberseguridad.

ISO 27033: Su fecha de publicación fue entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes

mediante *gateways*, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y remuneración de ISO 18028.

ISO 27034:según (ISO 27000, 2009), su fecha de publicación fuefebrero de 2009.Consiste en una guía de seguridad en aplicaciones.

ISO 27799: Publicada el 12 de junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. Define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma.

Además especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud.

Se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

2.2 Contenido

A continuación se detalla el contenido de (ISO 27000, 2009) reveladas:

2.2.1 ISO 27001:2005.

Esta información también es tomado del trabajo de (Lamilla & Patiño, 2009) y (Lema, 2013) en su presentación “ISO 38500 y 27000”.

Introducción:generalidades e introducción al método PDCA.

Objeto y campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.

Normas para consulta: otras normas que sirven de referencia.

Términos y definiciones: breve descripción de los términos más usados en la norma.

Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.

Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.

Auditorías internas del SGSI: cómo realizar las auditorías internas de control y cumplimiento.

Revisión del SGSI por la dirección: cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.

Mejora del SGSI: mejora continua, acciones correctivas y acciones preventivas.

Objetivos de control y controles: anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.

Relación con los principios de la OCDE: anexo informativo con la relación entre los apartados de la ISO 27001 y los principios de buenaadministración de la OCDE (Organización para la Cooperación y el Desarrollo Económicos).

Correspondencia con otras normas:según (Lema, 2013)el anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.

Bibliografía: normas y publicaciones de referencia.

2.2.2 ISO 27002:2005 (anterior ISO 17799:2005)

Introducción: conceptos generales de seguridad de la información y SGSI.

Campo de aplicación: se especifica el objetivo de la norma.

Términos y definiciones: breve descripción de los términos más usados en la norma.

Estructura del estándar: descripción de la estructura de la norma.

Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

Política de seguridad:documento de política de seguridad y su gestión.

Aspectos organizativos de la seguridad de la información: organización interna; terceros.

Gestión de activos: responsabilidad sobre los activos; clasificación de la información.

Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

Seguridad física y ambiental:áreas seguras; seguridad de los equipos.

Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

Gestión de incidentes de seguridad de la información:(Orejuela, 2012) detalla al respecto, que se debenotificar eventos y puntos frágiles de la seguridad de la información; gestión de sucesos de inseguridad de la información y mejoras.

Gestión de continuidad del negocio:son parámetros de la seguridad de la información en la gestión de la secuencia del negocio.

Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

Bibliografía*:*normas y publicaciones de referencia.

2.2.3 ISO 27005:2008

Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Preámbulo

Introducción

Referencias normativas

Términos y definiciones

Breve descripción de los términos más usados en la norma.

Estructura del estándar

Descripción de la estructura de la norma.

Fundamentos del proceso de gestión de riesgos ISRM (*Information Security and Risk Management Conference*)

Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

Establecimiento del contexto

Evaluación de riesgos ISRA (International Society for Research on Aggression)

Tratamiento de riesgos

Aceptación del riesgo

Comunicación del riesgo

Monitorización y revisión del riesgo

Anexo A: Definiendo el ámbito del proceso

Anexo B: Valoración de activos y evaluación de impacto

Anexo C: Ejemplos de amenazas más comunes

Anexo D: Vulnerabilidades y métodos de evaluación

Anexo E: Aproximación a ISRA

2.2.4 ISO 27006:2007

Esta norma referencia directamente a muchas cláusulas de ISO 17021 requisitos de entidades de auditoría y certificación de sistemas de gestión.

Preámbulo: presentación de las organizaciones ISO e IEC y sus actividades.

Introducción: antecedentes de ISO 27006 y guía de uso para la norma.

Campo de aplicación: a quién aplica este estándar.

Referencias normativas: otras normas que sirven de referencia.

Términos y definiciones: breve descripción de los términos más usados en la norma.

Principios: principios que rigen esta norma.

Requisitos generales: aspectos generales que deben cumplir las entidades de certificación de SGSIs.

Requisitos estructurales: estructura organizativa que deben tener las entidades de certificación de SGSIs.

Requisitos en cuanto a recursos: competencias requeridas para el personal de dirección, administración y auditoría de la entidad de certificación, así como para auditores externos, expertos técnicos externos y subcontratos.

Requisitos de información: información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre la entidad de certificación y sus clientes.

Requisitos del proceso: requisitos generales del proceso de certificación, auditoría inicial y certificación, auditorías de seguimiento, recertificación, auditorías especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.

Requisitos del sistema de gestión de entidades de certificación: opciones, opción 1 (requisitos del sistema de gestión de acuerdo con ISO 9001) y opción 2 (requisitos del sistema de gestión general).

Anexo A - Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector: potencial de riesgo de la organización (tabla orientativa) y categorías de riesgo de la seguridad de la información específicas del sector de actividad.

Anexo B - Áreas de ejemplo de competencia del auditor: consideraciones de competencia general y consideraciones de competencia específica (conocimiento de los controles del Anexo A de ISO 27001:2005 y conocimientos sobre SGSIs).

Anexo C - Tiempos de auditoría: introducción, procedimiento para determinar la duración de la auditoría y tabla de tiempos de auditoría (incluyendo comparativa con tiempos de auditoría de sistemas de calidad -ISO 9001- y medioambientales -ISO 14001).

Anexo D - Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005: tabla de apoyo para el auditor sobre cómo auditar los controles, sean organizativos o técnicos.

2.2.5 ISO 27799:2008

Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. Define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma:

Alcance

Referencias (Normativas)

Terminología

Simbología

Seguridad de la información sanitaria (Objetivos; Seguridad en el gobierno de la información; Información sanitara a proteger; Amenazas y vulnerabilidades)

Plan de acción práctico para implantar ISO 17799/27002 (Taxonomía; Acuerdo de la dirección; establecimiento, operación, mantenimiento y mejora de un SGSI; *Planning; Doing; Checking, Auditing)*

Implicaciones sanitarias de ISO 17799/27002 (Política de seguridad de la información; Organización; gestión de activos; RRHH (Recursos Humanos); Físicos; Comunicaciones; Accesos; Adquisición; Gestión de Incidentes; Continuidad de negocio; Cumplimiento legal)

Anexo A: Amenazas

Anexo B: Tareas y documentación de un SGSI

Anexo C: Beneficios potenciales y atributos de herramientas

Anexo D: Estándares relacionados

2.3 Beneficios del empleo del estándar ISO/IEC 27001.

(Veintimilla, Ramirez, Pita, & Quirumbay, 2014)En su trabajo académico “Relación entre COBIT y la norma 27001: un estudio comparativo”señalan el establecimiento de una metodología de gestión de la seguridad clara y estructurada.

Reducción del riesgo de pérdida, robo o corrupción de información.

Los usuarios tienen acceso a la información a través de medidas de seguridad.

Los riesgos y sus controles son continuamente revisados.

Confianza de usuarios y socios estratégicos por la garantía de calidad y confidencialidad en la red.

Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).

Continuidad de las operaciones necesarias delsistema tras incidentes de gravedad.

Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.

Imagen de institución a nivel internacional y elemento diferenciador de la calidad.

Confianza y reglas claras para las personas de la organización.

Reducción de costos y mejora de los procesos y servicios.

Aumento de la motivación y satisfacción del personal.

Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.(ISO/IEC207001)(bsi)

2.4 Puesta en práctica de un SGSI basado en ISO/IEC 27001.

En la figura 2.2 se representa una estructura general a seguir para la puesta en práctica de un SGSI, basado en el típico PHVA. Mientras que en la figura 2.3 se muestra el arranque del proyecto.

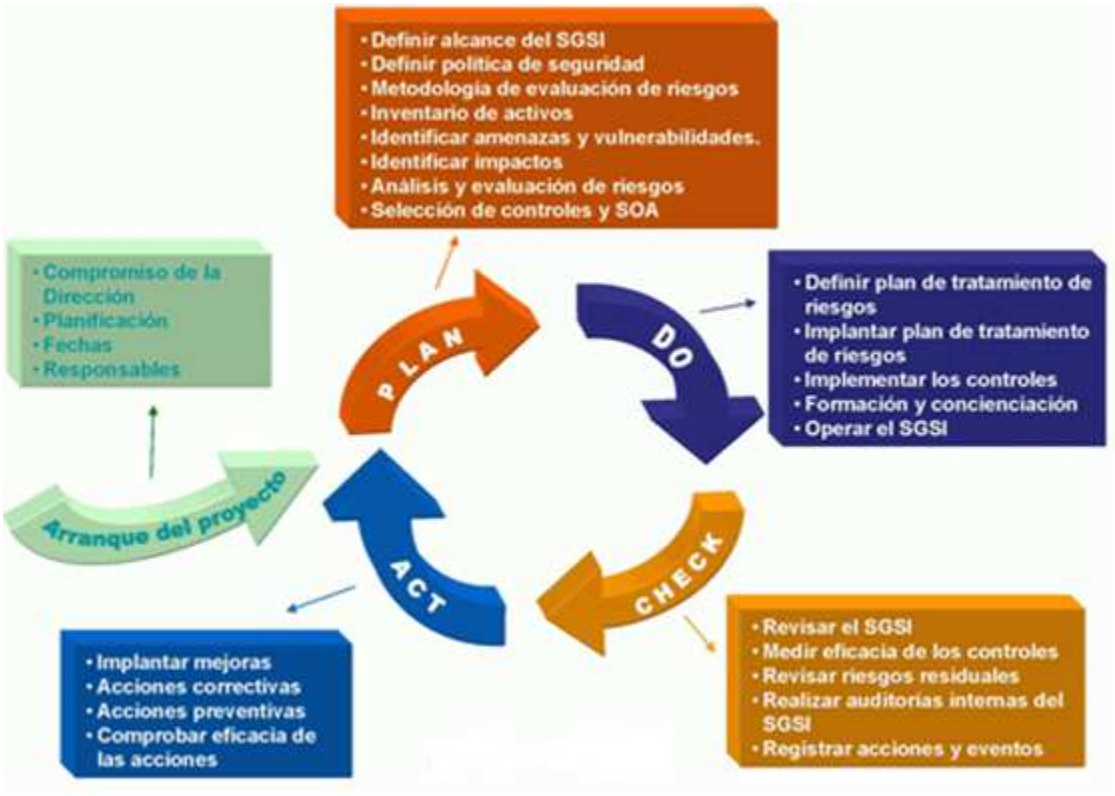

Figura2.2 Estructura general a seguir (¿Cómo adaptarse?)

Fuente: www.ISO27000.es

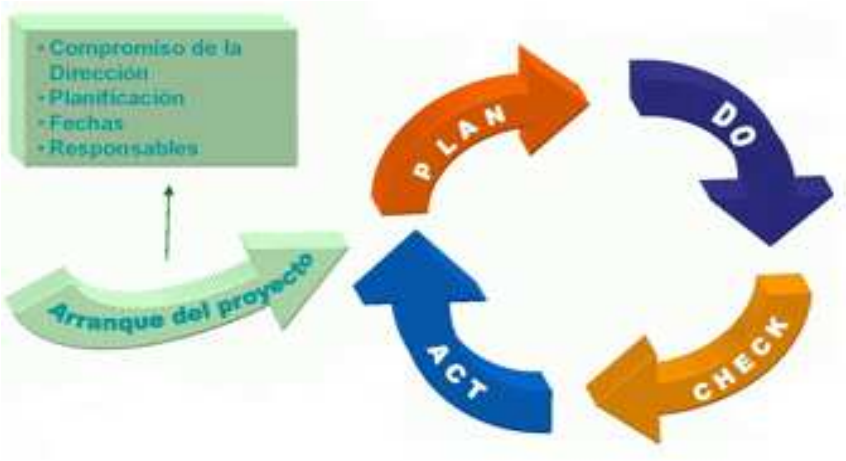

Figura 2.3 Arranque del proyecto

Fuente: www.ISO27000.es

Compromiso de la Dirección*:* una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la dirección. En la figura 2.4 se recogen los principales objetivos a seguir durante la etapa de planificación.

Figura 2.4 Planificación

Fuente: www.ISO27000.es

Planificación, fechas, responsables*:* como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

Definir alcance del SGSI: en función de características del sistema, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI, el cual no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.

Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, hay que tener en cuenta los requisitos delsistema, legales y contractuales en cuanto a seguridad, que esté alineada con la gestión de riesgo general, que establezca criterios de evaluación de riesgo y sea aprobada por la dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la dirección.

Definir el enfoque de evaluación de riesgos: definir un modo de análisis de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar poruna de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla, en el futuro, ISO 27005 proporcionará ayuda en este sentido.El riesgo nunca es totalmente eliminable, ni sería rentable hacerlo, por lo que es necesario definir una estrategia de aceptación de riesgo.

Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.

Identificar los impactos: los que podrían suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza utilice una vulnerabilidad) y la probabilidad de

ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

Identificar y evaluar opciones para el tratamiento del riesgo: el riesgopuede ser reducido (atenuado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato).

Selección de controles: seleccionar controles para el tratamiento del riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

Confeccionar una Declaración de Aplicabilidad: la denominada SOA *(Statement of Applicability)* es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A,de la norma excluido. En la figura 2.5 se observa la planificación e implementación de un SGSI sobre una determinada red.

Figura2. 5 Planificación e implementación de un SGSI.

Elaborada por el autor

La implementación es la segunda etapa a desarrollar dentro de un SGSI, siendo los parámetros que se recogen en la figura 2.6 los que se pongan en función.

Figura2.6 Implementación

Fuente: www.ISO27000.es

Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.

Implementar los controles: todos los que se seleccionaron en la fase anterior.

Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.

Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

La etapa de seguimiento, como muestra la figura 2.7 permite revisar y medir como se encuentra el SGSI.

Figura2.7 Seguimiento

Fuente: www.ISO27000.es

Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.

Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y *feedback* de todos los interesados.

Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.

Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos del sistema, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001,

el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

Revisar regularmente el SGSI por parte de la dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones. Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

La última etapa del SGSI implanta mejoras y comprueba la eficacia de las acciones emprendidas como se refleja en la figura 2.8.

Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

Acciones correctivas: para solucionar no conformidades detectadas.

Acciones preventivas: para prevenir potenciales no conformidades.

Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.

Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

Figura2.8 Mejora continua

Fuente: www.ISO27000.es

2.5 Aspectos claves de la norma.

Los siguientes aspectos son tomados del portal(ISO 27000, 2009), el cual establece los siguientes criterios:

- Responsabilidad y soporte de la dirección de la organización.
- Justificación de un alcance apropiado.
- Concienciación y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a la organización.
- Obligación de mejora constante.
- Establecimiento de políticas y normas.
- Integración del SGSI en la organización.
- La propuesta de esta norma no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos organizativos de la seguridad informática.

2.6 Factores de éxito.

Según el manual (ISO 27000, 2009)y (Lema, 2013)recomienda los siguientes aspectos:

- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

2.7 Riesgosen su implementación.

Exceso de tiempos de implantación: conlos consecuentes costos descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.

- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos informáticos.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

A continuación, la figura 2.9 muestra el seguimiento y la mejora continua de un SGSI sobre una determinada red de computadoras.

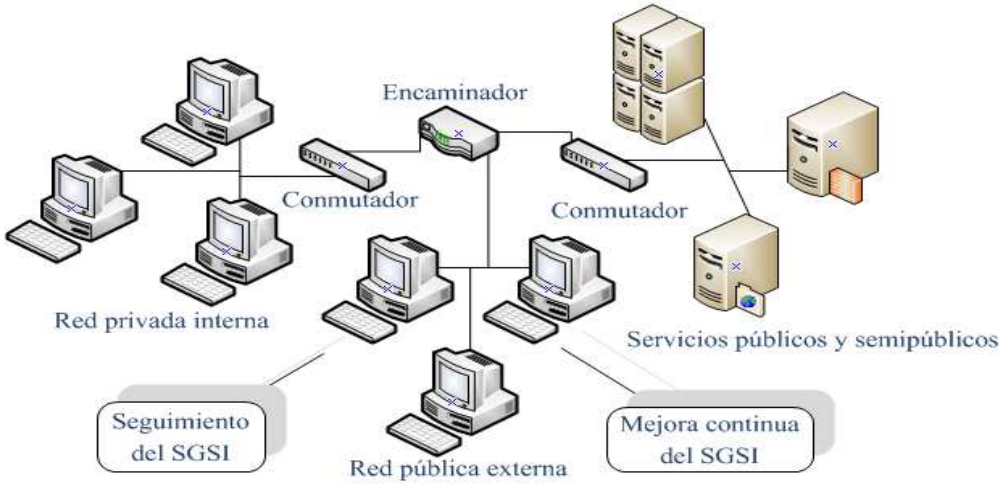

Figura2.9 Seguimiento y mejora continua de un SGSI

Elaborada por el autor

2.8 Medidas básicas a desplegar.

La (ISO 27000, 2009) indica que hay que mantener la simplicidad y limitarse a un alcance manejable y reducido: un lugar de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.

Percibir en detalle el proceso de creación: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; lograrhábito de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.

Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.

La autoridad y compromiso decidido de la dirección de la entidad incluso si al inicio el alcance se restringe a un alcance mínimoimpedirán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos esenciales de la norma.

La certificación como objetivo: aunque se puede lograr la conformidad con la norma sin certificarse, la certificación por un tercero cerciora un mejor rumbo, un objetivo más claro y tangible y, por lo tanto, excelentesiniciativas de conseguir el éxito.

No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.

Servirse de lo ya implementado: otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.

Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.(ISO/IEC207001)(bsi)

2.9 Opciones para el tratamiento de riesgos con ISO/IEC 27001.

Cuando los riesgos han sido identificados y evaluados, la organización debería identificar y evaluar la acción más apropiada para tratar los riesgos, lo que se conoce

como el Plan de Tratamiento de Riesgos (PTR), que es un documento o conjunto de ellos, de vital importancia para el SGSI. El objetivo fundamental es describir de forma bien clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, qué recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las posibles prioridades en la ejecución de las actualizaciones. Para el tratamiento del riesgo existen cuatro estrategias.

Reducción de riesgos: según el trabajo de (Lamilla & Patiño, 2009) recomiendan para los riesgos,la implementación deadecuados controles para reducir a niveles de aceptación previamente identificados por la entidad. Al identificar los controles a ser implantados es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como las vulnerabilidades y las amenazas previamente identificadas. Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando o recuperándose de ellos.
- La elección de cualquiera de estas maneras para controlar los riesgos dependerá de una serie de factores, tales como requerimientos específicos de la organización, el ambiente, y las circunstancias en que esta requiere operar.

Aceptación deriesgos: Es probable que a la organización se le presenten situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

En el caso de que no se pueda manejar el riesgo debido al costo de la implantación de los controles y las consecuencias son devastadoras para la entidad, se deben considerar las opciones de transferencia de riesgos o la de evitar los riesgos.

Transferencia de riesgos: La transferencia de riesgos, es una opción para la organización, cuando es muy difícil, tanto técnica como organizativamente para la entidad llevar los riesgos a un nivel aceptable. En estas circunstancias podría ser factible, transferir los riesgos a otras instituciones que pudieran ayudar. La transferencia de los riesgos por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuánto de estos riesgos están siendo transferidos. Otra posibilidad sería la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. En la medida en que la organización referida se encuentre preparada para asumir dicha responsabilidad. Lo que debe estar claro, es que al transferir servicios, el riesgo residual no se delega, sino que continúa siendo responsabilidad de la entidad.

Riesgosresiduales enel tratamientode riesgos: Una vez que las decisiones del tratamiento de riesgos han sido implementadas, siempre habrá riesgos residuales. Es necesario calcular cuánto las decisiones del tratamiento de riesgos ayudan a reducir los riesgos, y cuánto queda de riesgos residuales. Los riesgos residuales son definidos como aquellos riesgos que quedan en la organización después de haber implementado el plan de tratamiento de riesgos. El riesgo residual es muchas veces difícil de calcular, pero por lo menos un estimado debe ser determinado. En el caso de que el riesgo residual no fuera aceptable, una decisión administrativa debe ser tomada para resolver la situación. Una opción es la de identificar diferentes opciones de tratamiento del riesgos, incrementar los controles, o establecer arreglos con otras instituciones, para finalmente poder reducir los riesgos a un nivel aceptable. Es importante estar claros, que una buena práctica es la de no tolerar riesgos inaceptables, pero en algunas circunstancias, podría ser necesario tener que aceptarlos. Los riesgos residuales que son aceptados, deben ser documentados y aprobados por la dirección. Si la opción de tratamiento de riesgos no está demostrando eficacia en alcanzar los niveles deseados de riesgo, deben tomarse las acciones correctivas necesarias.

Evitar los riesgos: La opción de evitar los riesgos, describe cualquier acción donde las actividades de la organización, o las maneras de conducir la gestión de esta, se modifican, para así poder evitar la ocurrencia de algún riesgo.Las maneras habituales para implementar esta opción son:

- Dejar de conducir ciertas actividades.

- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

La decisión por la opción de *evitar los riesgos* debe ser balanceada contra las necesidades de la entidad.

2.10 Selección de controles para reducir los riesgos.

La norma ISO/IEC 27001 contiene un anexo A, que considera los controles de la norma ISO/IEC 17799 actual ISO/IEC 27002, para su posible aplicación en el SGSI que implemente cada organización.Para reducir los riesgos evaluados dentro del alcance del SGSI considerado resulta necesario implementar los controles de seguridad apropiados y justificados. Estos deben ser identificados y seleccionados.La selección de los controles debe ser sustentada por los resultados de la evaluación de riesgos. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y en qué forma debe tenerse. Cuando se seleccionan controles para su implementación, un número de factores deben ser considerados:

- Empleo de controles.
- Transparencia del usuario.
- Ayuda otorgada a los usuarios para desempeñar su función.
- Relativa fuerza de controles.
- Tipos de funciones desempeñadas.

2.11Compatibilidad entre las normas ISO/IEC 27001 e ISO/IEC 9001.

La norma ISO/IEC 27001 establece un modelo para implementar, operar, monitorear, revisar, mantener y mejorar un ISMS. La norma ISO/IEC 9001 define los requisitos para un Sistema de Gestión de la Calidad. Dado que la 27001 toma como modelo la

9001, ambas normas poseen 8 capítulos, nombrados de la misma forma, del primero (Objeto y campo de aplicación) hasta el octavo (Medición, Análisis y Mejora). Ambas se basan en la orientación a procesos. La ISO/IEC 27001 adopta una orientación a procesos para el ISMS y enfatiza la importancia de:

-Entender los requerimientos organizacionales para un ISMS.

-Implementar y operar controles para manejar riesgos.

-Monitorear y revisar la performance y efectividad del ISMS.

-Mejorar continuamente el ISMS basado en medidas por objetivos.

La ISO 9001 plantea el enfoque basado en procesos con el modelo Plan-Do-Check-Act o sea Planear, Realizar, Controlar y Actuar para mejorar, siendo el Plan responsabilidad de la dirección. Esto implica además realizar la gestión de recursos, controlar la realización de producto y actuar en base a la medición, análisis y mejora.En la 27001 se propone Establecer, Implementar, Operar, Monitorear y Revisar el ISMS y actuar manteniendo y mejorando el mismo.

Los Capítulos 2 y 3 son referencias normativas, términos y definiciones propias de cada campo de aplicación, es decir, la ISO 9000 para los Sistemas de Gestión de la Calidad en el caso de la 9001 y la 17799 para los Sistemas de Gestión de la Seguridad en el caso de la 27001, o sea, que las normas referenciadas son diferentes de acuerdo al sistema que se trate de implementar.

El Capítulo 4 en ambas normas es el referido a requisitos generales, donde si bien difiere el objeto del sistema a implementar, en ambos casos determina que la organización debe: establecer, documentar, implementar y mantener un sistema de gestión.Sin embargo, existen algunas diferencias en el contenido de los subtemas considerados. El 4.2 para la 9001 plantea requisitos de documentación en el caso de la 27001, éstos se encuentran en el subtema 4.3.

En el caso de la 27001 se desarrolla en el subtema 4.2 un detalle exhaustivo de cómo debe establecerse, implementarse y operarse el sistema, monitorearse y revisarse el Sistema de Gestión de la Seguridad de la Información, además cómo debe mantenerse y mejorar el mismo, es decir, si se compara los requisitos expuestos en el Capítulo 4 para la 9001 se puede decir que los requisitos generales son mucho menos detallados que en el caso de la 27001 y esto es razonable en virtud de que la 27001 es una aplicación específica y técnica del modelo de la 9001. En la 9001 se establece el Requerimiento del Manual de la Calidad en el subtema 4.2.2 que no está incluido en la 27001.

Sin embargo, se puede decir que está implícito el Manual de la Seguridad ya que en el punto 4.2.1 se establece la necesidad de definir una política, determinar, analizar y evaluar los riesgos, determinar el tratamiento de los riesgos seleccionando objetivos de control y controles adecuados y publicando un documento de aplicabilidad del sistema, es decir que finalmente existe documentado y publicado el equivalente a un Manual de la Seguridad de la Información, aunque no esté explícito en la norma.Los siguientes capítulos también difieren en su contenido no así en su espíritu. El quinto en ambos casos establece los requisitos de la responsabilidad de la dirección para establecer distintos sistemas de gestión.

En ambos casos existe un compromiso de la dirección claramente definido, la gestión de recursos de infraestructura y humanos que en la 9001 corresponde al Capítulo 6, la revisión por la dirección a partir de auditorías internas que en la 27001 se visualiza en el Capítulo 6, la revisión por la dirección que en la 27001 corresponde al capítulo 7.Como se había dicho, el Capítulo 6 de la 9001 se corresponde con la gestión de recursos, el capítulo 7 de la 9001 es específico de un Sistema de Gestión Productivo ya que establece los requisitos de diseño, compra y producción de bienes, por lo tanto, no tiene un capítulo equivalente en el 27001, que sólo es un sistema de operación y basado en información.

Finalmente, se puede ver que el Capítulo 8 es tanto en espíritu como en contenido similar en ambas normas y que trata de la mejora continua del sistema basado en acciones correctivas y preventivas.Como corolario se puede establecer que ambas

normas utilizan el mismo modelo de gestión basado en un sistema que se desagrega y relaciona procesos específicos, donde el objeto es diferente pero las actividades y responsabilidades son similares.

La norma ISO/IEC 27001 no solamente guarda relación con esta norma, sino también con otras como la UNE 71502 (Ver anexo 3).Seguidamente se muestra en la figura 2.10 el ciclo de seguridad basado en las normas ISO/IEC 27001 e ISO/IEC 9001.(ISO/IEC)

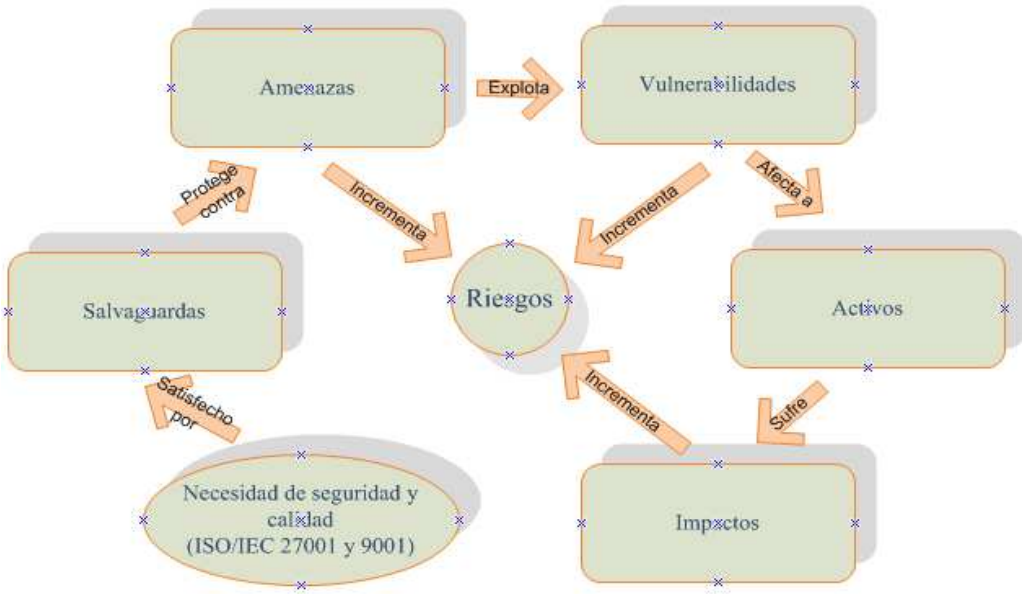

Figura 2.10 Ciclo de seguridad de la información y la calidad basado en ISO/IEC 27001 e ISO/IEC 9001

Fuente:(Certificación)

En este capítulo se obtuvieron las siguientes conclusiones:

La norma ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI.Como se expuso, su conformación en cuatro fases fundamentales (Panificar, Hacer Verificar y Actuar), según el Ciclo de Deming, permite desarrollar una metodología de gestión clara y estructurada y se observa que la revisión periódica de los controles que sean seleccionados e implementados reduce los riesgos de pérdida, robo o corrupción de la información. Debido a que la norma analizada se relaciona con otros estándares como el ISO/IEC 9001, y se adapta a las condiciones existentes en Ecuador, se pueden realizar varias certificaciones simultáneamente en una

misma organización de nuestro paíssiempre que esta cumpla con lo dispuesto en cada una de las normas.

El capítulo 3 se refiere al Plan de Seguridad Informática de una Entidad basado en ISO/IEC 27001, estableciendo los Módulos y Criticidad en la entidad, las diferentes fallas que se pueden presentar, el Sistema de Respaldos en la entidad y el Propuesta del Plan de Tratamiento de Riesgos.

Capítulo 3. Plan de Seguridad Informática de una empresa basado en ISO/IEC 27001.

En este capítulo se presentará de manera detallada el Plan de Seguridad Informática de una empresa basado en ISO/IEC 27001.

3.1 Introducción.

Con el análisis de la serie ISO/IEC 27000, profundizando en la norma ISO/IEC 27001, que se desarrolló durante el capítulo 2, se mostró como está estructurado dicho estándar y como ponerlo en función en un SGSI, lo cual permitiría realizarla prevención, detección y respuestas a incidentes, además de propiciar el mantenimiento y mejora continua de la organización. A partir de aquí, se pretende llevar a cabo durante este capítulo una posible implementación de la norma ISO/IEC 27001 en una empresa. Para ello se conformará el Plan de Seguridad Informática de la empresa a partir de un nuevo Plan de Contingencias, de Tratamiento de Riesgos y la selección e implementación de los controles necesarios de la norma mencionada, acordes a las exigencias de seguridad existentes en esa empresa. Resulta imprescindible argumentar que los controles a desarrollar junto con la gestión de riesgos son considerados como renglones esenciales dentro del plan a realizar, siendo mostrada esta última en las cuatro etapas del PHVA.

3.2 Propuesta del Plan de Contingencias.

Para la realización del Plan de Contingencias es necesario indicar que la prioridad de los módulos determinará el orden en el cual se deberán habilitar. En la tabla 3.1 se presentan los Módulos de la empresa y la criticidad de los mismos.

TABLA 3.1 Módulos y Criticidad en la entidad.

Elaborada por el autor

Módulo	Criticidad
Gerencia	Alta
Local de servidores	Alta
Laboratorios	Media
Departamentos	Media

A continuación se detallan los puntos a considerarse en el Plan de Contingencias así como los responsables de cada proceso. Se inicia este detalle con las fallas eléctricas mostradas en la Tabla 3.2.

TABLA 3.2 Falla eléctrica.

Elaborada por el autor

Contingencia	Falla eléctrica
Afecta a	Seguridad del edificio
Descripción	Corte del suministro eléctrico (horas)
Tiempo de falla (horas)	Indeterminado
Personal a ser informado	Administrador de la red de la empresa
Criticidad	Baja
Acciones	Informar al responsable de seguridad informática. Apagar y desconectar toda la tecnología informática. Conectar la tecnología luego de normalizada la situación.

Recomendaciones	Verificar el estado de la tecnología informática ante la contingencia. Contar con suministro de corriente eléctrica alternativa

La tabla 3.3 se refiere a la posibilidad de sufrir inundaciones

TABLA 3.3 Inundación.

Elaborada por el autor

Contingencia	Inundación
Afecta a	Seguridad del Edificio
Descripción	Los servidores de la empresa se encuentran ubicados en lugares donde una afectación por inundación es poco probable, aunque no se puede dejar pasar por alto esta contingencia, ya que pudiera suceder.
Tiempo de falla (horas)	Indeterminado
Criticidad	Alta
Personal a ser informado	Administrador de la red de la empresa Gerente
Acciones	Apagar el suministro de corriente eléctrica. Ubicar la posible causa de la inundación. Utilizar el último respaldo existente e importar la base de datos en el servidor de respaldo.

	Informar a los responsables de lo sucedido y comunicarles el tiempo aproximado que demorará el restablecimiento del servicio.
Recomendaciones	Proteger el local de servidores de todas las seguridades recomendadas para su operación como: Impermeabilizadores Protección de servidores Alarmas

A continuación, en la Tabla 3.4 se considera la posibilidad de incendio

TABLA 3.4 Incendio.

Elaborada por el autor

Contingencia	Incendio
Afecta a	Seguridad del Edificio
Descripción	El incendio puede iniciarse en instalaciones cercanas y propagarse a la empresa ocasionando graves daños.
Tiempo de falla (horas)	Indeterminado
Criticidad	Alta
Personal a ser informado	Administrador de la red de la empresa Gerente
Acciones	Utilizar el último respaldo existente e importar

	la base de datos en el servidor de respaldo. Informar a los responsables de lo sucedido. Protección de los equipos. Informar al cuerpo de bomberos.
Recomendaciones	Dotar al local de servidores como al edifico de detectores de humo. Dotar al local de servidores como al edificio de los debidos extintores de incendio.

La Tabla 3.5 se refiere a las pérdidas que se pueden presentar por hurto

TABLA 3.5Hurto.

Elaborada por el autor

Contingencia	Hurto
Afecta a	Integridad del Edificio
Descripción	Pérdidas totales o parciales de la tecnología informática de la empresa
Tiempo de falla (horas)	Indeterminado
Criticidad	Alta
Personal a ser informado	Administrador de la red de la empresa Gerente
Acciones	Verificar cuales fueron las tecnologías robadas. Informar a las autoridades.

	Esclarecer los hechos y erradicarlos. Restaurar la tecnología hurtada y los servicios.
Recomendaciones	Restringir el acceso a los laboratorios y local de servidores. El local de servidores debe permanecer debidamente cerrado. La llave solo debe tenerla la persona responsable del local y una copia el gerente. Establecer un sistema de vigilancia.

La Tabla 3.6 corresponde a los problemas a causa de virus informático.

TABLA 3.6 Virus Informático

Elaborada por el autor

Contingencia	Virus informático
Afecta a	Integridad de los datos de la entidad
Descripción	Pérdidas totales o parciales de la información o de los servicios brindados por la red de la empresa.
Tiempo de falla (horas)	Indeterminado
Criticidad	Alta
Personal a ser informado	Administrador de la red de la empresa Gerente
Acciones	Informar la suspensión de los servicios afectados por virus informáticos. Excluir a la máquina afectada de la red de

	datos. Ejecutar el software de antivirus en la máquina afectada. Eliminar los virus de los archivos contaminados. Informar a la empresa encargada de mantenimiento de equipos y soporte técnico sobre el particular Restablecer el servicio
Recomendaciones	Adquirir un software de antivirus, que sea capaz de revisar automáticamente a todas las estaciones de trabajo, según la última versión de base de datos (virus) liberada en Internet. El antivirus debe tener la facilidad de ser administrado a través de una consola central que permitirá monitorear el funcionamiento de todos los equipos de la red. Establecer políticas de uso y acceso de Internet. Definir políticas de seguridad de la información. Mantener una constante actualización del software de antivirus.

También es importante considerar los ataques internos como se lo indica en la Tabla 3.7

TABLA 3.7 Ataques internos.

Elaborada por el autor

Contingencia	Ataques internos

Afecta a	Integridad de los datos
Descripción	Pérdidas totales o parciales de la información de los servidores de datos o equipos del personal de la empresa.
Tiempo de falla (horas)	Indeterminado
Criticidad	Alta
Personal a ser informado	Administrador de la red de la empresa Gerente
Acciones	Informar el tiempo de suspensión del servicio a los usuarios de la red de la empresa, según sea el caso.Restaurar el último respaldo de la información de la base de datos. Restablecer el servicio e informar a los usuarios la fecha hasta la cual se recuperaron los datos.
Recomendaciones	Cumplir la política de respaldos. Las claves y contraseñas son personales, no deben ser transferidas o difundidas a otras personas, no deben ser colocadas en lugares visibles. Los usuarios son responsables de cada uno de sus contraseñas y claves, tanto para Windows como para otras aplicaciones.

3.2.1 Sistema deRespaldos enla empresa.

El objetivo del sistema de respaldos de la entidad es salvaguardar la integridad y seguridad de los datos de la misma, adoptándose las precauciones para su

almacenamiento y recuperación.Es necesario sacar respaldos de los servidores de bases de datos, del aplicativo en soportes electrónicos que luego pueden ser transportados a un local secundario para almacenar esta información, en caso de algún fallo en el local principal. Estos respaldos de los servidores deben ser diarios, la principal ventaja es que el costo de implementación es bajo pues únicamente se requiere sacar respaldos diarios de la información de los servidores e información importante de máquinas de usuarios o departamentos. Pero una de las desventajas es la dependencia del daño del local central pues si es un daño mayor no se va a poder realizar una reposición rápida de la información.

Es necesario que se realice de forma constante la revisión del plan y del proceso del planeamiento, aunque no es un substituto para probar el plan. La revisión del proceso es importante pues ayuda a asegurarse de que el plan es completo y de que han examinado a todas las áreas de la entidad en el proceso.Los respaldos son los medios más comunes para asegurar la disponibilidad de los datos en las computadoras. Es necesario que los usuarios mantengan un respaldo periódico de sus datos a fin de que puedan recuperar su información en caso de que se requiera una *contingencia*, los medios en los cuales los usuarios pueden sacar respaldos de su información son:

- Disquetes
- Memorias flash
- CD, DVD

Los respaldos de la información deben ejecutarse de forma automática a una hora y día específico cada semana en el servidor de Base de Datos de la entidad, o también de manera manual periódicamente.

Los programas ejecutables se deben respaldar una vez a la semana dentro de una carpeta que indique la fecha del mismo. Se debe mantener una copia de los discos de instalación de los programas no ejecutables y que se emplean en la entidad como son:

- Sistemas operativos (Windows 2003, Linux)
- Antivirus
- Programas profesionales con fines docente-educativos (Orcad, Proteus, Autocad, Matlab, etc.)

Los archivos de los respaldos de la base de datos y programas ejecutables o no, se deben guardar en un lugar seguro, fuera de la entidad, con un indicativo de la fecha y el contenido que poseen, a raíz de que puedan ser actualizados constantemente, o si sucede alguna contingencia se pueda contar con estos respaldos para ser empleados.En caso de suscitarse alguna contingencia que amerite el traslado del local de servidores a otro sitio, o algún otro local, todos los equipos del mismo serán debidamente protegidos e inspeccionados. Además previamente a ser empleado, una comisión debe inspeccionar las condiciones de seguridad del lugar y valorar si cumple con las exigencias imprescindibles para desempeñar la función a que será destinado.

3.3 Propuesta del Plan de Tratamiento de Riesgos.

A continuación se detalla la propuesta del plan de tratamiento de riesgos para una organización.

3.3.1 Método de análisis de riesgos en la entidad.

Se referencia un documento“Guía para el análisis de riesgos” encontrado en la web y cuyo autor corporativo es (MININT, 2011) y que está disponible en el link; http://calidad.egrem.co.cu/data/files//Documentos%20Externos/seguridad%%20y%2..
Para que una organización adquiera seguridad informáticaen sus sistema de red debeestablecer políticas y procedimientos que conforman la estrategia de cómo tratar los riesgos de seguridad, siendo estos aspectos definidos en la fase *Hacer* del PHVA. La base de este proceso a partir de un método radicaría en la realización de un análisis de riesgos basado en el estándar (ISO/IEC207001), el cual forma parte de la etapa *Planificar* del PHVA. Esto implicaría el análisis de cada uno de ellos y su

clasificaciónpor niveles. El (MININT, 2011) señala que a partir de la posibilidad de su ocurrencia y la severidad del impacto que puedan producir e incluye la toma de decisiones sobre la base de criterios de costo-beneficio con relación a las medidas a implementar para la protección de los activos de la entidad. De modo que, durante el diseño de un nuevo SGSI sería necesario tener en consideración la siguiente secuencia de acciones:

La (ISO 27000, 2009) recomienda:

- Establecer qué se trata de salvaguardar.
- Determinar de qué es necesario protegerse.
- Estipular cuan factibles son las amenazas.
- Implementar las medidas que protejan los activos informáticos de una manera rentable.
- Inspeccionarel proceso y corregirlo cada vez que una debilidad sea encontrada.

Los tres iniciales pasos son críticamente importantes para tomar disposicionesseguras sobre seguridad. Sin un discernimiento razonable de lo que se quiere proteger, contra qué se debe protegerlo y cuan probables son las amenazas, seguir adelante carecería de sentido.Teniendo en cuenta esto se pretende establecer un modo relativamente simple para la realización de las etapas fundamentales de un análisis de riesgos en el entorno informático de la empresa, que sirva de ayuda a quienes tienen la responsabilidad del diseño, implementación y mantenimiento del Sistemas de Gestión de la Seguridad de la Información en una institución, la cual hace uso de las tecnologías informáticas.

El término seguridad es usado en el sentido de minimizar las vulnerabilidades de los activos y recursos. Los activos son los elementos y bienes a proteger. Una vulnerabilidad es cualquier debilidad que pueda propiciar la violación del sistema o la información que éste contiene. Una amenaza es una potencial violación de la seguridad en la empresa. Los impactos son los daños producidos por la materialización de una amenaza y el riesgo es la posibilidad de que se produzca un impacto.

(ISO/IEC207001) Indica que el primer paso consiste en la identificación de los activos informáticos que necesitan ser protegidos. Una posible agrupación por categorías que puede ayudar a la identificación de los activos a proteger en la empresa, podría ser la siguiente:

- Hardware: computadoras personales, servidores y estaciones de trabajo, soportes magnéticos, líneas de comunicaciones, *módems, ruteadores*, concentradores, etc.
- Software: programas fuentes, programas ejecutables, programas de diagnóstico, utilitarios, sistemas operativos, programas de comunicaciones, etc.
- Datos: durante la ejecución, almacenados en discos, *backups*, bases de datos, rastros de auditoría, en tránsito por los medios de comunicaciones, etc.
- Personas: usuarios, operadores, personal de mantenimiento, etc.
- Documentación: de programas, de sistemas, de hardware, procedimientos de administración, etc.

Las Tablas 3.8 y 3.9 muestran una forma de relacionar los activos que componen el sistema informático, valorando su importancia a partir del papel que juegan dentro del mismo.La Tabla 3.8 se refiere a la Identificación de activos informáticos

TABLA 3.8 Identificación de activos informáticos.

Elaborada por el autor

No	Descripción	Tipo	Ubicación
1	2	3	4

Donde cada columna significa lo siguiente:

1. Número de orden consecutivo de los activos
2. Identificación del activo informático.
3. Tipo de activo.
    - HW: hardware

- SW : software
- DT : datos
- PR : personas
- DO : documentación

4. Ubicación del Activo Informático.

La Tabla 3.9 se refiere a la evaluación de los activos informáticos.

TABLA 3.9 Evaluaciónde los activos informáticos.

Elaborada por el autor

N	Do	Fn	Cost	Imag	Conf	Int	Disp	Val(Wi)
1	2	3	4	5	6	7	8	9

En cada una de las filas de esta tabla se relacionan los activos informáticos identificados en la Tabla 3.8 a fin de facilitar la evaluación de cada uno de ellos. El significado de cada una de las columnas es el siguiente:

1. Número: de orden consecutivo (se obtiene de la Tabla 3.8).
2. Dominio: Identificación para agrupar activos afines por las funciones que realizan. y/o por la administración sobre ellos. (D1, D2,...Dn según la cantidad que se cree).
3. Función: Importancia de la tarea que cumple el activo.
4. Costo:Valor y valor de uso del activo.
5. Imagen: Repercusión interna y/o externa que ocasionaría la pérdida del activo.
6. Confidencialidad: Necesidad de proteger la información que del activo se pueda obtener.
7. Integridad: Necesidad de que la información no se modifique o destruya.
8. Disponibilidad: Que los servicios que de los activos se esperan puedan ser obtenidos en todo momento de forma autorizada.

9. Valor (Wi): Importancia del activo.

La columna 9 (Wi) cuantifica la importancia de cada activo y se calcula por la media aritmética de los valores de la 3 a la 8, es decir, el resultado de la suma de éstas, dividido por 6.La suma total (Wt) de los valores (Wi) obtenidos en la columna 9 representa la importancia total de los activos informáticos que componen el sistema:

$Wt = W1 + W2 + ... + Wn$

Una vez que los activos que requieren protección son identificados y valorados según su importancia es necesario identificar las amenazas sobre estos activos y estimar la pérdida potencial (impacto) que puede producir su materialización.Por su origen las amenazas se clasifican en accidentales eintencionales, a partir de que su ocurrencia sea premeditada o no. Una amenaza intencional, si se materializa se considera una agresión o ataque. Por sus efectos o consecuencias las amenazas se clasifican en pasivasyactivas. Las amenazas pasivas son aquellas que de materializarse no implican ninguna modificación a la información contenida en el sistema ni cambios en el estado del mismo, por ejemplo fuga de información.

Las amenazas activas implican la alteración de la información contenida en el sistema o cambios en el estado del mismo, por ejemplo modificación no autorizada de una base de datos de la entidad.La Tabla 3.10 permite la realización de un análisis cruzado a partir de la identificación de las amenazas que pueden actuar sobre el sistema informático de la entidad y su incidencia sobre cada uno de los activos que componen el mismo.

En cada una de las filas de esta tabla se relacionan las amenazas, enumerándolas consecutivamente para su posterior identificación en la Tabla 3.11. Se abrirá una columna para cada activo identificado en la Tabla 3.8, marcando con una cruz en la fila correspondiente a cada amenaza que incida sobre él.

TABLA 3.10 Amenazas contra activos.

Elaborada por el autor

Activos

Amenazas		1	2	3
1				
2				
3				
M				

A partir de las amenazas identificadas en la Tabla 3.10 se cuantifica el riesgo de que cada una de ellas se materialice sobre cada uno de los activos, con ayuda de la Tabla 3.11.

TABLA 3.11 Estimación de riesgo sobre activo

Elaborada por el autor

No	Riesgos						
	Dom	R1	R2	Rn	Ri riesgo	Wi imp.	Ri * Wi peso
1	2	3	31	3n	4	5	6
2							
3							
N							

Las columnas 1 y 2 (Número de orden y Dominio) corresponden con las de la Tabla 3.9.

- Las columnas 3, 31,.....,3n reflejan la probabilidad de que se materialicen las amenazas identificadas en la Tabla 3.10 sobre cada activo, asignando valores entre 0 y 1.
- La columna 4 es la valoración del riesgo sobre cada activo. Se calcula a partir de la media aritmética de las columnas 3, 31,....,3n que tomaron valor, es decir, la suma de los valores de esas columnas entre la cantidad de columnas.
- La columna 5, Importancia del Activo, se obtiene de los valores estimados en la columna 9 de la Tabla 3.9.
- La columna 6, Peso del Riesgo sobre cada Activo, se obtiene como resultado de la multiplicación de los valores de las columnas 4 y 5.

El Riesgo Total del Sistema (WR) se puede obtener dividiendo la suma total de los valores de la columna 6 (Ri * Wi) por los de la columna 5 (Wi), en correspondencia con la siguiente expresión:

$$WR = \sum_{i=1}^{n} Ri * Wi \Big/ \sum_{i=1}^{n} Wi$$

De forma análoga se puede determinar el riesgo sobre un dominio dado. El riesgo residual (Wr) sería igual al riesgo total (WR) obtenido con este proceso luego de haber implementado las medidas de seguridad pertinentes. (ISO/IEC207001) indica que una vez que se ha determinado qué debe ser protegido y estimados los riesgos sobre los activos informáticos es necesario definir las políticas de seguridad que deben regir el funcionamiento del sistema informático y las medidas y procedimientos que hay que implementar para garantizar el cumplimiento de estas políticas.La definición de las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, junto a las medidas y procedimientos que permitan prevenir, detectar y responder a los riesgos reales del sistema informático conforman el Plan de Seguridad Informática de la empresa, que es el documento básico para la gestión de la seguridad informática en la entidad.(www.iso27000.es)A continuaciónse presenta un

ejemplo de un análisis de riesgos en la empresa. Se inicia con la Tabla 3.12 que corresponde a la identificación de activos informáticos en la institución.

TABLA 3.12 Identificación de activos informáticos en la empresa

Elaborada por el autor

No	Descripción	Tipo	Ubicación
1	Encaminador	HW	Local de servidores
2	Puente	HW	Local de servidores
3	Servidor	HW	Local de servidores

Con estos datos se realiza la evaluación de activos informáticos en la empresa en la Tabla 3.13.

TABLA 3.13 Evaluación de activos informáticos en la empresa

Elaborada por el autor

No	Dom	Func	Costo	Imagen	Confid	Integ	Dispon	Valor (Wi)
1	D1	8	6	8	4	5	5	6
2	D1	7	5	7	-	-	5	4
3	D1	8	8	10	8	10	10	9

Ahora se detallan las amenazas contra activos en la empresa en la Tabla 3.14

TABLA 3.14 Amenazas contra activos en la empresa

Elaborada por el autor

Activos

Amenazas		1	2	3
1	Acceso no autorizado	X	X	X
2	Pérdida de información			X
3	Destrucción de info.	X		X
4	Contaminación por virus			X

En la Tabla 3.15 se realiza la estimación de riesgos sobre los activos en la empresa.

TABLA 3.15 Estimación de riesgos sobre los activos en la empresa

Elaborada por el autor

No	Dom	Riesgos						
		R1	R2	R3	R4	Ri riesgo	Wi imp.	Ri * Wi peso
1	D1	0.8	-	0.6	-	0.7	6	4.2
2	D1	0.3	-	-	-	0.3	4	1.2
3	D1	0.8	0.8	0.8	0.8	0.8	9	7.2

Conociendo que: Debido a que:

$\sum_{1}^{3} Wi = 19$ y $\sum_{1}^{3} Ri * Wi = 12.6$ $Ri1= (R1+R3)/ 2 = 0.7$

$Ri2= R1/1= 0.3$

Ri3= (R1+R2+R3+R4)/4= 0.8

Entonces:

3 3

WR = Σ Ri * Wi/Σ Wi

1 1

WR = (4, 2+1, 2+7, 2)/ (6+4+9) = 12, 6/19 = 0, 66

Por lo tanto el riesgo total del sistema es de 0.66.

El Wr sería igual al WR existente luego de haber aplicado las medidas de seguridad. Este riesgo se pudiera obtener repitiendo el proceso mostrado anteriormente luego de haber aplicado dichas medidas. La figura 3.1 muestra los resultados del análisis de riesgos en la empresa.

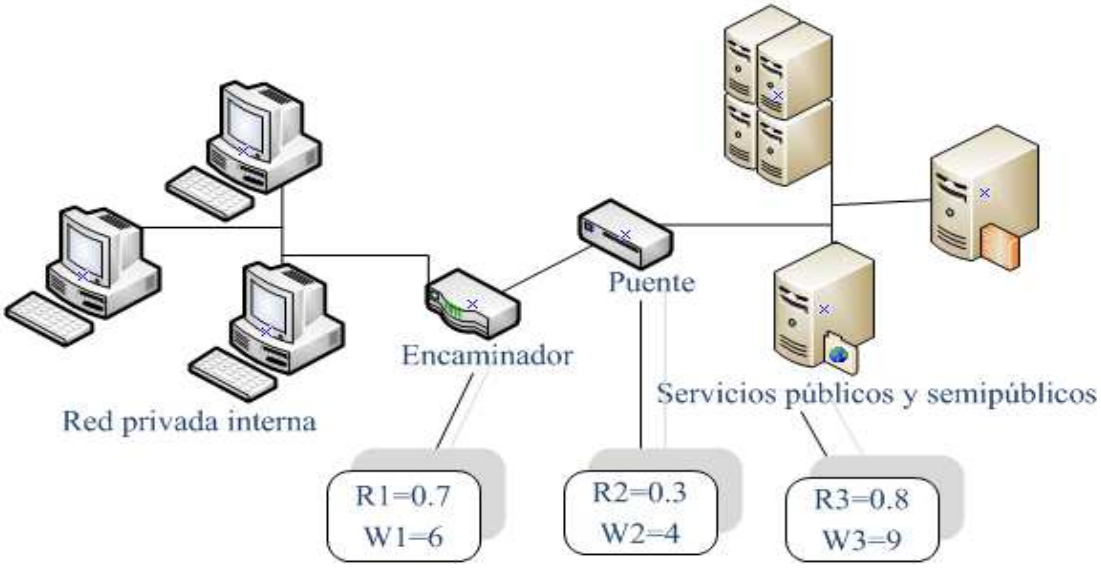

Figura 3.1 Resultados del análisis de riesgos en la empresa.

Elaborada por el autor

Es necesario señalar que:

WI = Importancia del activo i

Wt = W1 + W2 +..... + Wn = Importancia total de los activos del sistema.

Wi / Wt = Importancia relativa del activo i

Ri = Riesgo sobre el activo i

Wi*Ri = Peso del riesgo sobre el activo i

Ri*(Wi/Wt) = Peso relativo del riesgo sobre el activo i

$$WR = \sum_{i=1}^{n} Ri * Wi / Wt$$ = Riesgo total del sistema (suma de los pesos relativos)

= R1 * W1 / Wt + R2 * W2 / Wt +..... + Rn * Wn / Wt

= (R1*W1 + R2*W2 + ... + Rn*Wn) / (W1+W2+ .....Wn)

$$= \sum_{i=1}^{n} Ri * Wi / \sum_{i=1}^{n} Wi$$

3.3.2 Tratamiento de riesgos en la empresa.

El objetivo de este punto es tomar la acción más apropiada de tratamiento para cada uno de los riesgos que puedan ser identificados en la red de la entidad, en base alo

indicadoanteriormente donde se mostró un modo de análisis de riesgos compatible con la norma ISO/IEC 27001. La tabla 3.16 presenta el tratamiento de riesgos en la empresa.

TABLA 3.15 Tratamiento de riesgos

Elaborada por (Lamilla & Patiño, 2009)

Activos	Amenazas	Vulnerabilidades	PTR
Hardware portátil	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado	Falta de protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o falla en el aire acondicionado	Desempleo o mal funcionamiento de UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de	Falta de control de acceso	Reducción

	Software		
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los estudiantes	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte de los usuarios	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Copia de SW no autorizada o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
Estaciones de trabajo	Fuego	Falta de protección contra fuego	Reducción

	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado al equipo	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción

	Incumplimiento con Controles	Falta de conocimiento de seguridad	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Copia de SW no autorizada o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
Servidores de la entidad	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Corrupción de archivos de registros	Falta de Protección de los archivos de registro	Reducción

	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Acceso no autorizado a través de la red	Código malicioso desconocido	Reducción
	Degradación o Falla delHW	Falta de mantenimiento adecuado	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción

	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores	Reducción
	Ataque destructivo	Falta de protección física	Reducción
Equipos de oficina	Fuego	Falta de protección contrafuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación o Falla de HW	Falta de Mantenimiento	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Uso no previsto	Falta de Políticas Falta de Control de Acceso	Reducción
Soporte	Fuego	Falta de protección	Reducción

electrónico		contra fuego. (Miguel, 2013).	
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad	Aceptación
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de atención del personal	Reducción
	Escape de información	Manipulación inadecuada de información	Reducción
Documentación y registros	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los	Aceptación

		recursos son afectados por desastres	
	Pérdida de información	Errores de los usuarios Almacenamiento no protegido	Reducción
	Divulgación de información de clientes	Almacenamiento no protegido	Reducción
	Incumplimiento de leyes en cuanto a la información de visitantes o usuarios	Falta de conocimiento de los usuarios	Reducción
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema	Reducción
	Contratos incompletos	Falta de control para el establecimiento de contratos	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Incapacidad de	Falta de planes de continuidad	Reducción

	restauración	del negocio	
	Modificación no autorizada de información	Insuficiente entrenamiento de los usuarios	Reducción
Usuarios de la entidad	Errores de los usuarios y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Reducción
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de usuarios	Reducción
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad	Reducción
Establecimientos	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Acceso no autorizado	Falta de políticas Falta de protección física	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación

Servicios de comunicaciones de la empresa	Fuego	Falta de protección contrafuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación del servicio y equipos	Falta de mantenimiento adecuado	Reducción
	Errores de configuración	Falta de conocimiento del administrador	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Fallas de servicios telefonía	Falta de acuerdos bien definidos con terceras partes	Reducción
Servicio de energía eléctrica	Fuego	Falta de protección contra fuego	Reducción

	Daños por agua	Falta de protección física adecuada	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Ataque destructivo	Falta de protección física	Aceptación
Servicio de correo electrónico	Errores de los usuarios	Falta de conocimiento del uso del servicio	Reducción
	Suplantación de la identidad del usuario	Falta de control de acceso	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Fallas de servicios de soporte (servicios de Internet)	Falta de acuerdos bien definidos con terceras partes	Reducción

Suministros de oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Robo	Falta de atención Falta de protección física	Reducción
Imagen de la entidad(Reputación)	Divulgación de datos de los usuarios	Insuficiente seguridad de información de los .	Reducción
Paquetes o Software estándar	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Virus de Computación, Fuerza Bruta y ataques	Falta de Protección(AV) actualizada	Reducción
	Spoofing, Escape de información	Falta de control de acceso	Reducción
	Falta de capacidad	Falta de copias de seguridad	Reducción

	de restauración	continuas	
	Uso no previsto	Falta de políticas de seguridad	Reducción
Sistemas operativos	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Errores de Configuración	Falta de capacitación del administrador Incompleto o incorrecto documentación del sistema	Reducción
	Falta de capacidad de restauración	Falta de copias de seguridad continuas	Reducción
Medios y soportes	Acceso no autorizado a la información	Falta de control de acceso	Reducción
	Robo	Falta de protección física	Reducción
	Daños de cables	Falta de protección física	Aceptación
	Análisis de tráfico	Falta de establecimiento de conexión segura	Reducción

	Brechas de seguridad no detectadas	Falta de monitoreo de la red	Reducción

En el siguiente punto se describen los controlesseleccionados a implementar y emplear operacionalmente dentro del Plan de Seguridad Informática en base a la norma ISO/IEC 27001 en la entidad, los cuales se representan en la fase *Hacer* del PHVA.

3.4 Controles ISO/IEC 27001 a implementar.

Los controles de la norma en estudio que se van a implementar se describen a continuación:

3.4.1 Aseguramiento de nivel lógico.

Según (Cerini & Prá, 2012) en su trabajo de "Plan de Seguridad Informática", definen los siguientes aspectos en lo relativo al aseguramiento a nivel lógico, se tendrán en cuenta:

Identificación: Para facilitarel acceso a un usuario de la empresa al sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos:

- Identidad del usuario, corresponderá ser único e irrepetible.
- Su credencial de clave o *password*, debe ser único e ingresado por el usuario.
- Los nombres y apellidos, completos.
- Especificar el Grupo de usuarios al que corresponde.
- Fecha de anulación de la cuenta.
- Medidor de intentos fallidos.
- Definir fecha de vencimiento del *password*.

- Salvoconducto de ingreso al área de usuarios.

Convienenestablecer las autorizacionesmínimas y necesarias para que cada beneficiario de la organización desempeñe su labor. Corresponderálimitar la accesibilidad al sistema o manejo de recursos en un rango horario concreto, teniendo en cuenta que:

- Las cuentas de los usuarios no deben poder acceder al sistema en horarios determinados, de acuerdo al grupo al que pertenezcan.
- Durante el período no lectivo las cuentas de usuarios deben desactivarse.

La contraseña sindicada al acceso de un identificador de usuario a una computadora significa la primera verificación de su identidad, permitiendo posteriormente el acceso ala computadora y a la información que allí reside. Para su protección y de los recursos de la entidad debe mantener su contraseña de verificación de identidad en secreto, no compartirla con persona alguna (Ver anexo 5).

El administrador de la red obligará ejecutar unaverificacióncada mes a los usuarios del sistema, evidenciando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos. (Cerini & Prá, 2012)Además sugieren que en los computadores se instale un protector de pantalla con contraseña. Se debe bloquear el perfil de todo usuario que no haya accedido al sistema durante un período razonable de tiempo.Se deberá minimizar la generación y el uso de perfiles de usuario con determinados privilegios, los cuales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsables de laboratorios, de la administración, o de la seguridad de la red (Ver anexo 5).

Cuando un usuario de la empresa reciba una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta. La solicitud de una nueva cuenta o el cambio de privilegios deben ser hechos por escrito y debe ser debidamente aprobada (Ver anexo 4).

Contraseñas

Las reglas de contraseñas listadas a continuación están de acuerdo a los requerimientos y estándares internacionales.La contraseña de verificación de identidad no debe ser trivial o predecible, y debe cumplir los siguientes aspectos:

- Ser de al menos 8 caracteres de longitud.
- Contener una combinación de caracteres alfabéticos y no alfabéticos (números, signos de puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos.
- No contener su identificador de usuario como parte la contraseña.

Se recomienda bloquear el perfil de todo usuario que haya intentado acceder al sistema en forma fallida por más de cinco veces consecutivas (Ver anexo 5).

El usuario de la entidad debe poder modificar su *password* cuantas veces considere necesario, mediante un procedimiento formal de aviso. Las contraseñas predestinadas que traen los equipos nuevos tales como ruteadores, switches, etc., deben cambiarse seguidamente al ponerse en servicio el equipo en la empresa.Los usuarios no deben depositar su contraseña en una forma legible en archivos, en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser localizada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla prontamente.

3.4.2 Aseguramiento de la comunicación.

Dentro del ámbito de la seguridad de comunicaciones, se tomarán en consideración los siguientes aspectos:

Topologíadered

Debe existir una documentación detallada sobre los diagramas topológicos de la red de la entidad. Deben existir medios alternativos de transmisión en caso de que alguna contingencia afecte su medio primario de comunicación. Con relaciónalmanejo del correo electrónico corresponden,seguir un siguiente procedimiento propuesto por (Cerini & Prá, 2012):

- Guardar correos entrantes y salientes.
- Asunto del mensaje.
- Contenido del mensaje.
- Archivos anexos.
- Reporte de virus de cada parte del mensaje.
- Direcciones de máquina destino y fuente.
- Tamaño del mensaje.

Con respecto a la utilización de la red informática,(Lamilla & Patiño, 2009) indican que debe almacenarse datos sobre:

- Ancho de banda utilizado y cuellos de botella generados en el tráfico de red.
- Tráfico generado por las aplicaciones.
- Recursos de los servidores que utilizan las aplicaciones.
- El estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta).
- Intentos de intrusión.
- Uso de los protocolos.
- Solicitudes de impresión de datos de la empresa.

Todos los cambios en la red de la empresa, incluyendo la instalación de un nuevo software, el cambio de direcciones IP, la reconfiguración de conmutadores, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan

causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Conexionesexternas

La conectividad a Internet será otorgada para propósitos relacionados con la empresa. Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un cortafuego prohibiendo el paso de todo el tráfico que no se encuentre expresamente autorizado. El uso de Internet debe ser monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, la administración de la empresa debe revisar el contenido de las comunicaciones de Internet.

Correo

La (ISO 27000, 2009) señala que, deberá existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático. Todas las cuentas de correo quepertenezcan a la empresa deben estar gestionadas por una misma aplicación. Esta debe asociar una cuenta de correoa una computadora en particular de la red interna.El correo electrónico no debe ser utilizado para enviar cadenas de mensajes,no debe relacionarse con actividades ilegales y no éticas o para mensajes norelacionados con los propósitos de la empresa.Los datos que se consideraron “confidenciales” o “críticos” deben encriptarse.Debe existir un procedimiento de priorización de mensajes, de manera que loscorreos electrónicos de prioridad alta sean resguardados.Deberá asignarse una capacidad de almacenamiento fija para cada una de lascuentas de correo electrónico de los usuarios.

Antivirus

(Lamilla & Patiño, 2009) y la norma (ISO 27000, 2009) indican al respecto, todos los equipos de la entidad se debe instalar y correr un antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- Detectar y controlar cualquier acción intentada por un software viral en tiempo real.
- Periódicamente ejecutar el "*scanning*" para revisar y detectar software viral almacenado en la estación de trabajo.
- Hacer una revisión al menos diaria para actualizar la definición del software antivirus.
- Debe ser un producto totalmente legal (con licencia o Software libre).
- No deben usarse memorias flash u otros medios de almacenamiento en cualquier computadora de la facultad a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.

Mayor información sobre este tema se incluye en el anexo 5.

Cortafuegos

Deberá instalarse y correr un cortafuego para las estaciones de trabajo, el cual debe cumplir con los siguientes criterios básicos:

- Las redes detectadas deben ser tratadas como desconocidas y no confiables.
- Alertar a los usuarios ante nuevos programas solicitando acceso a la red.
- Impedir el acceso a sistemas no autorizados.
- Que el cortafuego tenga la versión más reciente disponible.
- Debe ser un producto totalmente legal (con licencia).

El cortafuego de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, habilitando los necesarios. El administrador de la red debe controlar periódicamente la configuración del cortafuego y los servicios de red, documentando los resultados de dichas pruebas.

3.4.3 Aseguramiento de aplicaciones.

En lo referente al aseguramiento de las aplicaciones, se tomarán en cuenta los siguientes aspectos:

Software

No debe utilizarse software bajado de Internet y en general aquel que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté autorizado su uso por la Dirección de la empresa.Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratis, a menos que haya sido previamente aprobado por el administrador de la red. Debe existir un responsable en cada área de la empresa, que responda por la información que se maneja en dicho sector. Debe definir la clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador de la red.

3.4.4 aseguramiento de nivel físico.

Las computadoras de la organización, sólo deben usarse en un ambiente seguro, es decir aquel en que se han implementado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles. Según el trabajo académico de (Candelario, Pinto, & Viteri, 2005) señalan que debe respetarse y no modificarse la

configuración de hardware y software establecida por la administración de la red. No se permite fumar, comer o beber mientras se está usando un computador.

Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua). Cualquier falla en las computadoras o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la entidad se requiere una autorización escrita.

La pérdida o robo de cualquier componente de hardware o software debe ser reportada inmediatamente (Ver anexo 5).

Control deaccesofísicoa laentidad

Se deberá asegurar que todos los individuos que entren a cadaárea se identifiquen y sean autenticados y autorizados para entrar. Deben existir custodios de seguridad en permanente monitorización, durante el horario laboral. Se deberán ubicar en el exterior. Los servidores de red y los equipos de comunicación (conmutadores, enrutadores, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

Dispositivosdesoporte

Deberán existir los siguientes dispositivos de soporte en la empresa:

- Aire acondicionado:en el local de servidores, laboratorios y departamentos la temperatura debe mantenerse entre 19º C y 20º C.
- Extintores: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación,

deberán estar instalados en lugares estratégicos de la entidad, el local de servidores deberá tener uno propio.

- Alarmas contra intrusos: deberán contar con una alarma que se active en horarios no laborables. Esta deberá poder activarse manualmente en horarios laborales ante una emergencia.
- UPS: (*Uninterruptible power supply*) deberá existir al menos uno de estos equipos en el local de servidores con tiempo suficiente para que se apaguen de forma segura yautomática ante una contingencia.

Todos estos dispositivos deberán ser evaluados periódicamente por los responsables de mantenimiento.

Cableadoestructurado

Se deberá documentar en planos los canales de tendidos de cables y las bocas de red existentes en la entidad. Deberá medirse periódicamente el nivel de ancho de banda de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias. Ante un corte del suministro de energía eléctrica deberán apagarse todos los equipos de forma segura, como medida de prevención.

3.4.5 La gestión de la red de la entidad.

El equipo de gestión de la red universitaria debe hacer énfasis en la concienciación de todos los usuarios, generando una cultura de la seguridad, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debe ser renovado y transmitido a los usuarios en forma anual. Los usuarios solicitarán asesoramiento o servicios al administrador de la red a través de mensajes, de manera que se genere un registro de los trabajos efectuados por el equipo de administración y de las solicitudes de los usuarios de la entidad. (Ver anexos 4 y 5)

Capacitación

Se debe obtener un compromiso firmado por parte de los usuarios respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas a los implicados. Asegurar que los usuarios reciban capacitación continua para desarrollar y mantener sus conocimientos mediante competencias, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz (Ver anexo 4).

Respaldos

Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la empresa, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas. Se deberá hacer una copia de respaldo de toda la documentación del local de servidores, incluyendo el hardware y el software, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento (Ver anexo 5).

Documentación

Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales, así como asignarse un responsable a cargo de la gestión de la documentación en la empresa y existir un registro de los eventos, errores y problemas del hardware y el software

utilizados en las operaciones de procesamiento de datos. Deberán existir además una documentación y un registro de las actividades del local de servidores (procesos normales, eventuales y excepcionales) que se desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.

Revisióndelsistema

La entidad debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad de forma de asegurar la integridad, exactitud y disponibilidad de la información. Para ello deben existir:

- Herramientas que registren todos los eventos relacionados con la seguridad de la información procesada en la red de la empresa.
- Herramientas que analizan los registros generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.
- Procedimientos de revisión de los eventos registrados, a cargo de un responsable designado por el administrador, de forma de detectar anomalías y tomar las acciones correctivas necesarias.

Se deberán registrar, mediante esquemas de auditoria, aquellos eventos relacionados con la seguridad de la información (Ver anexo 1). Dichos registros deberán contener como mínimo:

- Fecha y hora del evento,
- Fuente (el componente que ocasionó el evento),
- Identificador del evento (número único que identifica el evento),
- Equipo (máquina donde se generó el evento),
- Usuario involucrado,
- Descripción (acción efectuada y datos asociados con el evento).

Se deberán analizar periódicamente los siguientes eventos específicos como mínimo:

- Controles de acceso y permisos de los usuarios,
- Uso de recursos informáticos,
- Intentos fallidos de ingreso al sistema.

3.4.6 Seguridad física y del entorno.

La seguridad física en la empresa debe estar implementada en un modelo de defensa por capas, los controles físicos deben trabajar juntos en la arquitectura, es decir, si una capa falla, otras capas protegerán los recursos de la organización. Las capas están implementadas dentro del perímetro. Por ejemplo: se tendrá una cerca, guardias de seguridad, paredes y cerraduras en el caso de laboratorios, departamentos, local de servidores y de cableado. Esta serie de capas protegerán los recursos más sensibles.La seguridad necesita proteger todos los recursos de la empresa, incluyendo personas y hardware. La seguridad debe fortalecer la eficiencia ya que provee un ambiente seguro.

Esto permite a los usuarios enfocarse en sus tareas, en lo posible no permitir que la seguridad física se transforme en un hueco de seguridad informática.Las vulnerabilidades con respecto a la seguridad física tienen relación con la destrucción física, intrusos, problemas del ambiente y los usuarios que han perdido sus privilegios causen daños inesperados de datos o sistemas.

Revisióndelsistema

Los controles de acceso físico tendrán las siguientes características:

- Supervisar a los visitantes de la empresa y registrar la fecha y horario de su ingreso y egreso, esta tarea será realizada por el guardia de seguridad. Sólo se permitirá el acceso mediando propósitos específicos y autorizados.
- Implementar el uso de una identificación unívoca visible para todo el personal delaempresa e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

Seguridadde departamentos,local de servidoresy laboratorios

El Gerente es el encargado de asignar las funciones relativas a la Seguridad Informática de la empresa al administrador de la red, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo junto al resto del equipo de administracióny los técnicos de laboratorios las funciones relativas a la seguridad de los sistemas de información de la entidad, las cuales deben incluir la supervisión de todos los aspectos inherentes a la seguridad informática tratados en este trabajo.Seguidamente se definen los siguientes sitios como áreas protegidas de la empresa para lo cual se consideró el tipo de información manejada por cada área, las mismas que se presentan en la Tabla 3.17.

TABLA 3.17Áreas protegidas de la empresa.

Elaborada por el autor

Áreas protegidas
Local de servidores
Decanato
Departamentos
Laboratorios

Se establecen las siguientes medidas de protección para las áreas protegidas:

- Ubicar la información crítica en lugares a los cuales no pueda acceder personal no autorizado.
- Ubicar las funciones y el equipamiento de soporte, por ejemplo: computadoras, conmutadores, adecuadamente dentro del área protegida para evitar solicitudes de acceso, lo cual podría comprometer la información.
- Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.
- Restringir el acceso público a los locales protegidoslo cual permita evitar cualquier incidente de seguridad.
- Almacenar la información de resguardo en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

Mantenimientode equipos

Se realizará el mantenimiento del equipamiento de la entidad para asegurar su disponibilidad e integridad permanentemente. Para ello se debe considerar:

- Someter el equipamiento a tareas de mantenimiento preventivo, el responsable del área informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

A continuación se indica el período aconsejable para realizar los mantenimientos en los equipos de la red de la entidad, el cual se presenta en la Tabla 3.18.

TABLA 3.18 Período de mantenimiento en los equipos de la empresa.

Elaborada por el autor

Equipo	Frecuencia de mantenimiento	Personal responsable
Servidores	4 meses	Administrador de red
Estaciones de trabajo	6 meses	Administrador de red
soportes	6 meses	Administrador de red
Encaminadores y conmutadores	12 meses	Administrador de red

3.4.7 Acciones de cambios operacionales.

El administrador de la red será el encargado de implementar los cambios operacionales y de comunicaciones; previo a una justificación que explique las razones y cómo mejorará en la eficiencia y calidad en la red de la empresa. Este procedimiento de control de cambios contemplarán los siguientes puntos:

- Identificación y registro de cambios significativos.
- Evaluación del posible impacto de dichos cambios.
- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambio.
- Prueba del nuevo escenario.
- Comunicación de detalles de cambios a todas las personas pertinentes.
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Planificacióndelsistema

El equipo de administración de la red de la empresa, encabezado por su administrador debe efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación tomando en cuenta los nuevos requerimientos de los sistemas y proyectar las futuras demandas, para garantizar un procesamiento y almacenamiento adecuados. Para lo cual, debe recopilar información previa de los requerimientos de software y hardware en la organización.

Aceptacióndelsistema

Para la aprobación del sistema se deben considerar los siguientes puntos:

- Verificar si la capacidad de las computadoras está acorde con los requerimientos actuales y futuras proyecciones.
- Garantizar la recuperación ante errores.
- Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
- Garantizar la implementación de un conjunto acordado de controles de seguridad.
- Asegurar que la instalación un nuevo sistema no afecte negativamente los sistemas existentes, especialmente en los períodos pico de conexión.

Medidasde red

El equipo de administración de la red de la empresa debe definir medidas para garantizar la seguridad de los datos contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

- Establecer medidas especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos.
- Implementación de acciones para mantener la disponibilidad de los servicios de red y computadoras conectadas en la empresa.
- Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

Gestiónde medios removibles

Se deberán considerar las siguientes acciones para la administración de los medios informáticos removibles de la empresa:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la empresa.
- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

3.4.8 Política para el uso de servicios en la red.

Las conexiones no seguras a los servicios de red pueden afectar la seguridad de toda la empresa, por lo tanto, se debe controlar estrictamente el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a la red y a sus servicios, no comprometan la seguridad de los mismos. El administrador de la red es el responsable de otorgar los permisos tanto a servicios como recursos de la red, únicamente de acuerdo al pedido formal del responsable de cada local. Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información. Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a la red, los cuales comprenderán:

- Identificar la red y servicios de red a los cuales se permite el acceso.

- Realizar normas y procedimientos de autorización para determinar las personas y la red y servicios de red a los cuales se les otorgará el acceso.
- Para este control se debe implementar la asignación de un procedimiento de asignación de privilegios.

Configuraciónde acceso por defecto

Para asegurar que no exista alguna equivocación por parte del administrador de la red, por defecto se deben configurar a los usuarios como usuario estándar, es decir sin privilegios de instalación de programas, modificación de archivos de red, desinstalación de programas y sin acceso a los sistemas y aplicaciones. Al igual debe suceder con los conmutadores y enrutadores donde se configuran listas de control de acceso que por defecto bloqueen todo y solo permitan el paso de lo que se configura.

3.4.9 Manejo de sistema de información.

Se pueden establecer políticas para el manejo de información críticaque incluya controles criptográficos sobre la misma. Además se debe tener presente un tipo de procedimiento cuando se deseen realizar determinados cambios en la organización. Según (Miguel, 2013)detalla aspectos específicos para la empresa:

Solicitud de cambio*:* El requerimiento de solicitud de cambios debepresentarse al gerente, y presentarle además las actividades que se van a realizar en el cambio.

Aprobación del cambio*:* Los requerimientos individuales de cambio deberán justificar la razón y claramente identificar los beneficios y las posibles fallas del cambio. La directiva debe analizar el requerimiento de cambio y posiblemente solicitar mayor información antes de que el cambio sea aprobado.

Documentación del cambio*:* Cuando el cambio es aprobado, debe empezar una documentación donde se vaya identificando todos los pasos que se siguieron hasta finalizar el cambio en la empresa.

Pruebas y presentación: El cambio debe ser completamente probado para cubrir algún resultado inesperado.

Implementación: Cuando un cambio es completamente probado y aprobado, se programa el desarrollo para la implementación, el cual debe constar del procedimiento de monitoreo del mismo.

Documentación del control de cambios: Los cambios que deben ser documentados son:

- Instalación de nuevas computadoras.
- Instalación de nuevas aplicaciones.
- Implementación de configuraciones diferentes.
- Instalación de parches y actualizaciones.
- Nuevas tecnologías integradas.
- Políticas y procedimientos actualizados.
- Nuevos dispositivos conectados a la red.

Restriccionesdel cambio de paquete software

Para evitar que los usuarios sin privilegios de la entidad puedan modificar, sin autorización previa cualquier tipo de software, sus cuentas en el dominio no tienen permisos para realizar ninguna de estas actividades, así como tampoco pueden instalar ningún tipo de software ni remover sin previa solicitud del administrador de red y sin autorización de los responsables de cada laboratorio.

3.4.10 Gestión de incidentes de seguridad de la información.

Este punto se refiere a la divulgación de eventos y de posibles debilidades de seguridad de la información en la organización.Cuando un incidente en la empresa ha sido reportado, se pueden tomar diferentes acciones, como son:

- Validar que efectivamente el incidente se ha producido.
- Examinar archivos y registros para detalles del ataque.
- Determinar si puede garantizarse una acción legal.
- Reevaluar o modificar la seguridad de red de las computadoras en general.

Las pautas siguientes ayudarán a la empresa a entender y responder a los varios niveles de uso impropio de la computadora:

Molestia: Estas acciones generalmente muestran una falta de consideración de otros usuarios de la computadora, pero no amenaza, retiro o integridad de la computadora o violar algún principio ético. En otros términos, el individuo mostró un juicio pobre simplemente. El responsable debe responder emitiendo al usuario una respuesta verbal, o copia electrónica, donde advierta que su o sus acciones no eran aceptables.

Ética cuestionable:Estas acciones involucran a menudo violaciones dónde la ética de acciones son cuestionables o cuando el respeto de una persona o integridad de la computadora fueron violadas. La organización podría responder suspendiendo la cuenta del usuario o acceso a los bienes informáticos de la entidad transitoria o definitivamente.

Criminal: Es cuando un usuario realiza una acción que requiere la investigación local, declaración, o la entrada en vigor de una determinada regla. Si el usuario se encuentra culpable de la acción delictiva detectada bajo la investigación, debe efectuarse la separación temporal o definitiva de la empresa.

A continuación se detallan en la tabla 3.19 los pasos a seguir para iniciar el proceso de reportes de incidentes de seguridad que se puedan encontrar en la entidad:

TABLA 3.19 Proceso de reportes de incidentes.

Elaborada por el autor

Objetivo:	Responder apropiada y rápidamente ante un incidente de seguridad
Roles:	Identificar al responsable del local donde se ha generado un incidente de seguridad y trabajar de forma conjunta con el administrador de la red
Entrada:	Reporte de incidente
Salidas:	• Comunicación del incidente • Respuesta ante el incidente • Investigación del incidente • Planes de acciones correctivas • Reporte de mediciones • Mejora de los procesos
Consideraciones:	La fuente y calificación de severidad del incidente determina las acciones a seguir

Análisis del Incidente.-Los incidentes de seguridad son reportados por diferentes personas en la empresa. Por lo cual es necesario que todos los que sean reportados involucren al administrador de la red y el responsable de cada ubicación. Para que de forma conjunta se pueda definir el procedimiento a seguir para los diferentes problemas.

Reporte del incidente.-Evaluado el incidente con el administrador, se realiza un registro del mismo para que se pueda hacer un seguimiento hasta su solución. Los pasos necesarios para reportar un incidente en la empresa son los siguientes:

- Determinar si el incidente representa un serio problema como son: acceso no autorizado a información restringida, alteración de la integridad de un servidor,

negación de servicio, alteración de un servicio Web, penetración al sistema, destrucción de datos, fraude, etc.

- Contactar al administrador de la red para reportar el problema.
- Describir el problema.
- El administrador de la red debe inmediatamente registrar el incidente en un archivo para identificar información relacionada a cada evento.
- El administrador conjuntamente con el responsable de cada localidad deben realizar el procedimiento necesario para mitigar dicho incidente en caso de existir.

Estos procedimientos dependen del tipo de incidente, pues por ejemplo en caso de una vulnerabilidad en un sistema operativo debido a un virus en la red se debe eliminar el virus e informar los procesos que deben seguir los usuarios para que el daño no se propague en la red completa de la empresa.

Administración deincidentes y mejoras de laseguridad de la información

En este procedimiento se debe considerar:

- Como inició el incidente.
- Que fallas o vulnerabilidades fueron explotadas.
- Como ganaron el acceso.
- Como se dieron cuenta del problema.
- Como se resolvió temporalmente el incidente.
- Si los procedimientos de la resolución de incidentes existentes eran adecuados o requieren la actualización.

3.4.11 Gestión de continuidad de funciones en la empresa.

Al desarrollar el proceso de la continuidad de funciones para la empresa, se deben considerar los parámetros sobre los cuales se va a desarrollar el mismoy que se detallan a continuación:

Procesode gestión de la continuidad de funciones: Los responsables de cada local deben determinar las aplicaciones críticas de los mismos y desarrollar procedimientos regulares para mantener respaldos continuos de sus procesos críticos. Se debe considerar como mínimo:

- La administración de los recursos críticos, en caso de ser necesaria la implementación del Plan de Contingencias.
- Identificar los riesgos. Cada riesgo existente en la entidad debe identificarse con qué pasos sería necesario detenerlo, pues es más eficiente evitar la crisis que repararla.
- Documentar el impacto de una pérdida extendida a los funcionamientos y funciones de la entidad.
- Debe ser un modo entendible, fácil de realizar, y fácil para mantener por todos los miembros de la organización.

Salvaguardade losregistros de la empresa: Los registros críticos de la entidad se deben proteger contra pérdida, destrucción y posibles falsificaciones, el esquema que se puede utilizar para mantener un control de los registros es el que se muestra a continuación en la tabla 3.20:

TABLA 3.20 Control de registros en la empresa.

Elaborada por el autor

Tipo de registro	Sistema de información	Período de retención	Medio de almacenamiento	Responsable

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

- Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
- Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
- Mantener un inventario de programas fuentes de información clave.
- Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

Conformidadcon la política de seguridad: El equipo de administración de la red de la empresa debe realizar inspecciones (Ver anexo 1) con el fin de garantizar el cumplimiento de la política, normas y procedimientos de seguridad, este período como mínimo debe ser cada 6 meses. Entre las áreas a revisar se incluyen las siguientes:

- Local de servidores.
- Laboratorios.
- Departamentos.
- Usuarios.

Resulta necesario agregar que los controles implementados están basados en los resultados y conclusiones de la valoración y el proceso de tratamiento de riesgos, los requerimientos y regulaciones legales del país, las obligaciones contractuales y los requerimientos de funciones para la seguridad de la información que define la empresa. Con esta forma de proceder se exige considerablemente el mantenimiento de un nivel de seguridad aceptable en la organización, además de trabajar en pos de una certificación reconocida internacionalmente.

Con la ejecución de este capítulo se alcanzaron las siguientes conclusiones:

La implementación de un modelo de defensa por capas en la empresa eleva la seguridad física y del entorno en esta organización debido a que si una capa falla estará otra para mantener la debida protección.

El hecho de que pudieran existir contingencias en la empresa evidencia que se deben prevenir las mismas y conocer las acciones a realizar en cada caso.

Se muestra que el empleo del Plan de Tratamiento de Riesgos propuesto en este capítulo posibilita la aplicación de procedimientos y políticas de seguridad acordes con la norma ISO/IEC 27001.

En la empresa se pueden implementar los controles seleccionados para incrementar la seguridad del sistema, incluyendo el de gestión de continuidad de funciones.

Conclusiones

Luego de la realización de este trabajo se llegaron a las conclusiones siguientes:

La puesta en funcionamiento de un SGSI basado en la norma ISO/IEC 27001 garantiza la ejecución de un conjunto de procesos que gestionen la accesibilidad de la información en la empresa.

La implantación del estándar ISO/IEC 27001,a partir de cuatro fases fundamentales (Panificar, Hacer Verificar y Actuar), según el Ciclo de Deming, permite desarrollar una metodología de trabajo clara y estructurada.

La revisión periódica de los controles que se han seleccionado e implementadoreduce los riesgos de pérdida, robo o corrupción de la información en la empresa.

En la empresa se pueden implementar los controles propuestos para incrementar la seguridad del sistema, incluyendo el de gestión de continuidad de funciones.

Debido a que el estándar ISO/IEC 27001 se relaciona con otros como el ISO/IEC 9001, y se adapta a las condiciones existentes en Ecuador, se pueden realizar varias certificaciones simultáneamente en estaempresa siempre que cumpla con lo dispuesto en cada una de las normas.

El hecho de que pudieran ocurrir varias contingencias en la empresa evidencia que se deben prevenir las mismas y conocer las acciones a realizar en caso de que alguna de ellas suceda.

Se muestra que el empleo del Plan de Tratamiento de Riesgos propuesto en este trabajo posibilita la aplicación de procedimientos y políticas de seguridad acordes con la norma ISO/IEC 27001.

La implementación de la norma ISO/IEC 27001 en la empresa no solamente permite realizar la reducción de riesgos, sino que posibilita llevar a cabo la prevención de los mismos.

Recomendaciones

Luego de lo analizado en este documento se recomienda:

- Poner en funcionamientoel nuevo Plan de Seguridad Informática realizadopara la empresa.
- Elaborar un trabajo que recoja todas las actualizaciones posteriores que se deberán realizar a la propuesta mostrada anteriormente con el fin de mantener los niveles de seguridad definidos por la empresa.
- Evaluar la eficiencia dela puesta en funcionamiento del nuevo Plan de Seguridad Informática implementado bajo elestándar ISO/IEC 27001.
- Continuar el análisis de esta norma y de otras de actualidad en el tema.
- Extender esta experiencia a otros centros donde su aplicación resulte posible.

Bibliografía

Agé, M., Baudru, S., Crocfer, N., Crocfer, R., Ebel, F., Hennecart, J., . . . Rault, R. (2013). *Seguridad informática: conocer el ataque para una mejor defensa (Ethical hacking) Nueva edición.* ENI.

Alliance, Z. (2007). *ZigBee 2007 specification.* Recuperado el 5 de Enero de 2014, de http://www. zigbee. org/Specifications/ZigBee/Overview. aspx.

Alliance, Z. (2009). *IEEE 802.15. 4, ZigBee standard.* Recuperado el 5 de Enero de 2014, de http://www. zigbee. org.

Alvarez, F. (s.f.). Redes de Telecomunicaciones. Glosario-Redes.

ANAYA. (2012). *Hacker. Edición 2012.* ANAYA MULTIMEDIA.

Anderson, N., & Doherty, J. (2006). *Redes locales (Manuales imprescindibles).* ANAYA MULTIMEDIA.

Anderson, N., & Doherty, J. (2009). *Introducción a las redes CISCO.* ANAYA MULTIMEDIA.

Anfinson, D. (2009). Fundamentos de la tecnología de la información: hardware y software para PC. PRENTICE-HALL.

Arboledas, D. (2013). *BACKTRACK 5.* RA-MA.

Ardila, S. (2009). Estado actual del monitoreo remoto de pacientes usando redes de sensores inalámbricas. *Entérese Boletín Científico Universitario dic2009, Issue 27*, 64-69.

Ardita, J. (2010). *Aspectos prácticos de seguridad.* Recuperado el 5 de Julio de 2012, de http://ebookbrowse.com/aspectos-practicos-y-registro-confecoop-2010-pdf-d46054561

Arquitectura de Sistemas Computarizados, Instalación de Firewall . (2012). Recuperado el 15 de Agosto de 2012, de http://dns.bdat.net/documentos/cortafuegos/x235.html,

Baker, N. (2005). ZigBee and Bluetooth strengths and weaknesses for industrial applications. *Computing & Control Engineering Journal 16(2)*, 20-25.

Baronti, P., Pillai, P., Chook, V., Chessa, S., Gotta, A., & Hu, F. (2007). Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Computer Communications, Volume 30, Issue 7, 26 May 2007*, 1655–1695.

Black, U. (2010). *Redes (Manual imprescindible)* (2010 ed.). ANAYA MULTIMEDIA.

Bluetooth, S. (2001). *Specification of the Bluetooth System, version 1.1.* .Recuperado el 6 de Enero de 2014, de http://www. bluetooth. com.

Bluetooth, S. (2007). *Bluetooth specification.* Recuperado el 6 de Enero de 2014, de annotare.googlecode.com

Borghello, C. (2008). *Seguridad Informática, sus implicaciones e implementación* . Recuperado el 18 de Agosto de 2012, de http://www.informatica-juridica.com/trabajos/PRINCIPALES%20SUJETOS%20AGENTES%20EN%20EL%20UNDERGROUND.pdf

bsi. (s.f.). *Seguridad de la información ISO/IEC 27001*. Recuperado el 15 de Mayo de 2013, de http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001

Certificación. (s.f.). Recuperado el 15 de Mayo de 20013, de http://www.iso27001certificates.com

Chacón, D. (2009). *IDS/IPS.* Obtenido de Escuela Politécnica Nacional.

checkpoint.com. (s.f.). *Check Point Software Technologies*. Recuperado el 15 de Febrero de 2012, de http://www.checkpoint.com

Colobran, M., Arqués, J., & Galindo, E. (2008). *Administración de sistemas operativos en red.* Editorial UOC.

Comer, D. (1998). Reddes globales de información con Internet y TCP/IP. Principios básicos y arquitectura. Prentice-Hall Hispanoamericana S.A.

Dhanjani, N. (2010). *La nueva generación Hacker* . ANAYA MULTIMEDIA.

Egan, D. (2005). The Emergence of ZigBee in building automation and industrial controls. *Computing and Control Engineering, 16(2),* 14-19.

Eslava, A. (Octubre de 2003). *Análisis comparativo de la red Lan contra las redes inálambricas.* Recuperado el 5 de Enero de 2014, de eprints.uanl.mx: http://eprints.uanl.mx/1251/1/1020149259.PDF

Gallego, A. (2009). Routers CISCO: Edición revisada y actualizada 2010 (Guia practica). ANAYA MULTIMEDIA.

Gómez, A. (2011). *Auditoria de seguridad informática.* STARBOOK EDITORIAL.

Gómez, A. (2011). Gestión de incidentes de seguridad informática. STARBOOK EDITORIAL.

Gómez, A. (2011). Seguridad en equipos informáticos MF0486-3 Certificado de profesionalidad. STARBOOK EDITORIAL.

Goncalves, M. (s.f.). *Firewalls: A complete guide.*McGraw Hill.

González, N. (2012). *SEGURIDAD DE LA INFORMACION* . Obtenido de file:///C:/Users/USUARIO/Downloads/Seguridad%20de%20la%20Informaci%C3%B3n%20-%20Nancy%20Gonz%C3%A1lez.pdf

Guerrero, A., & Ruiz, E. (Mayo de 2013). Análisis, diseño y simulación de una red inalámbrica de sensores Wsn en el patio de tanques en la empresa petrolera "Grupo Synergy E & P Ecuador". Recuperado el 5 de Enero de 2014, de Repositorio Digital - UPS: http://dspace.ups.edu.ec/handle/123456789/4351

Harrington, J. (2006). Manual práctico de seguridad de redes (Hardware y redes) . ANAYA MULTIMEDIA.

ISO 27000. (2009). *EL portal de ISO 27000 en español*. Obtenido de http://www.iso27000.es/sgsi.html

ISO/IEC. (s.f.). *www.iso27000.es.* Recuperado el 25 de Mayo de 2013, de http://www.iso27000.es/download/9001similaties_sp

ISO/IEC207001. (s.f.). *ISO/IEC 27001*. Recuperado el 15 de Febrero de 2012, de www.iso27000.es: http://www.iso27000.es/

iso27000. (s.f.). *Modos de análisis de riesgos*. Recuperado el 30 de Enero de 2012, de www.iso27000.es: http://www.iso27000.es/doc_herramientas_all.htm#riesgos

iso27000.es. (s.f.). *Comparación entre la ISO/IEC y la ISO/IEC 9001*. Recuperado el 30 de Enero de 2012, de www.iso27000.es: http://www.iso27000.es/download/9001similaties_sp

iso27001certificates. (s.f.). *Certificación*. Obtenido de www.iso27001certificates: http://www.iso27001certificates.com

Jimeno, M., Miguez, C., & Matas, A. (2010). *Hacker (Guía Práctica)* (2010 ed.). ANAYA MULTIMEDIA.

Joskowicz, J. (agosto de 2008,). *Redes de datos.* . Recuperado el 3 de Agosto de 2012, de Instituto de Ingeniería. Facultad de Ingeniería Eléctrica. Universidad de la Republica .Montevideo, Uruguay: http://iie.fing.edu.uy/ense/asign/redcorp/.../Redes%20de%20Da

Katz, M. (2013). *Redes y seguridad.*Marcombo S.A.

Kernighan, B., & Pike, R. (1984). *The UNIX programming environment.* Prentice Hall.

La defensa en profundidad aplicada a los sistemas de información. (2006).

Las diez vulnerabilidades de seguridad más críticas en aplicaciones web. (2005).

Linux. (s.f.). *ARP Spoofing y Poisoning*. Recuperado el 6 de Enero de 2014, de www.linux-magazine.es: https://www.linux-magazine.es/issue/09/ARPSpoofing.pdf

Lockhart, A. (2007). Seguridad de redes: los mejores trucos (O REILLY). ANAYA MULTIMEDIA.

Malagón, C. (s.f.). *Hacking Ético.* Recuperado el 14 de Diciembre de 2013, de Universidad de Nebrija: http://www.nebrija.es/~cmalagon/seguridad_informatica/transparencias/Modulo_2.pdf

MCI. (2011). *Manual de Usuario X Bee IO.* Recuperado el 10 de Enero de 2014, de MCI electronics. Ingeniería MCI Ltda.: http://www.olimex.cl/pdf/Manual%20del%20Usuario%20MCI-WIR-00787.pdf

Mcmahon, R. (2003). *Introducción a las redes.* ANAYA MULTIMEDIA.

Mcmahon, R. (2003). *Introducción a las redes.* ANAYA MULTIMEDIA.

Mcnab, C. (2008). *Seguridad de redes.* ANAYA MULTIMEDIA.

Meyers, M. (2003). Redes: administración y mantenimiento. ANAYA MULTIMEDIA.

Meyers, M. (2005). *Redes: gestión y soluciones.* ANAYA MULTIMEDIA.

Miller, B., & Bisdikian, C. (2001). *Bluetooth Revealed* (2nd ed.). Prentice Hall PTR Upper Saddle River, NJ, USA ©2001.

ncoline. (s.f.). *La norma ISO/IEC 27001 en Cuba*. Recuperado el 30 de Enero de 2012, de www.ncoline.cubaindustria.cu: http://www.ncoline.cubaindustria.cu/Las_normas_en_la_sociedad_actual.htm

Orejuela, A. (2012). ELABORACIÓN E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA PARA LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. – EMELNORTE. Obtenido de Repositorio digital de Universidad Tecnica del Norte.

Plasencia, Z. (2010). Introducción a la informatica (Guía practica) (2010 ed.).

Plasencia, Z. (2013). *Introducción a la informática* (2013 ed.). ANAYA MULTIMEDIA.

pracgsi.ulpgc. (s.f.). *Cursos*. Recuperado el 12 de Febreo de 2013, de pracgsi.ulpgc.es: http://pracgsi.ulpgc.es/~a1467/cursos/tcp-ip/cap02s10.html

pragsi. (s.f.). *Puertos y sockets-Protocolos de la familia de Internet*. Recuperado el 15 de Enero de 2013, de pracgsi.ulpgc.es: http://pracgsi.ulpgc.es/~a1467/cursos/tcp-ip/cap02s10.html

Rabago, J. (2010). *Guía práctica ANAYA MULTIMEDIA: Redes locales* (2010 ed.). ANAYA MULTIMEDIA.

Ramos, A. (2011). *Seguridad Perimetral.* Madrid, España.

Sams, A. (s.f.). Hacker's Guide to protecting your Internet site and network.

Security. (s.f.). *Security*. Recuperado el 14 de Febrero de 2013, de www.Security.com

Segu-info. (s.f.). *Seguridad Lógica*. Recuperado el 20 de Febreo de 2012, de www.segu-info.com.ar: http://www.segu-info.com.ar/logica/seguridadlogica.htm.

SGSI. (s.f.). *Sistema de Gestión de la Seguridad de la Información*. Recuperado el 10 de Abril de 2013, de www.iso27000.es/sgsi: http://www.iso27000.es/sgsi.html

Silberschatz, A., & Peterson, J. (1994). *Operating system concepts.*Addison-Wesley.

Stallings, W. (2003). *Comunicaciones y redes de computadoras.* Madrid: Prentice Hall.

Stallings, W. (2007). Network security essentials: applications and standards. Prentice Hall.

Stallings, W. (2009). Operating systems: internals and design principles, 6/E. . Pearson Educación.

Subert, A. (2008). Curso de seguridad en Intranet e Internet.

Syngress. (s.f.). Managing Cisco Network Security.

Tanenbaum, A. (1997). *Redes de computadoras.* Pearson.

unet. (s.f.). *Enrutamiento*. Recuperado el 10 de Enero de 2013, de www.unet.edu.ve: http://www.unet.edu.ve/materias/electronica/ing_redes/C4/C4_enru.htm

ups. (s.f.). *Análisis activo y pasivo de redes*. Recuperado el 30 de Enero de 2012, de ups: www.ups.es

William, R., & Cheswick, S. (1994). *Firewall and Internet Security.*

www.iso27000.es. (s.f.). *Modos de análisis de riesgos*. Recuperado el 26 de Mayo de 2013, de http://www.iso27000.es/doc_herramientas_all.htm#riesgos

Zambrano, Y., & Jannina Cerón. (2012). Planificación de un modelo de gestión en la seguridad de la información, aplicable en el fondo de cesantía del magisterio ecuatoriano.

Glosario

Activos: Son los elementos que la seguridad informática tiene como objetivo proteger. (Información, equipos que la soportan y usuarios).

Administrador de red:Persona responsable del diseño, la configuración y la administración del funcionamiento diario de la red. También se le llama administrador del sistema.

BSI: **B**ritish **S**tandards **I**nstitution. En español significa Institución de Estándares Británicos.

CIA: **C**onfidentiality, **I**ntegrity, **A**vailability. En español significa confiabilidad, integridad y disponibilidad.

Cliente:Cualquier equipo o programa que se conecte a otro equipo o programa, o que solicite sus servicios. En una red de área local (LAN) o en Internet, equipo que utiliza recursos de red compartidos proporcionados por otro equipo (llamado servidor).

Contraseña:Cadena de caracteres o código para acceder a un sistema cerrado, utilizada como medida de seguridad para restringir el acceso a los sistemas y recursos de la computadora o la red. Puede estar formada por letras, números y símbolos, y distingue mayúsculas de minúsculas.

CPD: **C**entro de **P**roceso de **D**atos.

Cracker:Intruso. Persona que accede a un sistema sin autorización.

Cuenta de usuario:Registro que contiene toda la información que define a un usuario en

Windows. Incluye nombre de usuario y contraseña necesarios para iniciar sesión, grupos a los que pertenece la cuenta de usuario y los derechos y permisos de que dispone el usuario para utilizar el equipo y la red, y tener acceso a sus recursos.

IEC: **I**nternational **E**lectrotechnical **C**ommission. En españolsignifica Comisión Electrónica Internacional.

Información: Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

ISMS: **I**nformation **S**ecurity **M**anagement **S**ystem.Término en ingles de SGSI.

ISO: **I**nternational **S**tandard **O**rganization. En españolsignifica Organización de Estándares Internacionales.

ISO/IEC 27001: Norma internacional que abarca lo concerniente a las técnicas de seguridad, los sistemas de gestión de seguridad de la información y los requerimientos a tener en cuenta.

ITU: **I**nternacional **T**elecommunications **U**nion. En español significaUnión Internacional de Telecomunicaciones.

PCs: **C**omputadoras **P**ersonales.

PDCA: Acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar).

PTR: **P**lan de **T**ratamiento de **R**iesgos.

SAI: **S**istema de **A**limentación **I**ninterrumpida.

Seguridad: Estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo.

Seguridad física: Describe las medidas de protección externas al ordenador, que tratan de proteger a éste y su entorno de amenazas físicas.

Seguridad informática: Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Seguridad lógica: consiste en la aplicación de *barreras y procedimientos* que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

SGSI: **S**istema de **G**estión de **S**eguridad de la **I**nformación.

SOA:**S**tatement **O**f **A**pplicability. En español significaDeclaración de Aplicabilidad.

SOGP: **S**ecurity **F**orum's **S**tandard of **G**ood **P**ractice.En español significaEstándar de Fórum para Buenas Prácticas de Seguridad.

Subred:Subdivisión de una red IP. Cada subred tiene su propio identificador de red único en la subred.

Usuario**:** Persona que utiliza un equipo.

Anexos

ANEXO1: Acta de inspección empleada en la empresa actualmente y el Modelo de Inspección a la Seguridad Informática que se propone.

Empresa

Fecha:

Acta de inspección

Especialidad Controladora: Seguridad Informática

Dependencia:

Objetivo del Control:

Revisar las Medidas de Seguridad de los soportes y las maquinas computadoras.

Local:

Conformidades:

No Conformidades:

Recomendaciones:

Resultado del Control

Nombre	Nombre
Cargo que desempeña	Cargo que desempeña

Nombre

Cargo que desempeña

Nombre

Cargo que desempeña

Empresa

Modelo de Inspección a la Seguridad Informática

Período de inspección:Tiempo de duración de la inspección. Debe realizarse como mínimo cada seis meses

Grupo de inspección: Decano de la entidad

Administrador de la red de la entidad

Jefes de departamentos

Administradores de subredes

Técnicos de laboratorios

Tipo de inspección: *Exhaustiva*

Área(s) a inspeccionar: Local de servidores

Laboratorios

Departamentos

Usuarios

Propósito de la inspección: Garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad en la entidad.

Renglones de inspección:

Política de seguridad de la información

Recursos humanos

Seguridad lógica

Seguridad física y del entorno

Organización interna

Mantenimiento de equipos

Controles de cambios operacionales

Planificación y aceptación del sistema

Utilización de los medios de información

Adquisición, desarrollo y mantenimiento del sistema de información

Gestión de incidentes de seguridad de la información

Gestión de continuidad de funciones en la empresa

Informe del estado actual de los renglones inspeccionados: Debe recoger como se encuentra la seguridad en la entidad atendiendo al estado actual de los renglones inspeccionados.

Problemas detectados en la inspección: Problemas de seguridad detectados durante el período de inspección, deben considerarse como mínimo los aspectos siguientes:

- Fecha y hora del problema.
- Fuente (el componente que ocasionó el problema).

- Identificador del problema (número único que identifica el problema).
- Equipo (máquina donde se generó el problema).
- Usuario o responsable involucrado.
- Descripción (acción efectuada y datos asociados con el problema).

Medidas propuestas: Posibles soluciones a los problemas de seguridad detectados basadas en los controles ISO/IEC 27001 implementados en la entidad.

Valoraciones y resultado final de la inspección: Se ofrece la calificación final al o a las áreas inspeccionadas, se evalúan posibles transformaciones y mejoras en su desempeño, y se propone la fecha a realizar la próxima inspección.

Nombre	Nombre
Cargo que desempeña	Cargo que desempeña
Nombre	Nombre
Cargo que desempeña	Cargo que desempeña

ANEXO2: Organización Internacional para la Estandarización (ISO) y la Comisión de Electrónica Internacional (IEC).

La ***IS0 (International Organization for Standardization)***es una agencia internacional para el desarrollo de normalizaciones que abarcan un amplio abanico de materias. Es una organización sin ánimo de lucro, de voluntariado, cuyos miembros son organismos de estandarización de las naciones participantes además de una serie de organizaciones observadoras sin voto. Aunque IS0 no es gubernamental, más del 70 % de 1os miembros son instituciones gubernamentales. La mayoría de 1os miembros restantes tienen relaciones muy estrechas con las administraciones públicas de 1os respectivos países. Por ejemplo, elmiembro estadounidense es el organismo denominado (American National Standards Institute) (ANSI).

IS0 se fundó en 1946 y desde entonces ha especificado más de 12.000 normalizaciones en una gran cantidad de áreas de diversa índole. Su objetivo es promocionar el desarrollo de normalizaciones y deactividades relacionadas para facilitar el intercambio internacional de bienes y servicios, así como desarrollar la cooperación en la esfera intelectual, científica, tecnológica y económica.

IS0 ha definido estándares para todo, desde el paso de 1os tornillos hasta cuestiones de energía solar. Un área importante dentro del campo de las normalizaciones se encarga de la arquitectura de comunicaciones para la interconexión de sistemas abiertos (OSI, Open Systems Interconnection), así como de la definición de estándares para cada una de las capas de la arquitectura OSI u otras como la definición de estándares para la seguridad de la información (ISO/IEC 27001).

Los estándares OSI se han desarrollado en realidad como un esfuerzo conjunto con otras organizaciones como es la ***IEC (International Electrotechnical Commission)***. La IEC se encarga principalmente de la normalización en ingeniería eléctrica y electrónica.

En el área de las tecnologías de la información, ambas organizaciones se solapan, aunque la IECpone másénfasis en 1osaspectos hardware, mientras que IS0 lo hace en software. En 1987, 1os dosgrupos formaron el JTC (Joint Technical Committee). Este comité ha tenido la responsabilidad del desarrollode documentos en el área de las tecnologías de la información que han sido adoptados por IS0 (ypor el IEC).

El desarrollo de un estándar IS0 en particular, desde que empieza como una propuesta hasta que seformaliza como un estándar oficial, sigue un proceso que se puede describir en seis pasos o fases. Elobjetivo es que el resultado final sea aceptado por el mayor número posible de países. A continuaci6n sedescriben brevemente las fases:

1. Fase de proposición:se asigna un tema a1 comité técnico apropiado, y dentro de ese comité, al grupo de trabajo adecuado.

2. Fase de preparación:el grupo de trabajo prepara un borrador de trabajo. Durante esta fase es probable que se consideren sucesivos borradores hasta que el grupo de trabajo está convencido de que ha desarrollado la mejor solución técnica a1 problema abordado. En esta fase, el borrado se envía a1 comité jerárquicamente superior y al grupo de trabajo para entrar en la fase de consenso.

3. Fase en el comité:tan pronto como el comité apruebe el primer borrador, se registra en la SecretaríaCentral de la ISO. Se hace circular entre 1os miembros interesados para su consideración, emisión de comentarios técnicos y su posterior votación. Puede que en esta fase se considerensucesivos borradores hasta que se alcance el consenso en lo referente a1 contenido técnico.

Cuando hay un acuerdo suficiente, el texto está preparado para ser remitido como documentoDIS (*Draft International Standard*) Proyecto de la Norma Internacional.

4. Fase de indagación:la Secretaria Central de la IS0 hace circular el DIS entre todos 1os miembrosdel IS0 para su votación y formulación de comentarios durante un período de cinco meses.El documento se aprobará para su consideración como FDIS (Final Draft International Standard) Proyecto Final de la Norma Internacional siempre y cuando se consiga una mayoría de las dos terceras partes y no menos de un cuarto del

número total de votos sean negativos. Si no se consigue la aprobación, el texto se devuelvea1 grupo de trabajo proponente para su nueva reelaboración, para posteriormente hacerlo circularde nuevo como documento DIS y repetir el proceso.

5. Fase de aprobación:el documento FDIS se distribuye entre todos 1os estamentos del IS0 porparte de la Secretaria Central para una votación final (Si/No) durante un periodo de dos meses.Si se reciben comentarios técnicos durante ese período, no serán considerados durante estafase, pero serán registrados para su posterior consideración en una revisión futura del EstándarInternacional. El texto se aprobará como Estándar Internacional si obtiene una mayoría de las dos terceras partes y no más de un cuarto del número total de votos sean negativos. Sino consigue su aprobación, el estándar es devuelto a1 grupo de trabajo original para su reconsideración,teniendo en cuenta las razones técnicas argumentadas por parte de 1os votantes negativos.

6. Fase de publicaci6n:una vez que el documento FDIS se haya aprobado, se introducirán sólo cambios mínimos en el texto definitivo. El texto final será remitido a la Secretaria Central de laISO, la cual publicará el documento en su estado de Estándar Internacional.

El proceso de definición de un estándar IS0 puede ser lento. Ciertamente, sería deseable que la definición de estándares fuera tan rápida como 1os detalles técnicos lo permitieran, pero IS0 debe asegurarsede que el estándar recibe una aceptación suficiente.

ANEXO 3: Tabla comparativa entre UNE 71502e ISO/IEC 27001.

	UNE 71502	ISO/IEC 27001
Editada por	AENOR	ISO/IEC 27001
Fecha de publicación	Febrero del 2004	Octubre del 2005
Idioma	Español	Inglés
Ámbito	Español	Internacional
Elaborada por	AEN/CTN 71	ISO/IEC
# de páginas	12(+4 anexos)	12(+30 anexos)
Equivalencia de apartados y cláusulas		Prólogo
		Introducción
		Generalidades
		Enfoque por procesos
		Compatibilidad con otros sistemas de gestión
	Objetivo y campo de aplicación	Alcance
		Generalidades
		Aplicación
	Normas para consultas	Referencias normativas
	Términos y definiciones	Términos y definiciones
	Marco general del SGSI	SGSI

	Requisitos generales	Requisitos generales
	Planificación y diseño del SGSI	Establecer y gestionar el SGSI
		Establecer el SGSI
	Implantación del SGSI	Implantar y utilizar el SGSI
		Monitorear y revisar el SGSI

Tabla comparativa entre UNE 71502 e ISO/IEC 27001.Continuación

Equivalencia de apartados y cláusulas		Mantener y mejorar
	Selección de controles	Establecer el SGSI
	Documentación	Requisitos de documentación
		Generalidades
	Control documental	Control de documentos
	Registros	Control de registros
	Responsabilidad de la dirección	Responsabilidad de la dirección
	Compromiso de la dirección	Compromiso de la dirección
	Política de seguridad de la organización	Establecer el SGSI

	Implantación del SGSI	Implantar y utilizar el SGSI
	Implantación de los controles	
	Eficacia de los controles	
	Gestión de recursos	Gestión de recursos
	Provisión de recursos	Provisión de recursos
	Recursos humanos	Formación, toma de conciencia y competencia
	Generalidades	
	Competencia, toma de conciencia y formación	
	Auditorías internas	Auditorías internas del SGSI
	Revisión del SGSI	Revisión del SGSI por la dirección
	Generalidades	Generalidades
		Entrada de la revisión
		Salida de la revisión
	Auditorías internas	Auditorías internas del SGSI

Tabla comparativa entre UNE 71502 e ISO/IEC 27001. Continuación

	Proceso de mejora	Mejora del SGSI

	Mejora continua	Mejora continua
	Acción correctiva	Acción correctiva
	Acción preventiva	Acción preventiva
	Bibliografía	Bibliografía
	Anexo A: Relación de procedimientos para establecer el SGSI.	Anexo A: Objetivos de control y controles
		Anexo B: Principios de la OCDE
		Anexo C: Correspondencia con ISO 9001 e ISO 14001

ANEXO4: Conducta a seguir por todo usuario de la red de la empresa.

A continuación se detallan los puntos principales en cuanto a seguridad que deberían darse a conocer a los usuarios de la entidad, para que tengan conocimiento de cuáles son las responsabilidades de seguridad que se comprometen a cumplir una vez que son miembros de la facultad.

Laconfidencialidad: Si algún usuario tiene conocimiento de una situación de riesgo informático o ilegalidad, debe informar inmediatamente al responsable de laboratorio, al administrador de la red de cada área, o al administrador de la red de la entidad con vista a que el hecho sea conocido y se le pueda brindar la debida solución.

ConductaPersonal: La reputación de la entidad depende de sus usuarios en gran medida, si los responsables de cada local encuentran una conducta dentro o fuera de este que afecte en forma adversa sudesempeño, el de otros usuarios, o los propios intereses de la facultad y no se combaten debidamente se estaría incurriendo en un acto de indisciplina, y como tal se debe juzgar.

Protecciónde losactivosdelaentidad: La entidad tiene una gran variedad de activos, los cuales incluyen activos físicos e información importante. Resulta imprescindible proteger todos estos activos. Los usuarios son responsables en gran medida de proteger la propiedad de la facultad confiada a ellos y de ayudar a proteger los activos de la entidad en general. Se debe estar alerta ante cualquier situación o incidente que pueda llevar a la pérdida, mal uso, o robo de las propiedades de la facultad.

Alsalirdelaentidad: Si un estudiante deja de formar parte de la facultad, sea temporalmente debido a licencias o período vacacional, o permanentemente debido a que haya solicitado traslado o cause baja por una determinada razón, este debe devolver toda la propiedad perteneciente a la entidad, incluidos los documentos y medios que contengan información de la entidad, antes de retirarse.

Accesoa informacióncrítica: El manejo de información confidencial o restringida por un determinado usuario no puede llevarse a cabo mientras no se haya acordado formalmente los términos de su empleo por parte de la entidad y mediante una constancia escrita y aprobada.

Sancionesprevistasporincumplimiento: Se aplicarán las sanciones previstas de acuerdo al reglamento universitario a quienes incumplan lo dispuesto en las Políticas de Seguridad.Las sanciones sólo pueden imponerse mediante un acto administrativo que así lodisponga cumpliendo las formalidades impuestas por los preceptos universitarios.

ANEXO5: Guía para el correcto desempeño de los usuarios de la entidad.

Contraseñas: Son las claves de la información electrónica. Resulta relativamente fácil acceder a la informaciónque no esté protegida mediante contraseñas. Si un usuario escoge contraseñas débiles, es posibleque puedan serdescubiertas o descifradas. A continuación se muestran algunos aspectos para contar con una contraseña fuerte:

- Escoger una determinada palabra o frase extraída de un libro o manual en especial.
- En caso de haber escogido una palabra, procurar que sea larga,seguidamente se divide en dos partes. Ambas partes se subdividen en dos partes más pequeñas, poniendo entre la división de la primera parte el número de la página en que se encuentra la palabra y en la segunda división el número del párrafo. Y finalmente sustituir las vocales por un símbolo en específico.Por ejemplo:

(estrepitoso) (estrepi toso) (estr253epi t1oso) (estr253epit1oso)

Resultado final: (*str253*p*t1*s*)

- En caso de haber escogido una frase sería como se muestra seguidamente:

"soy un estudiante universitario y estoy en 5to año de tle"

Esta frase convertida en contraseña sería: (sueu&2e5toadtle)

Indicaciones a cumplir para la gestión de contraseñas en la entidad:

- Usar no menos de 8 caracteres en la contraseña.
- Cambiar las contraseñas regularmente, se recomienda que sea mensualmente.
- Si un usuariocausa baja de la facultad, se debe desactivar su contraseñainmediatamente.

- Se recomienda emplear una contraseña distinta para cada aplicación (Correo electrónico, Internet, UOclas)

Acciones que no deben realizarse con las contraseñas:

- Escribirlas contraseñas en algún formato.
- No usardatos personales o de personas conocidas en las contraseñas.
- No usar los mismos caracteres. Ejemplo: (55555) o (hhhhh), para una contraseña
- No usar como contraseña la palabra contraseña.
- No compartir la contraseña con otras personas.
- No usar las contraseñas predefinidaspor un Software, sino que debe ser cambiada.

Resulta de suma importancia cumplir con todos los parámetros especificados anteriormente para mantener una seguridad apropiada de nuestra información.

Virusinformáticos: Todo software antivirus puede utilizarse porque todos trabajan de manera parecida y realizan la misma función que radica en la detección y eliminación de virus informáticos. Lo primordial es simplemente emplear el más adecuado. Lo que la mayoría de los usuarios no considera, o no le presta la debida atención es que el software antivirus debe seractualizado constantemente. Esto significa periódicamente actualizar sus parámetrosdebido a que todos los días se escribennuevas versiones tanto de virus como de actualizaciones contra ellos, y estas están disponibles en Internet. En el caso de la entidad, los técnicos de laboratorio son los encargados de mantener actualizados los antivirus de cada una de las estaciones de trabajo, a aquellos usuarios que posean privilegios de administrador, pero compete a los usuarios en general velar porque dichos software estén actualizados correctamente.

Si nose instala un SW Antivirus en la facultado no se actualizada debidamente, se está incurriendo en un riesgo potencial de quedar contaminada la computadora con algún

virus, y si no se toman las acciones pertinente pasar entonces a quedar infectada toda la red, pudiendo ocasionar incontables problemas.Cuando se conecta a la máquina algún dispositivo externo de almacenamiento (Disco compactos, memorias flash, disquetes, etc.) estos deben ser procesados primeramente por el antivirus antes de ser abiertos, en caso de estar infectado se procede a su descontaminación, este proceso debe realizarse constantemente hasta que el dispositivo que desinfectado. La mejor opción sería que si un determinado virus afectó archivos o datos, estos deben serdestruidos. El antivirus exigirán desinfectar los archivos, pero esto nunca esgarantizado. Lo más seguro es que se destruya el archivo con el virus.

Spyware: Estos son pequeños programas que se insertan en el sistema de la computadora pararecoger secretamente la información sobre usuarios / facultad en este caso sin que ellos lo sepan.Esto es principalmente para anunciar los propósitos, puede recoger información sobredirecciones de correo electrónico e incluso las contraseñas y detalles de la entidad.Spyware no es una buena idea y el usuario cuidadoso trata de restringirlo o quitarlocompletamente. Hay dos paquetes disponibles en Internet, los cuales eliminan el spyware. Los dos paquetes son gratis para el uso personal, estos son:

- Lavasoft's (Ad-aware)
- Spybot

Es recomendable que se descarguen los dos paquetes, y se ejecuten al menos una vez a lasemana. Es necesario recalcar que estos paquetes también necesitan ser actualizados.

Losparches: son muy importantes y están relacionados con los virus y el *hacking*. Todo software tiene problemas y defectos. En la mayoría de los casos, los defectos son minoritarios, es así que estos son ignorados y probablemente no tendrán impactos en la facultad. Mientras que otros defectos son demasiados importantes para ser ignorados.

Todos los productores de software proveen parches. Las computadoras que no estén conectadas a ningún sitio probablemente no necesitarán preocuparse por los parches mientras se encuentren trabajando correctamente.El problema principalmente tiene

relación con el sistema operativo dela computadora.Este es el programa básico que corre en una máquina. En nuestra facultad se empleauna determinada versión de Microsoft Windows y/o Linux. Estos sistemasoperativos necesitan actualizarse periódicamente. Pero muchas aplicacionestambién necesitan ocasionalmente parches.

Si no se tienen actualizado los software, se tiene el riesgo de que el software falle o en el casode browser o email un software malicioso corrompa alguna computadora de la red, o un usuariomalicioso tenga acceso a una estación en específico.La mayoría de los proveedores de software proporcionan un servicio de notificación víaemail a sus clientes cuando un nuevo parche está disponible. Estas notificacionespueden ser de criticidad baja y ser actualizadas en cualquier tiempo o pueden tener criticidad alta y deben ser actualizadas inmediatamente. La continuidad de funciones en la entidad puede depender grandemente de esto.La mayoría de proveedores de software ofrecen automáticamente actualizaciones víaInternet.

Empleoderespaldos: El respaldo es el proceso de tomar una copia de todos los datos electrónicos, como una copia de archivos contables. Es necesario que los usuarios de la entidad realicen un respaldo continuo de su información, pues en el momento menos pensado fallos en los equipos, la red en general, o también debido a actividades de mantenimiento pueden ocasionar la pérdida de la información. Para ello debe considerarse lo siguiente:

Un respaldo formal y eficiente evitará que amenazas naturales o intencionadas provoquen que dejen de existirsus datos. Un usuario de la empresa puede copiar datos a:

Disquetes

Memoria flash

Discos compactos a DVD

Discos externos

Los usuariosdeben considerar hacer múltiples respaldos para datos críticos. Un apropiadorespaldo debería considerar lo siguiente:

- Al final de cada jornadarealizar un respaldo de todos los archivos que se han cambiado.
- Al final de cada semana realizar un respaldo de todas las aplicaciones por parte de los técnicos de laboratorios.
- Al final de cada mes realizar un respaldo del sistema operativo por parte de los técnicos de laboratorios.

Si se tiene que restaurar una determinada computadora después de una falla catastrófica, se deberá usar el respaldo mensual para restaurar el sistema operativo, luego se usará elrespaldo semanal para restaurar las aplicaciones y finalmente se usará elrespaldo diario para recuperar los archivos. Con ello se ha reconstruido el sistema completo. Si cualquiera de los respaldos no puede ser reconocido, serecomienda usar unrespaldo previo y empezar desdeeste punto.Uno de los mayores problemas con respaldos ocurre cuando el propietario olviderotular la información apropiadamente.

Robodeinformacióne identidad: Para la entidad es de vital importancia tener la información almacenadaapropiadamente, esto incluye papeles o copias electrónicas.vUn individuo puede robar una identificación de un usuario de la facultad para realizar algún fraude. Mientras el usuario no esresponsable por el fraude perpetrado por otros, el problema después del robo de un identificador es recuperar su confidencialidad nuevamente para continuar desarrollando sus funciones dentro de la organización.Algunas acciones que no deben hacerse son:

- No ofrecer información personal en Internet o por el correo electrónico, mientras no se esté seguro que la comunicación es confiable.
- Cualquier evento extraño debe ser reportado inmediatamente al responsable de seguridad informática para ser investigado apropiadamente.
- No ser partícipe de un robo de información o identidad.