UNIVERSIDAD AUTÓNOMA
DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS
E INGENIERÍA

LIC. EN SISTEMAS COMPUTACIONALES

ELEMENTOS DE SEGURIDAD APLICADOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (TIC´S)

MONOGRAFÍA

QUE PARA OBTENER EL TITULO
DE LICENCIATURA EN SISTEMAS COMPUTACIONALES

PRESENTA:
P.L.S.C. PELÁEZ GIL RICARDO

ASESOR:
L.C LUIS ISLAS HERNÁNDEZ

Agradecimientos

A Dios:

"Dios es quien da la sabiduría, la ciencia y el conocimiento brotan de sus labios. El Señor da su ayuda y protección a los que viven rectamente y sin tacha; cuida de los que se conducen con justicia y protege a los que le son fieles. Así sabrás lo que es recto y justo y estarás atento a todo lo bueno, pues tu mente obtendrá sabiduría y probarás la dulzura del saber".

Proverbios 2.6-10

Gracias Señor por conducirme siempre por tu senda. Este paso que doy en mi vida ha sido por obra y causa tuya. Permíteme siempre prestar atención a Tu Palabra para ser bendecido y prosperado en Ti.

A mis padres:

Quienes me han enseñado las virtudes más grandes que hay en la vida: el temor de Dios, el amor, la perseverancia y la decisión para triunfar en todo lo que emprenda. Gracias papá por convertirme en un hombre de carácter y enseñarme la manera en como el trabajo dignifica al hombre. Gracias mamá por darme esa sensibilidad en mi corazón e inculcarme que la honradez, el respeto y la dignidad deben ser una parte inherente de mi ser. Para ustedes con mi más grande admiración.

A mi familia y amigos:

Por todas las muestras de apoyo que me brindaron a lo largo de mi carrera profesional. Una gran parte de lo que hoy he logrado ha sido por su ayuda incondicional y sincera.

A mis sinodales y asesor:

Por su amistad y su apoyo que me dieron como estudiante y ahora como egresado. Y por sus conocimientos y experiencias que me trasmitieron tan amablemente y que me ayudaron a formarme como una persona profesional.

Ricardo Peláez Gil

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Planteamiento del problema

Actualmente el intercambio de información vía electrónica es una actividad muy importante en toda organización, sin embargo el problema de falta de seguridad es muy serio ya que muchas de ellas no cuentan con una cultura de seguridad y prevención adecuada.

El problema se hace aún más delicado, puesto que muchas organizaciones no conocen los elementos de seguridad necesarios así como también no cuentan con mecanismos de control que regulen las diferentes operaciones realizadas a la información. Por lo anterior, resulta necesario realizar un análisis minucioso sobre cada uno de los riesgos que amenazan la integridad total de los sistemas y de los elementos que los rodean tales como usuarios, equipos de cómputo y lugar de trabajo. Del mismo modo, este análisis habrá de hacerse a los elementos de seguridad que tendrán como objetivo regular el correcto accionar de la función informática.

Objetivo

El objetivo de este trabajo es dar a conocer un panorama general de lo que son y lo que engloban las Tecnologías de Información y Comunicaciones (TIC's) por medio de descripciones, definiciones y diagramas; así como la manera en que éstas se relacionan e implementan con los elementos de seguridad informática a fin de gestionar mecanismos y acciones que prevengan cualquier tipo de amenaza.

Justificación

Hablar de TIC's y seguridad informática es un tema que concierne a toda organización. En los últimos años, ambas han tenido un mayor auge puesto que desde hace tiempo se ha estado desarrollando un cambio significativo en todas las formas de manipulación, envío y recepción de información. Teniendo en cuenta lo anterior, debemos considerar que las organizaciones tienden hacia una automatización basada en las TIC's que será regulada por una serie de medidas de seguridad a fin de evitar cualquier tipo de ataque.

Por lo anterior, este trabajo se encuentra orientado hacia dos grandes vertientes: la primera consiste en conocer los diferentes riesgos que pueden atentar no sólo en contra de la información, sino también de la integridad de los equipos de cómputo y de los mismos usuarios que hacen uso de ellos; y la segunda que enfoca los elementos de seguridad necesarios que garanticen en la medida de todo lo posible la concreción de una amenaza en contra de la información, usuarios o equipos de cómputo.

Así, teniendo en cuenta los riesgos y conociendo los elementos de seguridad informática habrán de traducirse éstos últimos en la gestión de mecanismos de control que vigilen el comportamiento de la función informática dentro de la organización.

Introducción

La tecnología es la aplicación de conocimientos científicos en las actividades cotidianas del hombre con el objetivo de optimizar los métodos utilizados para lograr una meta determinada. Por consiguiente es considerada como un factor de gran importancia que culmina en el mejoramiento total de cualquier tipo de proceso.

En informática, la sociedad se ha encaminado hacia la "era de la información", en donde un número de personas cada vez mayor se relaciona con la captura, el manejo, la distribución y el uso de grandes cantidades de datos, excediendo en mucho lo que se podría haber imaginado hace algunos años. Dentro de este cambio tecnológico se encuentran las TIC's, las cuales han brindado a los individuos y a las organizaciones un conjunto de capacidades que antes no se tenían para accesar, almacenar, procesar, duplicar, combinar y rastrear información.

El capítulo uno brinda un análisis acerca del origen de las TIC's mostrando la manera en como fue evolucionando la interacción del hombre con la computadora. Del mismo modo, se expone la manera en como surgió la seguridad informática así como la importancia que fue cobrando con el paso del tiempo. Finalmente, se describen algunas reseñas de ataques a la seguridad de la información.

El capítulo dos expone de una manera sistematizada el entorno general que rodean a las TIC's, desde su definición, potencial y evolución hasta factores de relación con la seguridad informática. Del mismo modo, se estudian aspectos de importancia dentro de las TIC's como la reingeniería y tendencias a futuro de éstas.

El capítulo tres describe los diferentes riesgos a los cuales podrían estar vulnerables los sistemas de cómputo, equipos, usuarios y, por supuesto, la información que tenga que ser almacenada, procesada e intercambiada.

El capítulo cuatro expone los elementos de seguridad informática que se deben tomar en cuenta para evitar la concreción de algún tipo de amenaza expuesta en el capítulo tres.

Por último, **el capítulo cinco** gestiona un reglamento de seguridad informática tomando en consideración los elementos de seguridad que se vieron, analizaron y explicaron en el capítulo cuatro.

Capítulo 1.

Antecedentes históricos de las TIC's y la seguridad informática

1.1 Antecedentes de las TIC's

Desde varios siglos antes de nuestra era no ha parado la investigación del hombre en la búsqueda de herramientas y métodos que nos ayuden en las tareas de cálculo y procesos de la información; por tanto, todos aquellos descubrimientos que poco a poco, a lo largo del tiempo, han llevado al estado actual de la informática tienen su parte correspondiente en el conjunto de elementos pertenecientes a la ciencia [3].

Las TIC's tienen como principal antecedente las generaciones de computadoras a partir de su creación. Conforme las máquinas se fueron volviendo más eficaces, rápidas y seguras, el modo de procesar la información cambió radicalmente.

1.1.1 La era electrónica

La primera generación de computadoras se inicia con el uso de la Univac 1, en 1951. En esta época las máquinas se construían con tubos de vacío, que eran tubos de vidrio del tamaño de un foco que albergaban circuitos eléctricos. El transistor, inventado en 1947 por John Bareen, Walter Brattain y William Shockley, desplazó la teoría del tubo de vacío. En 1956, con el uso de los transistores empezó con lo que se considera como el despegue de las computadoras de la segunda generación, además de que revolucionaron la electrónica. Puede decirse que la era electrónica se inicia con la invención del transistor en los laboratorios Bell [1].

Las crecientes necesidades del programa espacial de Estados Unidos de América requerían mejores computadoras en espacios más pequeños y con mayor capacidad, lo cual fue posible gracias a la tecnología del circuito integrado desarrollado de manera independiente por Jack Kilby, de Texas Instruments, y Robert Noyce, en Fairchild Semiconductor. La técnica consistía en reunir los elementos electrónicos y las conexiones entre ellos, en una pequeña oblea de silicio [ídem].

A mediados de los años sesenta las máquinas de transistores fueron sustituidas por máquinas más potentes de la tercera generación

confeccionadas por circuitos integrados. Algunos historiadores de la tecnología consideran que el tubo de vacío, el transistor y el chip de silicio tuvieron un impacto social, de manera tal que han marcado los cambios generacionales o fronteras. En 1968, Borroughs produce las primeras computadoras, 82500 y B3500, que utilizaban circuitos integrados. En 1969, el Departamento de Defensa de Estados Unidos crea ARPANET[1]. [ídem]

En 1971 Intel desarrolló el microprocesador 4004. Algunos historiadores consideran la invención del microprocesador como el inicio de la cuarta generación de computadoras. Este fue el primer chip en contener todos los componentes de un CPU[2] en una sola unidad. En 1972, con la introducción del microprocesador 8008 de Intel, se da el mayor paso en la evolución de los microprocesadores. Este fue el primer microprocesador de 8 bits y fue doblemente complejo que el 4004. El progreso de todos los componentes electrónicos, especialmente de los transistores y circuitos integrados, afectó todas las áreas de la electrónica y el desarrollo de las computadoras, por lo que la electrónica digital puede considerarse como una revolución técnica [ídem].

La era electrónica engloba las tres primeras generaciones de la computadora: tubos de vacío, transistores y circuitos integrados. Esta época se caracterizó por una serie de descubrimientos que fueron abriendo camino hacia lo que actualmente es el microprocesador y la **inteligencia artificial**[3]. Al principio las máquinas eran demasiado grandes y tenían grandes posibilidades de sufrir daños, sin embargo con el tiempo, fueron sustituyendo sus componentes y su forma de operar mediante nuevos descubrimientos y nuevas maneras de realizar operaciones, que trajeron por principio de cuentas, menores dimensiones a los equipos y más eficiencia en la resolución de procesos.

[1] Red precursora de Internet.
[2] Unidad Central de Procesamiento.
[3] Rama de las ciencias computacionales que emula el proceso de pensamiento del cerebro humano.

1.1.2 Utilización de la computadora en la era electrónica

Durante las décadas de 1960 y 1970 y comienzos de la de 1980, el mainframe "anfitrión" y los sistemas basados en minicomputadoras eran esencialmente el único juego en el medio. Quienes tenían el acceso directo a estas computadoras y a los sistemas de computación hacían parte de una minoría aislada y muy especializada, a menudo conocida como sistemas de información administrativa (*management information systems, MIS)* [11].

Si bien es cierto que durante esta época las computadoras pasaron de los bulbos a los circuitos integrados, aún resultaba complicado manejarlas. Sólo los especialistas en cómputo tenían acceso a ellas y se encontraban aislados del mundo organizacional. Los sistemas se encontraban centralizados en este pequeño grupo de profesionales que ofrecían a las empresas sus servicios como organismo independiente y no como parte de la organización en sí.

Con frecuencia, los sistemas eran demasiado engorrosos y complicados, de manera que sólo los especialistas en computación podían usarlos. A menudo se requería trabajarlos de manera continua para mantenerlos en funcionamiento. Los empleados ajenos a los departamentos encargados de procesamiento de datos tenían poco o ningún acceso a la tecnología diferente de ver lotes de resultados impresos acerca de ventas, inventario y finanzas de la compañía, en tanto que las personas pertenecientes a departamentos encargados de procesamiento de datos estaban inmersas en la tecnología. La mayoría de los empleados de la compañía, incluidos los ejecutivos, usualmente sentían que aunque la tecnología de la computadora era útil, tenía poca importancia para las operaciones diarias reales de las organizaciones [ídem].

La computadora personal (PC) fue el comienzo del fin de la antigua perspectiva. La microcomputadora permitía a todos los empleados, desde secretarias y vendedores hasta profesionales y ejecutivos trabajar directamente con la tecnología y obtener ventaja de los muchos beneficios que ella podía brindar. Los paquetes estándares de software que apoyaban el hardware de la PC facilitaron el uso de la tecnología. Al hacer

computadoras accesibles a todo el mundo en la organización, la revolución de la microcomputadora proporcionó a la tecnología una reputación y presencia totalmente nueva en la empresa. La PC dio acceso directo a las herramientas tecnológicas que facilitaron a las personas realizar sus operaciones de manipulación de información de manera más rápida, efectiva y segura [ídem].

El uso diario de la PC proporcionó una revolución total dentro de las empresas. Se volvió más eficaz el manejo de grandes cantidades de datos, se redujeron costos y una cantidad de tiempo verdaderamente considerables. Con la implementación de la PC se daba paso a la era de la información.

1.1.3 La era de la información

Durante las décadas de 1950, 1960 y 1970, el procesamiento de datos en esencia tuvo como objetivo reducir los costos de oficina. Posteriormente, la tecnología desplazó a la línea frontal en la mayor parte de las organizaciones. Se ha hecho estratégica en cuanto a que es un componente necesario para la ejecución de una estrategia de negocios. También ocurrieron cambios en cuanto a quién utilizaría las computadoras. Durante la era electrónica los usuarios principales eran los especialistas técnicos, profesionales y gerentes que diseñaban, implementaban, administraban, controlaban y a menudo eran los dueños de la infraestructura computacional de la empresa. Con la transición a la era de la información, los usuarios de la tecnología se han colocado a la vanguardia [11].

Actualmente, los usuarios desean modelar la tecnología que se implementa en sus organizaciones, desean controlar su uso y determinar el efecto que tendrá en su propio trabajo. Rápidamente comprenden que el uso efectivo de la tecnología acoplada a un cambio en la manera en como se desempeña el negocio determinará el éxito profesional y organizacional. Éstos mismos se han convertido en la vanguardia de una revolución tecnológica de la información que con mucha rapidez ha alterado las formas antiguas de la computación organizacional y la generación y manipulación de información [ídem].

La era de la información comienza con la implementación masiva de la PC dentro de las corporaciones. Este momento determinó la descentralización de los procesos de información en unos cuantos para dar acceso a los datos a toda persona dentro de la empresa trayendo como consecuencia una mejora en el comportamiento general de la organización. Los antiguos paradigmas empresariales fueron cambiados por nuevas tendencias en cuanto al manejo de datos; comenzaba la llamada "revolución de la información".

1.1.4 Utilización de la computadora en la era de la información

El cambio en la forma de uso de las computadoras personales marcó la transición hacia la era de la información. El creciente número de aparatos aislados concientizó a las organizaciones de la necesidad de comunicarse. La capacidad de comunicaciones de la tecnología de red de área local (LAN[4]) y las demandas y complejidad crecientes del usuario individual, llegaron en conjunto al mismo tiempo. Si pudiera compartirse más información, memoria, potencia de computación y otros recursos computacionales, los usuarios se beneficiarían. El resultado fue la aparición de una red LAN. Aunque en principio estas redes fueron creadas para reducir costos compartiendo recursos tecnológicos como software, impresoras y otros dispositivos periféricos, las redes LAN facilitaban el trabajo en grupo entre empleados, como grupos de un mismo departamento. Así, en vez de compartir solo tecnología, las personas comenzaron a compartir información y funciones finales de usuario, como correo electrónico [11].

Posterior al cambio radical que dieron las PC's al uso y manipulación de información nacieron las redes LAN y la posibilidad de interactuar con otras empresas. Esto trajo como consecuencia que muchos procesos manuales fueran automatizados como el cambio del correo tradicional al correo electrónico. Estos cambios se mantuvieron al margen de la estructura funcional de la empresa hasta hace muy poco tiempo, ya que actualmente es posible ver organigramas diferentes a los tradicionales y funciones entrelazadas entre diferentes departamentos que vuelven más eficaz el accionar de las diferentes tareas dentro del lugar donde son implementadas.

[4] Local Area Network.

1.1.5 Evolución de la automatización de oficinas

Mucho antes de la automatización de las computadoras, las compañías reunían, almacenaban y actualizaban información en lo que era el curso normal de hacer negocios. En el pasado, los sistemas de información consistían en los procedimientos y reglas establecidas para entregar información a la gente dentro de una organización. Diferentes personas requerían distinta información para realizar su trabajo y las reglas del sistema gobernaban qué información debería ser distribuida a cada persona, cuándo y en qué formato [6].

La introducción de sistemas de administración de bases de datos permitió que los trabajadores en toda la organización tuvieran acceso a los datos de las computadoras. De este modo, los dirigentes de las organizaciones reconocieron el potencial de los procesadores de textos, hojas de cálculo y otras aplicaciones incorporando las PC's a los planes de la organización. El trabajo pasó de las macrocomputadoras a las PC's y la gente usó estas máquinas personales en tareas para las cuales no estaban programadas dichas macrocomputadoras [5].

La automatización de las oficinas englobó a la gran mayoría de las acciones que hasta hace poco tiempo se realizaban de manera manual. La realización de todo tipo de documentos, rotafolios, informes y balances financieros pasaron a ser hechos de manera electrónica. El tiempo en su elaboración se vio minimizado y al mismo tiempo se volvieron más presentables y fidedignos con ayuda de la computadora.

1.2 Antecedentes de la seguridad informática

La seguridad informática como tal hace su aparición en el año de 1983 cuando el primer virus informático fue concebido como un experimento para ser presentado en un seminario semanal de seguridad informática. A partir de este momento, se inició una posterior lucha entre los virus y antivirus cuyas pautas han venido marcadas por las tendencias en la evolución misma de la tecnología y su impacto sobre las modalidades que van dando resultado en la realización de códigos maliciosos y malas intenciones [21].

A partir del desarrollo del primer virus informático, fueron dándose al mismo tiempo, mecanismos de defensa para evitar estragos que podrían ocasionar dichos virus. Los antivirus fueron la primer herramienta desarrollada para tal fin. Sin embargo, con el paso del tiempo, el asunto de la seguridad fue cobrando más importancia, ya que con el almacenamiento electrónico de la información se hizo necesario el contar con mecanismos que garantizaran su integridad en todo momento.

1.3 Casos recientes de ataques a la seguridad informática

La seguridad de los sistemas de cómputo constituye un problema general en la mayoría de las empresas. De ahí que la protección de los datos se considere un asunto de vital importancia. Por tanto, la pérdida de un archivo o un banco de datos para tener acceso a los recursos computacionales, ocasionada por un error de programación, un acto de sabotaje o un desastre natural, pueden significar la destrucción de una empresa [10].

No solo existen amenazas que se encuentran fuera de la organización, los riesgos pueden estar inclusive dentro de la misma empresa, no necesariamente virus o hackers, pero si puede haber personas malintencionadas que ocasionarían pérdida o robo de información, sabotaje a los sistemas o destrucción de los mismos. También este apartado merece un análisis si es que se desea el mayor nivel de seguridad y específicamente, integridad de la información.

1.3.1 SQL Slammer (Sapphire)

Fue un virus que en tan solo diez minutos recorrió el mundo causando numerosos estragos en el Internet convirtiéndose en el virus informático de mayor velocidad en la historia de la seguridad informática. Este virus impidió el acceso a la red en Corea del Sur y paralizó miles de cajeros automáticos en Estados Unidos; además de duplicar el número de computadoras infectadas cada 8.5 segundos en el primer minuto de su ataque en comparación con el virus Code Red que se había propagado antes duplicando su infección en 37 segundos [23].

Los virus informáticos representan una de las grandes amenazas a la seguridad de los sistemas. El caso anterior expone el riesgo que representa la propagación de un virus poderoso por la red y el peligro que corren los sistemas si no se encuentran debidamente protegidos.

1.3.2 Hacker saquea cuentas de Banamex

Decenas de clientes en el estado de Nuevo León resultaron afectados por un **hacker**[5] que logró desviar dinero de sus cuentas de cheques por un monto cercano a un millón quinientos mil pesos. Se trató de un ladrón cibernético que operaba en varios estados de la República Mexicana. El banco cerró el acceso a sus sistemas, pero no se logró la captura del hacker. Sin embargo, Banamex no ha detenido sus investigaciones pero extraoficialmente se considera que el monto de lo defraudado podría acceder a varios millones de pesos [23].

Este fue uno de los ataques que puso de manifiesto la vulnerabilidad de los sistemas bancarios. Si bien es cierto que se expone el grave peligro que corren las transacciones electrónicas financieras, también es cierto que hace reflexionar sobre la implementación de un plan de seguridad completamente detallado y analítico. Esta experiencia debe fomentar un cambio en la cultura de la seguridad no sólo de los bancos, sino en toda organización.

[5] Persona dedicada principalmente a buscar debilidades dentro de un sistema de cómputo.

Capítulo 2.

Marco teórico conceptual

2.1 Definición de informática

Para el presente término, se tienen las siguientes definiciones:

La informática se puede definir como la ciencia que estudia el tratamiento automático y racional de la información [3].

Rama de la ciencia y de la técnica que trata de la concepción y utilización de los sistemas de transmisión y del procesado de datos [50].

Básicamente, la informática hace su aparición debido a la necesidad de apoyar al hombre en la realización de procesos repetitivos y rutinarios tanto de cálculo matemático como de gestión de datos. Así, tenemos que como ciencia, estudia las operaciones realizadas a la información auxiliándose de programas destinados para tales tareas.

2.1.1 Elementos de la informática

Desde el punto de vista informático, el elemento físico utilizado para el tratamiento de la información es el computador, computadora u ordenador, que se define como la máquina compuesta de elementos físicos, en su mayoría de origen electrónico, capaz de realizar una gran variedad de trabajos a gran velocidad y con gran precisión (Figura 2.1) [3].

Figura 2.1 Elementos físicos de la informática (computadora)

El conjunto de los elementos físicos de la computadora recibe el nombre de hardware. Éstos, son una parte importante de todo sistema informático pues es en ellos donde son implementados los programas y sistemas de comunicaciones con el objetivo de interactuar entre sí o con el exterior.

El conjunto de órdenes que se le dan a una computadora para realizar un proceso determinado se denomina programa, mientras que el conjunto de uno o varios programas más la documentación correspondiente para realizar un determinado trabajo, se denomina aplicación informática (Figura 2.2) [3].

Figura 2.2 Aplicación informática

Este conjunto de programas se le conoce también como software y se ha clasificado en dos categorías: de base y de aplicación. La primera está formada esencialmente por el sistema operativo y la segunda engloba diferentes tipos de aplicaciones (como su nombre lo indica) en donde cada una de ellas realiza una serie definida de tareas según su orientación tales como documentos, cálculos matemáticos, realización páginas de Internet, etc.

El término sistema informático se utiliza para nombrar al conjunto de elementos necesarios (computadora, terminales, impresoras, etc.) para la realización y explotación de aplicaciones informáticas (Figura 2.3) [3].

En general, un sistema informático no es más que la conjunción de los elementos físicos y lógicos dentro de un área de trabajo determinada.

Figura 2.3 Sistema informático

Los datos que maneja un programa son en un principio informaciones no elaboradas y una vez procesados (ordenados, sumados, comparados, etc.) constituye lo que se denomina información útil o simplemente resultados. Para que la información sea tratada necesita transmitirse o trasladarse de un lugar a otro, y para que exista transmisión de información son necesarios tres elementos (Figura 2.4):

- El emisor que da origen a la información.
- El medio que permite la transmisión.
- El receptor que recibe la información.

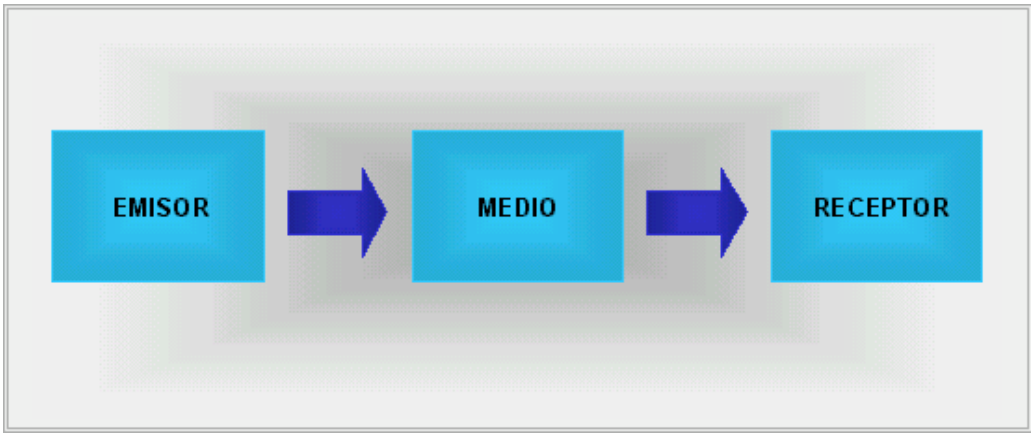

Figura 2.4 Tratamiento de la información

Finalmente, al conjunto de operaciones que se realizan sobre una información se le denomina tratamiento de la información [3].

El proceso de tratamiento de la información requiere de una serie de pasos ordenados para que el objetivo que se busca se cumpla, ejecutándose de manera ordenada y eficaz las operaciones de cada uno de los elementos que componen este sistema.

2.2 Definición de TIC's

Este es un concepto bastante discutido por diferentes autores, sin embargo, seguiremos el concepto dado por Gerstein[6]:

Se refiere a los medios colectivos para reunir y posteriormente almacenar, transmitir, procesar y recuperar electrónicamente palabras, números, imágenes y sonidos, así como a los medios electrónicos para controlar máquinas de toda índole, desde los aparatos de uso cotidiano hasta las vastas fábricas automatizadas [1].

Otra definición, en un sentido más general, pero no por ello menos importante y que complementará a la primera es la siguiente:

Una forma de denominar al conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recogida, almacenamiento, tratamiento, difusión y transmisión de la información [14].

La primera definición lleva el concepto de las TIC's de un modo más analítico mientras que la segunda lo hace de un modo más general y sintetizado. Sin embargo, en ambos conceptos la idea fundamental es la misma: el procesado de todo tipo de datos se ha de llevar de manera electrónica apoyándose en la tecnología desarrollada para tal fin.

[6] **REBOLLOSO,** Gallardo Roberto., La globalización y las nuevas tecnologías de información, Primera Edición, Editorial Trillas, México (2000)

2.3 Evolución de las TIC's

El procesado de información se ha vuelto cada vez más visible e importante en la vida económica, social y política. Una prueba es el rápido crecimiento de las ocupaciones especializadas en actividades concernientes a la información. Por otro lado, el cambio tecnológico está orientado hacia las innovaciones destinadas al guardado y procesado de información, tales como discos duros, flexibles y compactos principalmente [21].

Podemos observar que así como las TIC's llevan consigo una serie de cambios sociales, también traen cambios de orden tecnológico. Por ejemplo, ahora el almacenamiento de datos se realiza en discos destinados específicamente para tal fin y no de modo manual como se realizaba anteriormente, es decir, se lleva a cabo de manera electrónica. En conclusión, la evolución de las TIC's se encuentra orientada hacia la manera en como se trata y procesa la información pasando de manera manual a formas automatizadas auxiliándose específicamente de computadoras.

2.4 Las TIC's y la organización

Las TIC's y la organización se relacionan estrechamente. Aquí destacan algunos aspectos que hay que tener en cuenta:

1. La creación de bases de datos internas que puedan ser usadas a través de los límites funcionales.
2. El establecimiento de correo electrónico.
3. La conexión con las bases de datos internas y los tableros de anuncios electrónicos externos a la firma.
4. El uso extenso del intercambio electrónico de datos para convertir en rutina y automatizar las transacciones con el exterior [1].

Las TIC's se relacionan profundamente con la organización y su estructura jerárquica. La influencia que ejercen sobre ésta última resulta muy importante ya que trae como consecuencia un cambio no sólo a sus procesos cotidianos, sino que además permiten cambios radicales en su manera de

interactuar con otras corporaciones, sustitución de métodos manuales por métodos electrónicos tales como la implantación del correo electrónico entre otros servicios.

2.5 Potencial de las TIC's

La evolución de las TIC's nos brinda un nuevo conjunto de capacidades que antes no teníamos, entre las cuales se mencionan las siguientes:

- *Capacidad de acceso.* Las TIC's hacen posible que un mayor número de usuarios accesen gran cantidad de datos o información a un mayor nivel de detalle.
- *Capacidad de captura.* Las TIC's permiten capturar y utilizar información que anteriormente hubiera sido imposible o incosteable contener.
- *Capacidad de transmisión y procesamiento.* Las evolución de las TIC's ha hecho posible contar ahora con dispositivos de gran poder de procesamiento que pueden realizar cálculos, manejar símbolos y apoyar la toma de decisiones en las organizaciones. Esto ha traído consigo el manejo digital de diferentes tipos de información y una mayor convergencia entre la computación y telecomunicaciones.
- *Capacidad de almacenamiento.* Las TIC's permiten almacenar grandes cantidades de información por periodos ilimitados de tiempo reduciendo el espacio requerido para almacenarla, el tiempo requerido para clasificarla y el tiempo necesario para recuperarla.
- *Capacidad de duplicación.* Las TIC's permiten duplicar información y programas para procesar esta información, no sólo de una manera más rápida o simplificada, sino haciendo esto posible en instancias que antes no existían.
- *Capacidad de rastreo.* Las TIC's permiten seguir paso a paso las transacciones realizadas a lo largo de un determinado proceso o llevar un registro periódico de la posición de vehículos, materiales o personas.
- *Capacidad de combinación.* Gracias a las capacidades señaladas anteriormente, la evolución de las TIC's permite que ahora se combinen piezas de información para obtener nueva información; es

decir, el conjunto de estas piezas proporciona más información que la suma de ellas [2].

Podemos ver que las TIC's ofrecen una serie de ventajas sobre el tradicional proceso de datos. Las operaciones de captura, manipulación y presentación de información se puede hacer de una manera más rápida y efectiva; el almacenamiento ha adquirido un nivel de seguridad más alto y podemos duplicar o combinar esta información según se tenga deseado. En resultado, se obtendrá una mejora considerable en el actuar de las organizaciones en general.

2.5.1 Ventajas competitivas de las TIC's

Se considera a las TIC's como tecnologías de infraestructura, es decir, se utilizan para procesar, almacenar y transportar información de manera digital. Estos recursos tangibles son fáciles de copiar y de adquirir, de tal manera que se podrían considerar de escaso valor estratégico. Sin embargo también es sabido que las TIC's aportan otros recursos intangibles como la generación de conocimiento, la creación de sinergias, la gestión del saber hacer o la transformación de los procesos. Estos recursos son considerados el fruto de importantes ventajas competitivas [19].

El peso específico de los sistemas y programas informáticos donde se centraban tradicionalmente las TIC's, se han desplazado hacia una visión más moderna, donde han ido cobrando mayor importancia las personas que hay detrás de cada ordenador y en la información generada a través de las relaciones con otros empleados o terceras personas [ídem].

La generación de ventajas competitivas a partir de la inversión en TIC's dependerá principalmente del uso que se haga de la información dentro de las organizaciones. A partir de este punto, será necesario desarrollar nuevos sistemas de procesamiento de datos, esto con el fin de que la empresa refuerce y mejore operaciones de interacción con el medio ambiente y dentro de ella.

2.6 Tendencias de las TIC's

La incorporación de las computadoras en las organizaciones ha pasado por cuatro fases: grandes computadoras centrales, computadoras personales y procesamiento de datos distribuido, la red de las microcomputadoras y la red de redes. Cada una de estas fases ha mejorado la anterior, sin embargo podemos observar nuevas características entre las que se encuentran:

- Digitalización de los datos.
- Constante renovación de la interfaz del usuario.
- Incremento de la movilidad para las TIC's.
- Especialización, miniaturización y dispersión de las TIC's.
- La red de redes [1].

Con estas nuevas tendencias, las TIC's se está moviendo en dos direcciones contrastantes: hacia una gran especialización y una mayor diversidad. En cuanto a la especialización en el trabajo de oficina, de alguna manera reduce cierto tipo de trabajo y ofrece la posibilidad de desarrollar otro. Otra tendencia es la adopción de computadoras en las actividades diarias de la gente que tiene poco interés en estos asuntos por lo que habrá una adaptación masiva [ídem].

La implementación de TIC's está creando una serie de nuevas tendencias. Cambios en la estructura de las corporaciones, generación de información, automatización de tareas, etc. Sin embargo, todos estos factores convergen en un mismo punto: aumentar la productividad y competitividad organizacional que, hoy día, resulta determinante para toda organización.

2.6.1 Tendencias de software, hardware y comunicaciones

En particular, las TIC's seguirán las siguientes tendencias en lo que a software, hardware y comunicaciones se refiere:

1. El hardware y software para reconocimiento de escritura y las plumas electrónicas tendrán un desarrollo importante. Las tecnologías de multimedia diseñadas para combinar video, animación, fotografía, voz,

música, gráficos y texto, tendrán una mayor penetración que en años anteriores; nuevas tecnologías para la realidad virtual que permitan a los usuarios interactuar con ambientes tridimensionales generados por computadora se utilizarán para desarrollar aplicaciones. Algunas áreas de la inteligencia artificial, en particular los sistemas basados en conocimiento; las herramientas para el procesamiento del lenguaje natural y las aplicaciones de redes neuronales y de lógica difusa continuarán en expansión hacia nuevas aplicaciones.

2. Nuevas herramientas, sistemas operativos y librerías orientadas a objetos que permitirán reutilizar software, desarrollarlo con mayor velocidad y facilitar su mantenimiento [1].

Como se ha visto, las tendencias que siguen las TIC's están orientadas generalmente hacia un cambio en la manipulación, envío y recepción de datos haciéndose todas estas operaciones de manera electrónica y apoyándose en la vanguardia tecnológica.

2.7 Reingeniería de las TIC's

De acuerdo con Donald A Shön[7], la reingeniería viene a ser un modelo enteramente respaldado en las nuevas formas de organización, como producto de las TIC's. Los procesos de reingeniería dependen totalmente de la información para poder ejercer un cambio en las organizaciones. En el fondo de todo, la informática subyace de diferentes maneras, de acuerdo con los intereses de cada empresa. En consecuencia, podemos concluir que el papel de la informática es determinante para la organización por las siguientes razones:

- El desarrollo de nuevas formas de organización.
- El descubrimiento de nuevos potenciales a raíz del avance de las innovaciones tecnológicas.
- La flexibilidad en el acceso de la información [2].

[7] ZOLONDZ, Vogel Alfredo., Nuevas Tecnologías de Información, Editorial EDAMEX, México (2001)

La reingeniería es el replanteamiento de ideas y operaciones con el objetivo de mejorar la situación actual de la organización y su importancia resulta vital, ya que el mejoramiento de los procesos tecnológicos y gestión de datos determinará a largo plazo, el éxito de la organización que las lleva a cabo.

2.8 Retos comunicativos de las TIC's

La comunicación es imprescindible para el buen funcionamiento de toda organización. Es preciso tomar en cuenta la manera en como la empresa se nutre de la información, y cómo se vale de las TIC's para establecer su plan de comunicación interna. La incorporación de las nuevas tecnologías informáticas precisa modificaciones estructurales, organizativas y comportamentales tales como estructuras jerárquicas más horizontales (figura 2.5) [16].

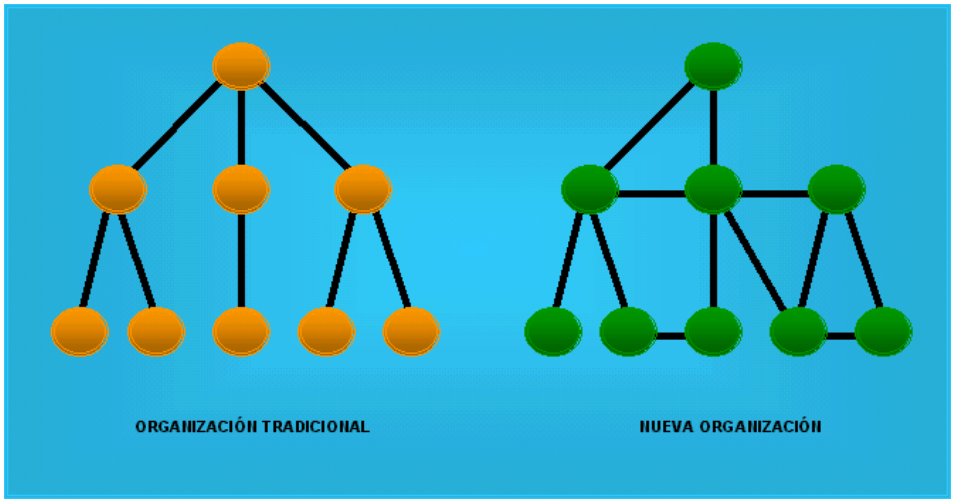

Figura 2.5 Impacto de las TIC's en la estructura jerárquica

2.9 TIC's y seguridad informática

La masiva utilización de TIC's cuestiona la confianza y seguridad de los sistemas y productos informáticos y electrónicos en una sociedad que depende cada vez más de ellos. Ante esta situación, se está asistiendo a los primeros pasos para la construcción de la confianza tanto en los sistemas de información como en las posibles interacciones de los mismos [16].

Como ya hemos visto, las TIC's deben almacenar y procesar información. Del mismo modo deben considerar los siguientes riesgos:

- Riesgo de filtración: los datos confidenciales deben ser tratados de tal manera que el acceso a ellos sea posible exclusivamente para las personas e instituciones autorizadas.
- Riesgo de imposibilidad de Acceso: los datos deben ser almacenados de tal forma que el acceso a ellos por parte de las personas e instituciones autorizadas esté garantizado durante toda la vida útil de la información.
- Riesgo de manipulación: la modificación de los datos debe estar restringida, nuevamente, a las personas e instituciones autorizadas [17].

Los procedimientos de firma digital y de encriptamiento son elementos que hoy en día no se puede dejar de considerar en todo lo que tiene que ver con seguridad informática. Los **hackers**, hoy son una realidad inocultable. Estos "rompedores de sistemas" y productores intelectuales de virus informáticos son personas que se dedican a hacer caer sistemas y programas. Lo anterior desencadena la decisión de tomar medidas de seguridad suficientes para limitar el accionar de hackers y virus, protegiendo de esta forma el sistema y a los usuarios del mismo [22].

Las tres principales amenazas hacia la seguridad informática deben ser tomadas en cuenta muy seriamente. No hay que olvidar que cualquier sistema puede estar vulnerable a los ataques de hackers y virus informáticos. Por consiguiente, cuando los datos tengan que ser procesados y se tenga que compartir información, se deben tener todas las medidas de seguridad correspondientes para evitar el daño, robo o manipulación de ésta.

Capítulo 3.

Riesgos informáticos

3.1 Planeación y dirección de las TIC's y la seguridad informática

Planeación, estrategia y TIC's son tres elementos de gran importancia para las organizaciones de nuestro tiempo, por si solos son principios básicos en la gestión de las empresas modernas y competitivas, pero aplicados de manera conjunta y ordenada logran una sinergia que aporta gran valor a las organizaciones. El reto es establecer como haciendo planeación, usando estrategia y aplicando las TIC's podemos establecer proyectos que nos permitan capitalizar las oportunidades que se presenten en las épocas difíciles. Se debe comenzar llevando a cabo un ejercicio de planeación estratégica que determine hacia donde queremos llevar a nuestra organización, es fundamental que los objetivos estratégicos establecidos en este ejercicio tengan la característica de ser cuantificables, es decir que se puedan medir [29].

El proceso de planeación de TIC's tiene por objetivo asegurar que las metas establecidas por la organización se cumplan. Todo lo que se invierta en estas TIC's deben de generar resultados, mismos que producirán beneficios a la empresa. Lo anterior contribuirá a lograr una ventaja competitiva y productiva que será regulada y dirigida por los altos mandos de la corporación.

3.1.1 Computación empresarial

Hoy día, casi todas las organizaciones han reconocido la importancia de las PC's en la estructura de la computación. En la era de las redes, el reto para el gerente de sistemas de información (o de informática) es integrar todo tipo de computadoras en un solo sistema uniforme. Esta estrategia, denominada computación empresarial, permite que las estaciones de trabajo, minicomputadoras y macrocomputadoras se complementen [5].

La computación empresarial es una nueva tendencia que viene a emplearse en todos los niveles jerárquicos de las empresas. Los diferentes departamentos necesitan de computadoras para la realización de sus actividades diarias: ya sean tareas de estados financieros, diseño y publicidad electrónica, generación de bases de datos y presentación de informes e inventarios.

3.1.2 Planeación de la seguridad

Se debe identificar que es lo que se va a proteger, por tanto se tiene los siguientes pasos a ejecutar:

- Lista de objetos a definir como son las computadoras, el software, los routers y los cables entre otros.
- Categorizarlos.
- Asignar una métrica.
- Priorizar: asignar cuál es el más importante [27].

Planear la seguridad resulta un asunto bastante delicado. Este método de planeación requiere seguir una serie de pasos ordenados y bien definidos para lograr el objetivo. En primer lugar se debe tomar en cuenta a todos los elementos que se desea proteger, analizando las características respectivas de cada uno de ellos; posteriormente se clasificarán según su tipo y sus actividades que desempeñan; de este modo, se debe incluir un período de prueba y entrenamiento a cada elemento para, finalmente, definir las prioridades que estarán regidas por las iniciativas de la empresa misma.

3.1.3 Análisis de las amenazas a la seguridad informática

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios [24].

Las cuatro categorías generales de amenazas o ataques son las siguientes:

- *Interrupción*: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

- *Intercepción*: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).
- *Modificación*: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- *Fabricación*: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo [ídem].

La clasificación anterior es la más general en cuanto a tipo de amenazas se refiere. Cada una de ellas pone en riesgo a las diferentes características que debe tener la información para su seguridad, tales son la autenticidad, confidencialidad, disponibilidad e integridad. El análisis de estas amenazas es diseñado por los especialistas en sistemas que habrán de tomar en cuenta a cada una de ellas y determinar que acciones deberán seguir dependiendo del tipo de ataque que no es más que la realización de una amenaza.

3.1.3.1 Ataques pasivos

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

- *Obtención del origen y destinatario de la comunicación*, leyendo las cabeceras de los paquetes monitorizados.
- *Control del volumen de tráfico* intercambiado entre las entidades monitorizadas, 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 [24].

Este tipo de ataques no tienen por objeto la destrucción de la información, sino la visualización y el robo de la misma. Además, son muy difíciles de que sean detectados puesto que no producen anomalías de los datos ni en el canal de comunicación. Aun así, pueden evitarse estos ataques con operaciones de encriptamiento de datos principalmente.

3.1.3.2 Ataques activos

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

- *Suplantación de identidad:* el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- *Reactuación:* uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- *Modificación de mensajes*: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
- *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*, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc. [24].

Los ataques activos resultan más peligrosos que los pasivos. Aquí, los objetivos que se siguen son la modificación, pérdida y robo de la información. Existen mecanismos para contrarrestar estos ataques como la implementación de firewalls.

3.2 Tipos de riesgos informáticos

Las empresas relacionadas con la informática se encuentran expuestas a una serie de riesgos que a continuación se describirán.

3.2.1 Riesgos de integridad

- *Interfase del usuario:* Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio / sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones. Otros riesgos en esta área se relacionan a controles que aseguren la validez y completitud de la información introducida dentro de un sistema.
- *Procesamiento:* Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.
- *Procesamiento de errores:* Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada / proceso de información de errores (*Exceptions)* sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

- *Interfase:* Los riesgos en esta área generalmente se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.
- *Administración de cambios:* Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuadas de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.
- *Información:* Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos. La integridad puede perderse por: Errores de programación (*buena información es procesada por programas mal construidos)*, procesamiento de errores (*transacciones incorrectamente procesadas)* ó administración y procesamiento de errores (*Administración pobre del mantenimiento de sistemas)* [30].

Los riesgos de integridad están orientados hacia el proceso de tratamiento de información, puesto que atentan contra la seguridad en las operaciones de generación, modificación y presentación de grandes cantidades de datos.

3.2.2 Riesgos de relación

Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones [30].

La concreción de estos riesgos repercute en la actividad de toma de decisiones ya que, alteran los datos en el momento justo antes de tomar la decisión correcta.

3.2.3 Riesgos de acceso

- *Procesos de negocio:* Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.
- *Aplicación:* La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.
- *Administración de la información:* El mecanismo provee a los usuarios acceso a la información específica del entorno.
- *Entorno de procesamiento:* Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.
- *Redes:* En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.
- *Nivel físico:* Protección física de dispositivos y un apropiado acceso a ellos [30].

Como su nombre lo indica, este tipo de riesgos atentan contra el uso inapropiado de los sistemas en general. Por consecuencia principal se tendrían bases da datos alteradas.

3.2.4 Riesgos de utilidad

Estos riesgos se enfocan en tres diferentes niveles:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación y restauración usadas para minimizar la ruptura de los sistemas.
- Backups[8] y planes de contingencia controlan desastres en el procesamiento de la información [30].

Los riesgos de utilidad están enfocados hacia los mecanismos de seguridad que son implementados en los sistemas. Incluyen a los planes de

[8] Copia completa de información que estará disponible en caso de pérdida o modificación.

recuperación en casos de desastres y los manuales de seguridad de los sistemas en sí.

3.2.5 Riesgos de infraestructura

- *Planeación organizacional:* Los proceso en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio. Además, verifica si existe una adecuada organización (*gente y procesos)* asegura que los esfuerzos de la tecnología informática será exitosa.
- *Definición de las aplicaciones:* Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio. Estos procesos abarcan: la determinación de comprar una aplicación ya existente ó desarrollar soluciones a cliente. Estos procesos también aseguran que cualquier cambio a las aplicaciones (*compradas o desarrolladas)* sigue un proceso definido que confirma que los puntos críticos del proceso control son consistentes (*Todos los cambios son examinados por usuarios antes de la implementación).*
- *Administración de seguridad:* Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.
- *Operaciones de red y computacionales:* Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado. También aseguran que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.
- *Administración de sistemas de bases de datos:* Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de

definición, correspondan con los requerimientos y reduzcan el potencial de redundancia.

- *Información / Negocio:* Los proceso en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan [30].

Estos riesgos hacen referencia a la mala estructura de tecnología dentro de la organización tal como software, hardware, redes y procesos en general y que tendrá consecuencias graves a largo plazo. Del mismo modo, los riesgos de infraestructura cubren las operaciones de generación y mantenimiento de información que son presentadas mediante alguna aplicación informática tales como presentación de inventarios o balances generales.

3.2.6 Riesgos de seguridad general

- *Riesgos de choque eléctrico:* Niveles altos de voltaje.
- *Riesgos de incendio:* Inflamabilidad de materiales.
- *Riesgos de niveles inadecuados de energía eléctrica.*
- *Riesgos de radiaciones:* Ondas de ruido, de láser y ultrasónicas.
- *Riesgos mecánicos:* Inestabilidad de las piezas eléctricas [30].

Los riesgos de seguridad general están enfocados hacia el entorno físico en donde los sistemas se encuentran establecidos. Definen los siniestros de los cuales pudieran ser víctima como incendios, inundaciones, descargas eléctricas o exposición a radiaciones.

Capítulo 4.

Elementos de seguridad informática

4.1 Preparación de espacios

La preparación de espacios representa el preámbulo de la planeación de la seguridad. Este es el primer punto importante a tratar antes de la seguridad del software, hardware y comunicaciones ya que es en donde estarán concentrados todos estos elementos.

4.1.1 El edificio

El estudio del edificio donde se encontrarán ubicado los sistemas es el primer paso en cualquier estudio de seguridad, y también suele ser el más problemático, puesto que nos encontramos con un entorno ya construido, no modificable y que suele tener un uso compartido por nuestros sistemas hardware y otro tipo de sistemas. Se intentará siempre resaltar todos los fallos de seguridad que se puedan encontrar, y se tendrá en cuenta si éstos son subsanables o inherentes a la estructura del edificio [25].

El estudio del edificio se realizará para elaborar un informe detallado en donde se expongan los detalles que pudieran ser modificados para minimizar riesgos de seguridad general a los sistemas.

4.1.2 Suministros de energía del edificio

El primero de los puntos que debemos observar al realizar el estudio del edificio es el suministro de energía. Debemos centrarnos en los sistemas de suministro de energía que puedan afectar a los sistemas que queremos proteger, dejando de lado otras consideraciones como la disponibilidad de servicios para el personal y similares. El suministro de gas y agua es menos crítico que el suministro de energía eléctrica para la seguridad de los sistemas hardware del edificio. Debe tenerse en cuenta el suministro de gas porque algunos sistemas de calefacción funcionan con gas, y pueden ser necesarios en climas muy fríos para mantener una temperatura mínima en nuestros centros de datos. El frío no suele ser un problema para los sistemas hardware, por lo que el gas no será una preocupación en la mayor parte de los casos [25].

Los suministros de energía no sólo se enfocan al cableado eléctrico, sino que también es necesario revisar sistemas de gas y de agua. Sin embargo, en todos ellos se deberá realizar un análisis de su estado general así como tener en cuenta las posibilidades de ataques a la seguridad física. Es conveniente realizar revisiones periódicas a cada uno de éstos sistemas para garantizar su óptimo funcionamiento.

4.1.2.1 Sistemas UPS

Es necesario instalar una fuente de energía ininterrumpida o UPS[9], esto es cuando trabajamos con datos muy valiosos o delicados en la PC. Después del regulador o UPS se conecta la computadora. Si el regulador no tiene las salidas o tomacorrientes necesarios para conectar todos los cables, habrá que adicionarle una multitoma con 4 o 6 posiciones adicionales y a éste conectar la PC. Los UPS tienen baterías que en caso de un corte de energía, le permiten continuar trabajando con la PC durante algunos minutos (entre 5 y 15 minutos aproximadamente). Entre más capacidad tenga un UPS y menos dispositivos tenga conectados, más tiempo tendrá para continuar trabajando. Generalmente, los UPS son como los que se muestran en la figura 4.1: [40].

Figura 4.1 Sistema UPS para equipos de cómputo

[9] Uninterruptible Power Supply.

Los sistemas UPS ofrecen un apoyo considerable durante el proceso de generación de información. Resulta indispensable para toda organización contar con este tipo de sistemas que nos ofrecen numerosas ventajas en caso de fallas eléctricas como evitar la pérdida de información o daño a los componentes físicos de los equipos de cómputo.

4.2 Seguridad física

4.2.1 Accesos físicos al edificio

Debemos tener en cuenta que el edificio tiene una serie de accesos obvios y otros no tan obvios que un intruso puede usar para entrar en nuestras instalaciones. Los obvios son las puertas principales de acceso y las ventanas que se encuentran cercanas a la calle. Los no tan obvios son las puertas de servicio, las ventanas superiores, las claraboyas, los accesos de mantenimiento o los sistemas de ventilación o calefacción [25].

Analizar cada uno de los accesos físicos al edificio es una de las primeras tareas del especialista en seguridad informática. Se debe asegurar por todos los medios posibles, el acceso a potenciales personas malintencionadas que pudieran causar daños severos a los sistemas informáticos. Algunas formas son colocando rejas protectoras en los accesos principales al lugar donde se encuentren concentradas las computadoras y teniendo personal humano de seguridad que impida el acceso a toda persona no autorizada.

4.2.2 Acceso al site

El site[10] debe tener un sistema de acceso suficientemente seguro, preferiblemente con una puerta blindada y siempre que sea posible con personal de vigilancia que compruebe el acceso por medio de tarjetas de identificación o medios similares [25].

El acceso al site debe ser lo más seguro posible ya que es en ese lugar donde se encuentran concentrados los principales sistemas informáticos de toda la organización. Se debe revisar de manera periódica que la puerta se encuentre en buenas condiciones, así como su cerradura.

[10] Área de trabajo donde se encuentran concentrados los servidores de datos.

4.2.3 Control de la temperatura

A mayor temperatura menor tiempo entre fallos para todos los dispositivos electrónicos, incluidos los ordenadores, los dispositivos de red y cualquier sistema que genere por sí mismo calor. Aún así, es conveniente poseer ventiladores y sistemas de climatización artificial dentro del lugar donde trabajen los equipos de cómputo (Figura 4.2) [25].

Figura 4.2 Ventilador utilizado dentro de las áreas de cómputo

Generalmente los equipos de cómputo poseen ventiladores para sus procesadores y su fuente de energía (Figura 4.3). Esto garantiza el funcionamiento correcto del dispositivo.

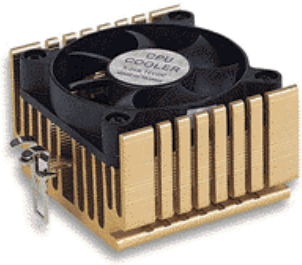

Figura 4.3 Ventilador para procesador

Los sistemas de climatización artificial desempeñan un papel importante dentro del área de trabajo teniendo como objetivo principal mantener la temperatura adecuada. Por su parte, las computadoras poseen ventiladores en sus procesadores y fuentes de energía para evitar el calentamiento excesivo de estos dispositivos.

4.2.4 Seguridad física del cableado

La seguridad física del cableado comprende principalmente el fallo de fabricación que pudiera tener éste o los daños que pudiera sufrir por una persona malintencionada. Por lo anterior, resulta conveniente realizar revisiones periódicas de su estado.

4.2.4.1 Cableado eléctrico

Se deberá estudiar el cableado que proporciona energía a nuestros sistemas computacionales y dispositivos de red e incluso otro tipo de dispositivos como impresoras ó faxes. Habrá que estudiar que los enchufes y clavijas donde se conectan los dispositivos cumplen con las normativas aplicables y que no existe peligro de que pueda saltar una chispa entre terminales [25].

El cableado eléctrico deberá cumplir con los requerimientos de la organización. Éste deberá ser de un solo polo (Figura 4.4)

Figura 4.4 Cable eléctrico utilizado para el suministro de energía

El cableado eléctrico es un punto muy importante ya que por este medio los equipos de cómputo recibirán energía eléctrica. Se debe tomar en consideración revisiones periódicas del estado actual del cableado y realizar las operaciones de mantenimiento necesarias con el objetivo de asegurar siempre la integridad de las computadoras y por ende, de la información que almacenan, manipulan e intercambian.

El estado de los enchufes a los cuales se conectan los sistemas deberán estar en buenas condiciones y éstos deberán ser aterrizados para evitar descargas eléctricas a los equipos de cómputo. (Figura 4.5)

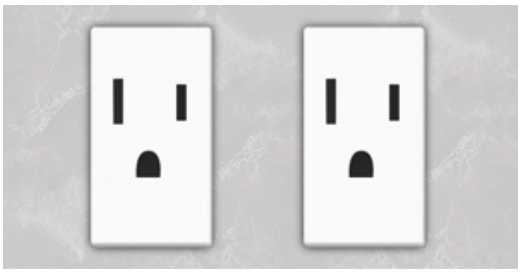

Figura 4.5 Tomacorriente aterrizado

4.2.4.2 Cableado telefónico

Es aconsejable que el cableado telefónico se mantenga lejos del cableado eléctrico que transporte mucha potencia. Por lo demás el cableado de telefonía no suele dar problemas, más que los puramente físicos como seccionamientos del cable, conectores mal montados o defectuosos [25].

Por lo general, el cableado telefónico utilizado es de cuatro hilos (Figura 4.6)

Figura 4.6 Cable telefónico

4.2.4.3 Cableado de red

El cable de red **Ethernet**[11] normal a 10Mbps o 100Mbps (Figura 4.7) que se suele instalar en las redes departamentales o locales deberá ser observado de que esté protegido mediante entubado o integrado en la estructura del edificio, además de revisar que no se encuentre cercano a conducciones de electricidad de alta potencia que puedan crear interferencias

[11] Red de área local de alta velocidad.

electromagnéticas sobre él. Se deberán tomar las medidas precisas para evitar el supuesto seccionamiento del cable por parte de un intruso malintencionado [25].

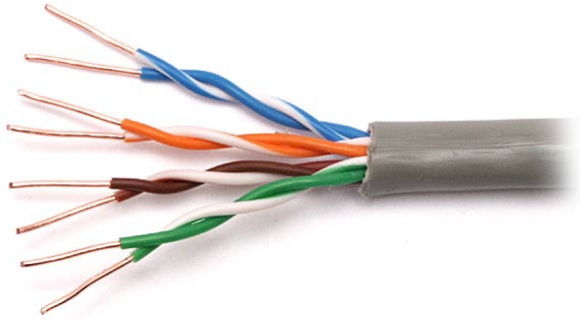

Figura 4.7 Cable UTP categoría 5 para redes Ethernet

Por lo general, este tipo de cable utiliza conectores de tipo RJ-45, los cuales se muestran en la siguiente figura:

Figura 4.8 Conectores RJ-45

4.2.5 Seguridad contra incendios y otros desastres

Los sistemas de seguridad contra incendios y otros desastres naturales deben ser instalados normalmente cuando el edificio es construido. Dentro de estos sistemas se encuentran los extintores, detectores de humos y señalamientos que nos indicarán las acciones a realizar en caso de alguna contingencia.

4.2.5.1 Extintores

Los sistemas de detección de incendios pueden ser instalados después de construido el edificio y no suponen una gran inversión, pueden avisar rápidamente de pequeños incendios y permitir al personal el sofocarlos antes de que alcancen mayor entidad [25].

El tipo de extintores que se deberán utilizar serán de CO2 o de espuma puesto que el agua representa un riesgo importante hacia los componentes físicos de la computadora. (Figura 4.9)

Figura 4.9 Extintor de CO2

4.2.5.2 Detectores de humo

Los detectores de humo se clasifican en las siguientes categorías:

- *Los ópticos o fotoeléctricos.* Detectan el humo utilizando los efectos que éste produce sobre la luz. Existen varios tipos, entre los que destacan los basados en el oscurecimiento de la luz y en su difusión. (Figura 4.10) [39].

Figura 4.10 Detector de humo fotoeléctrico

Los detectores por ionización. Funcionan por sensibilidad a la humedad, la presión atmosférica y las partículas suspendidas en el aire. Reaccionan rápidamente si hay humo (incluso no visible) y son más baratos que los de tipo fotoeléctrico que, sin embargo, dan menos falsas alarmas. (Figura 4.11) [ídem]

Figura 4.11 Detector de humo por ionización

La selección e instalación de detectores de humo tendrá en consideración las características de diseño del detector y las zonas en que se van a instalar, de forma que se eviten falsas alarmas o el no funcionamiento después de su instalación [38].

Los detectores de humo son un componente de seguridad necesario. Dependiendo de las necesidades que persiga la organización, se elegirá el tipo de dispositivo a utilizar aunque es siempre conveniente que la empresa posea ambos tipos de detectores.

4.2.5.3 Señalamientos

Son los elementos gráficos que nos indican las restricciones o prevenciones de un lugar para evitar un accidente o en caso de que éste se presente como enfrentarlo tales como incendios, sismos o inundaciones [40].

El principal señalamiento que debe tener el área informática es mostrar la ruta de evacuación (Figura 4.12). No menos importante resultan los señalamientos que muestran las acciones a realizar en caso de alguna contingencia.

Figura 4.12 Señalamiento común en áreas de cómputo

4.3 Aspectos principales para la seguridad de la información

La seguridad informática tiene como objetivo el mantenimiento de la confidencialidad, integridad y disponibilidad de los sistemas de información. Es necesario identificar y controlar cualquier evento que pueda afectar negativamente a estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias. Para ello, deben utilizarse métodos formales de análisis de riesgos que lo garanticen [26].

La confidencialidad, integridad y disponibilidad representan los aspectos más relevantes que se deben tomar muy en cuenta en toda organización que desea implementar un sistema de seguridad hacia la información que procesan y manipulan. La correcta identificación de amenazas así como la puesta en marcha de mecanismos que garanticen su seguridad deben ser cubiertas por personal altamente profesional en esta materia.

4.3.1 Confidencialidad

Protege los activos de información contra accesos o divulgación no autorizados; es decir, debe garantizar que los datos que se envían en los formularios de la transacción sólo serán visualizados por usuario y servidor; que nadie, en un paso intermedio podrá tener acceso a dicha información [26].

La confidencial se enfoca hacia la visualización de la información sólo por la o las personas que tengan los privilegios necesarios para poder tener acceso a ella.

4.3.2 Integridad

Garantiza la exactitud de los activos de información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta [26]. En otras palabras, la integridad debe asegurar que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor [33].

La integridad se encuentra orientada hacia la presentación correcta de los datos. Considera el hecho de que la información que es enviada hacia un destinatario será la misma que posea el remitente de ésta.

4.3.3 Disponibilidad

Asegura que los recursos informáticos y los activos de información pueden ser utilizados en la forma y tiempo requeridos [26]. Este aspecto debe garantizar que el sistema de computación esté disponible a las partes autorizadas siempre que sea requerido y no existan problemas de caída o funcionamiento dudoso de las máquinas que prestan el servicio [33].

El apartado de la disponibilidad se refiere a que en todo momento que se requiera obtener la información o tan solo tener acceso a ella se lleve a cabo sin contratiempo alguno. Del mismo modo, el sistema que ofrecerá éste y otros servicios se encontrará siempre en las condiciones necesarias para llevar a cabo sus respectivas operaciones de funcionamiento.

4.3.4 Seguridad de los backups y alojamiento de datos

El sistema más eficaz para mantener los backups seguros es mantenerlos fuera del edificio, o al menos mantener una copia de éstos, ya sea en otro edificio o en un centro de almacenamiento de backups. Estos últimos son centros que proporcionan almacenamiento de las cintas de backup con todas las medidas de seguridad física imaginables y que son una buena alternativa

al mantenimiento de los backups cerca de las máquinas de las que se ha hecho éste. La elección de un sistema de alojamiento para backups es una decisión del personal de administración, teniendo en cuenta una serie de razones como la necesidad de disponibilidad inmediata de los backups o el tiempo que éstos deben almacenarse. Como regla general deberemos mantener al menos una copia de los backups principales fuera del edificio, o incluso mantener fuera todos los backups [25].

La seguridad de los backups dependerá de los planes que se lleven a cabo, sin embargo es recomendable que éstos se encuentren fuera de la organización, puesto que dentro de ella corren riesgos como siniestros o robos. La mejor opción para mantenerlos es teniéndolos en un lugar alterno en donde puedan ser actualizados periódicamente.

4.4 Seguridad del software

Se refiere a controles lógicos dentro del software que se implementa mediante la construcción de contraseñas en diversos niveles del sistema donde permita solo el acceso en base a niveles de seguridad de usuarios con permiso. Para asegurar el éxito del sistema es necesario establecer campañas constantes sobre la funcionalidad y logros que se alcanzarán con el sistema los cuales puedan crear una conciencia en el usuario y lograr formar en él un interés en el uso del sistema mediante boletines, videos y conferencias que no entren en el adiestramiento sino que sirvan para reforzar el uso hacia el sistema por parte de los usuarios [31].

Básicamente, la seguridad del software se enfoca hacia la implementación de contraseñas dentro de un sistema que garantice la disponibilidad, integridad y confidencialidad de la información. Otra tarea importante para el diseñador del sistema es realizar un análisis acerca del funcionamiento del sistema por parte de los usuarios que tienen acceso a él y su nivel de privilegio que poseen para poder detectar posibles fallos o problemas que pudiera tener.

4.4.1 Calidad del software

El software, tanto en su vertiente de producto como de aplicación, conlleva una serie de especificidades con relación a la calidad. Si intentamos detallar lo que entendemos por calidad del software tendríamos que hablar de:

- *Funcionamiento.* El software debe funcionar siempre, en todo momento; debe permitirnos utilizarlo cuando sea necesario.
- *Funcionalidad.* El software deberá cubrir las funcionalidades que publica; en resumen, debe hacer lo que dice que hace. En este punto es importante el recubrimiento, las facilidades para conocerlo. El usuario de una aplicación o producto software muchas veces no dispone de la información suficiente para realizar aquellas tareas para las que fue adquirido, simplemente por la ausencia de un manual de usuario completa.
- *Usabilidad.* No sólo el software debe hacer lo que dice que hace; también debe permitirnos hacerlo de forma adecuada, natural. Si para realizar una acción tenemos que apretar tres botones simultáneamente, y ésta información se encuentra escondida en un manual complejo y mal redactado, la consecuencia es que el usuario no conseguirá su objetivo y asociará el producto con un nivel de calidad inferior al supuesto [7].

Con lo anterior expuesto, se concluye que la calidad del software aborda tres características que éste deberá cubrir: se deberá observar que funcione como deseamos, que sea fácil de operar y que sus opciones se realicen de la forma más intuitiva posible para el usuario.

4.4.2 Antivirus

Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominado *malware*). Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la

búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras [10].

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real [44].

Al elegir un programa antivirus, primero debe tenerse en cuenta el tipo de hardware (una estación independiente o una red), el tipo de información manejada y el nivel de seguridad deseado. Por este motivo, es importante evaluar las opciones de acuerdo con los siguientes criterios:

- Asegurarse de que el software sea compatible con el sistema operativo y los demás programas instalados en el sistema de cómputo.
- Asegurarse de que el programa elegido sea fácil de usar y que no requiera de amplios conocimientos técnicos.
- Leer la documentación incluida en el programa para verificar que esté completa y sea comprensible.
- Asegurarse de que los programas de detección operen de manera efectiva y no se activen sin necesidad.
- Evaluar el tiempo requerido por el programa para ejecutar las tareas de localización y destrucción, a fin de comprobar que no reduzca la velocidad de procesamiento del sistema.
- Consultar a otros usuarios que hayan usado programas antivirus sobre los resultados obtenidos.
- Asegurarse de actualizar el programa con frecuencia para incluir las nuevas formas de virus identificadas [10].

Los programas antivirus resultan una herramienta de suma importancia dentro de los sistemas que manejan grandes cantidades de información. Existen muchos tipos de antivirus, sin embargo debemos elegir el que más se acerque a nuestras necesidades. La interacción con otras estaciones de trabajo, el compartir información y el estar trabajando dentro de una red, son factores que se deben considerar en la elección del software antivirus.

Aún cubriendo todas estas especificaciones, un sistema nunca será completamente infalible por lo que siempre es necesario realizar todas las operaciones de manipulación de datos e interacción con otras computadoras de una manera completamente profesional.

4.4.3 Spyware

El spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados, recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono [41].

El spyware no es un virus en sí, pero si trae consecuencias en la computadora donde se aloja como la merma de rendimiento del sistema, problemas de estabilidad y dificultad para conectarse a Internet. El spyware no se duplica dentro de las máquinas sino que funciona solo como un parásito dentro de ella. Para eliminar el spyware existen diferentes aplicaciones informáticas que resultan de gran utilidad (ver Anexo 1).

4.5 Seguridad del hardware

Entendemos como seguridad del hardware al entorno en el que está situado nuestro hardware, dispositivos de red y centros de computación. Comprende el estudio de su localización, el acceso físico que las personas puedan tener a éste, todo el cableado que lo interconecta o que le provee de energía, el control de la temperatura y demás condiciones climáticas del entorno donde se encuentre, así como el estudio del tipo de montaje de este hardware dentro de la infraestructura y los métodos de administración y gestión del cual es objeto y de su entorno [25].

Del mismo modo, podemos definir a la seguridad del hardware como las técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados [43].

Básicamente, la seguridad del hardware comprende un análisis detallado hacia el entorno donde desarrollará sus actividades correspondientes. Debemos tomar en cuenta que los riesgos a los que está expuesto son la pérdida de información, mal funcionamiento de alguno de sus componentes físicos y el acceso que personas sin la debida autorización pudieran hacer a los equipos.

4.5.1 Seguros

En todas las instalaciones existe equipo tanto comprado como rentado; el rentado se debe considerar en forma separada ya que el contrato por lo general establece previsiones específicas. En muchos casos, el vendedor posee su propio contrato de seguros y no se requiere duplicación. Sin embargo, en general esta cobertura no incluye daños causados por la negligencia del personal donde se instala el equipo, y se requiere especificación al respecto. De esta manera, es necesario examinar los contratos y, si se requiere, pedir aclaración acerca de la cobertura y los riesgos a los cuales se considera expuesto el equipo [9].

Los seguros deberán cubrir los siguientes tipos de daños:

- *Daño por causas externas:* El primer riesgo externo es el fuego, pero podría ser necesario considerar ciertos peligros especiales como los relámpagos. En ocasiones, los peligros especiales se pueden añadir a la póliza como incendios de la institución, terremotos, inundaciones, rompimiento de cañerías daño por impacto, disturbios, tumultos civiles, etc. El punto principal consiste en asegurar que se tomen en cuenta todos estos casos.
- *Daño por causas internas.* Muchos de estos aspectos no son asegurables. Algunos ejemplos son las acciones deliberadas o de negligencia por parte de los operadores que puedan causar daños al equipo y los daños a consecuencia del paro prolongado del funcionamiento de la planta del aire acondicionado [ídem].

Los medios de almacenamiento como los discos y las cintas magnéticas casi siempre se aseguran por su costo de compra, pero los datos no están

adecuadamente cubiertos. Por lo tanto, los registros de los sistemas deben asegurar:

- Contra la pérdida o el daño causado al medio.
- Según el costo de reposición de la información registrada en ellos [ídem].

Todo el equipo que la organización adquiera debe ser asegurado contra los tipos de daños anteriormente mencionados. El no aseguramiento de ellos podría traer graves consecuencias a la empresa que van desde pérdidas económicas hasta la modificación o pérdida de información. Para los daños internos como la negligencia, se deberán tomar medidas adicionales como la implantación de métodos de procedimiento para el manejo de los equipos y planes de contingencia en casos de desastres.

4.6 Control de acceso a las comunicaciones

Sin importar el medio utilizado, las líneas de comunicaciones siempre son vulnerables y están expuestas a un sinfín de peligros como la intercepción y los accesos ilícitos [49].

4.6.1 Administración de usuarios y asignación de privilegios

El control de acceso al hardware se realizará preferiblemente mediante personal que verifique mediante algún tipo de identificación a las personas que tienen permiso para acceder al hardware o mediante dispositivos electrónicos (claves, sistemas biométricos) o físicos (puertas blindadas, cerraduras seguras, etc.) que permitan controlar quien tiene acceso al hardware y quien no. Es muy útil en estos casos tener una política clara y concisa sobre quien, como, cuando y para que puede tener acceso al hardware. Estas normativas deberán ser conocidas por todo el personal con acceso al hardware [25].

Para los administradores deberemos crear unas normas de acceso y uso de los dispositivos servidores y de red donde se expliquen claramente los pasos que se deberán seguir para acceder al hardware y realizar modificaciones

sobre éste. Para este personal es esencial el conocimiento de las implicaciones en la seguridad física de los sistemas que su trabajo diario pueda tener y las medidas de precaución que deberán tomar para implementar esta seguridad. Para los usuarios finales de los sistemas se debe crear una normativa de uso de la red y del hardware, donde se indicará de forma clara y fácil de entender como cumplir las normas que se deben seguir para el uso de los dispositivos hardware y de la red corporativa [ídem].

Este apartado debe cubrir tanto a los administradores de los sistemas como los usuarios de éstos últimos. Para cada uno de ellos, se deberán tomar en cuenta una serie de factores. Así, observamos que se deberán establecer medidas de seguridad física y lógicas propios de un administrador de red. Para los usuarios en cambio, se deberán cubrir otras necesidades que principalmente van orientadas hacia el uso que harán dentro de la red y de los sistemas en general.

4.6.2 Políticas de contraseñas

Las **contraseñas**[13] son las herramientas más comunes para restringir el acceso a los sistemas de computación (Figura 4.13). En su mayoría, los usuarios suelen elegir contraseñas fáciles de adivinar. Debemos tomar en cuenta a los hackers quienes podrían en determinado momento adivinar este tipo de contraseñas. Sin embargo, cada vez hay más sistemas de seguridad que prohíben a los usuarios usar cualquier palabra o nombre real como contraseña, para que los hackers no puedan utilizar software de diccionario y adivinarlas sistemáticamente [5].

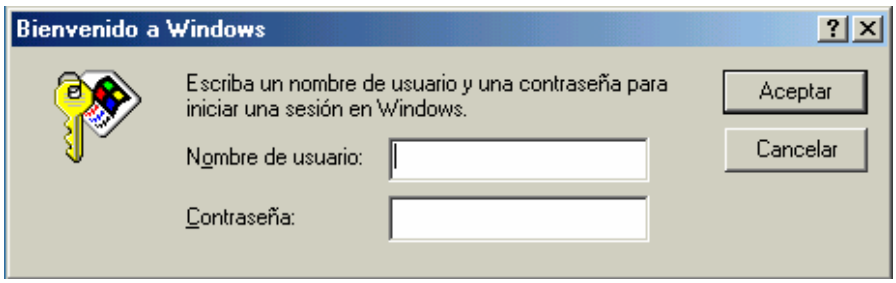

Figura 4.13 Ventana de contraseña

[13] Cadenas de caracteres que pueden estar formadas por letras, números o símbolos.

Las políticas de contraseñas comprenden el estudio de la generación de claves. Actualmente, no es recomendable utilizar contraseñas que pudieran ser fáciles de descifrar y es por esto que se han desarrollado programas que no permiten al usuario poseer contraseñas obvias. Una opción para la generación de contraseñas no tan obvias es la combinación de letras, números y signos matemáticos. Aún con todo esto, es necesario cambiar las contraseñas periódicamente.

4.7 Herramientas para la red

4.7.1 Firewalls

Existen varios módulos que componen el sistema Firewall:

- *Módulo de inspección*. Éste reside en el **kernel** o núcleo del sistema operativo antes de la capa de red, puede interceptar e inspeccionar todos los paquetes antes de que estos residan en el sistema operativo. Este módulo guarda y actualiza el estado y contexto de la información de los paquetes y guarda la información en tablas dinámicas de conexiones. Por medio de este módulo se tiene acceso a las políticas de seguridad.
- *Módulo del Firewall*. Éste módulo brinda el control de acceso para tener autentificación por cliente, usuario y por sesión y además de proveer el "network ardes translation", el cual reemplaza las direcciones de origen y destino del paquete en la red.
- *Módulo de manejo*. Provee la interfaz gráfica para el usuario en donde el administrador del Firewall representará de manera sencilla las políticas de seguridad de la empresa. Desde aquí se controlan los diferentes Firewalls con sus salidas respectivas. Aquí se encuentran las bitácoras y es estado de funcionamiento.
- *Módulo de encriptación*. Éste módulo es uno de los medios de protección que se tienen para la información, en Internet la información esta muy libre, para evitar este tipo de inseguridad en la información se utiliza la encriptación [27].

La función básica de un firewall[14] es evitar que entren intrusos y salga información secreta. El esquema que expone esta idea se muestra en la siguiente figura:

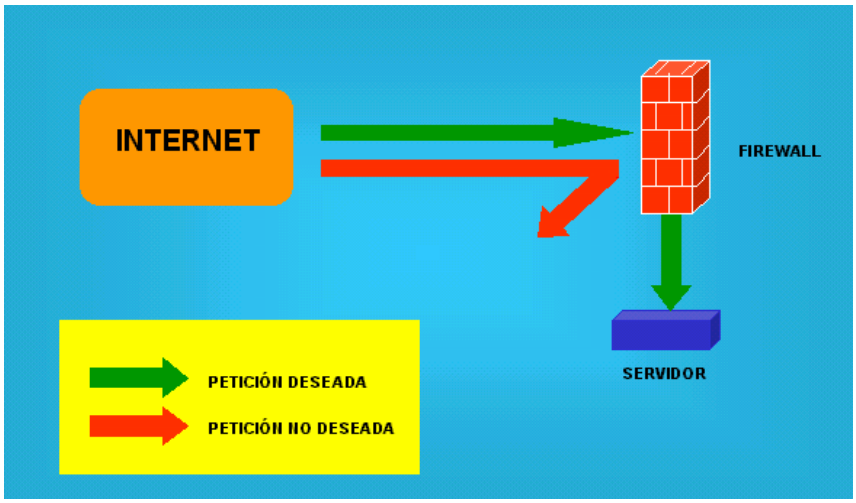

Figura 4.14 Esquema de implementación de un firewall

Los firewalls tienen por meta principal vigilar el tráfico de la red donde son implementados. Para elegir el firewall adecuado a las necesidades de la organización deben tomarse en cuenta aspectos como el tipo de servicios disponibles en la red, tales como el correo electrónico y el número de equipos que estarán conectados a Internet. A partir de aquí se elegirá el que cumpla con las expectativas de quien o quienes lo soliciten. Existen dos tipos de firewalls: proxies y filtrado de paquetes (ver Anexo 1).

4.7.2 Seguridad del correo electrónico

El correo electrónico es un sistema que permite intercambiar mensajes entre usuarios de computadoras enlazados electrónicamente a Internet. Al igual que el correo postal, el correo electrónico permite enviar mensajes privados de persona a persona, sin que sean leídos por personas no autorizadas. Además, como en el correo de oficina, es posible pedir que se envíe un mensaje con copia a terceros. Otra ventaja del correo electrónico es que, al

[14] También conocidos como cortafuegos.

enviar un mensaje, es posible anexar copias de uno o más documentos (archivos adjuntos) [8].

Sin lugar a dudas, el correo electrónico es el recurso más utilizado de Internet ya que dentro de las organizaciones es muy importante agilizar el proceso de comunicación. El sistema de correo electrónico es un servicio general que puede transportar cualquier tipo de información: documentos, publicaciones, programas de computadora y mucho más. El único requisito es que los datos deben almacenarse como caracteres ASCII; esto es, los caracteres habituales del teclado [4].

El correo electrónico es uno de los sistemas telemáticos más vulnerables a los ataques informáticos. Actualmente el correo electrónico es tan imprescindible a nivel profesional como el fax o el teléfono o a nivel doméstico es la herramienta que se ha desarrollado más rápidamente de Internet. Pero, durante muchos años, la asignatura pendiente ha sido la seguridad, con sus cuatro formas: confidencialidad, integridad, autenticación y firma.

En el correo ordinario la seguridad se soluciona de la siguiente manera:

- *Confidencialidad:* El sobre mantiene oculta la información del interior. Si la confidencialidad es violada, el receptor puede detectar la manipulación del sobre.
- *Integridad:* La integridad se mantiene por la protección del sobre y las propiedades de indelebilidad del papel y la tinta.
- *Autenticación:* En las cartas escritas a mano se puede detectar la autenticación del autor mediante técnicas grafológicas.
- *Firma:* La firma a final de las cartas o documentos identifica de manera unívoca al autor mediante un análisis grafológico y asegura que no se ha añadido más texto.

El correo electrónico ha buscado cumplir las mismas propiedades y la forma de hacerlo es mediante la **criptología.** Los primeros sistemas de seguridad funcionaban directamente sobre **SMTP**[15]**.**

- *PGP.* Fue inventado por un particular, Phil Zimmerman, y no tiene restricciones legales para la distribución.
- *PEM.* Fue desarrollado por la agencia de seguridad de Estados Unidos (NSA) y, por tanto, tiene muchas restricciones legales. Esto no ha permitido su desarrollo.

Después apareció el estándar **MIME**[16] como una extensión al SMTP para contenidos multimedia y corregir defectos del anterior sistema. Entre otras cosas permite:

- Formatear los mensajes de texto (tipos de letras, colores, etc.)
- Diversificar el sistema de adjuntar documentos, aplicaciones, etc.
- Jerarquías de mensajes.
- Fragmentación de mensajes automática.
- Mensajes de múltiples cuerpos multimedia.
- Diferentes alternativas de presentar mensajes (ASCII, audio, formateado, etc.) [28]

El correo electrónico es una de las herramientas de Internet más importantes. La seguridad que debe poseer este servicio se orienta hacia cuatro características: confidencialidad, autenticación, integridad y firma. Los diseñadores de programas deben buscar que cumplan cada uno de estos requisitos desarrollando aplicaciones destinadas a tales fines. Así, haciendo uso de la criptología se pueden crear programas que garanticen que la información intercambiada mediante el correo electrónico no sufrirá modificaciones ni pérdidas durante su recorrido del emisor al receptor.

[15] Simple Mail Transfer Protocol.
[16] Multipurpose Internet Mail Extensions.

4.7.2.1 PGP

Es un programa desarrollado por Phil Zimmerman y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales. Existe la posibilidad de que haya errores en la implementación, y si se utiliza descuidadamente es posible desproteger fácilmente un archivo de texto protegido. A diferencia de protocolos de seguridad como **SSL**[17], que sólo protege los datos mientras se transmiten a través de la red, PGP también puede utilizarse para proteger datos almacenados en discos, copias de seguridad, etcétera [32].

4.7.3 VPN

Una **VPN**[18] conecta los componentes de una red sobre otra red. VPN logra este objetivo mediante la conexión de los usuarios de distintas redes a través de un túnel que se construye sobre Internet o sobre cualquier red pública (Figura 4.15) [46].

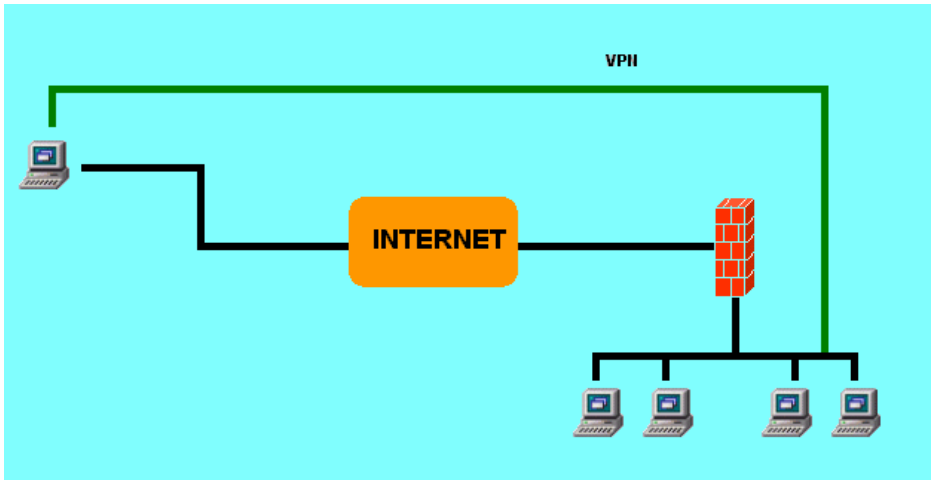

Figura 4.15 Diagrama de una VPN

Las redes VPN ofrecen una serie de ventajas a las empresas donde son implementadas. Permiten conectar oficinas centrales de una organización

[17] Protocolo que permite el viaje de datos encriptados a través de la red.
[18] Virtual Area Network.

con sus correspondientes sucursales sobre la red Internet. De este modo, el usuario conectado puede enviar y recibir información a través de la red como si la estación de trabajo con la cual interactúa se encontrara dentro del mismo espacio del usuario.

4.7.4 Restricciones en el uso de Internet

Teniendo en cuenta que la utilización de Internet no siempre se orienta hacia todos los usuarios de la red, y que el uso de Internet no siempre se orienta al trabajo de tipo académico, de investigación y de trabajo, se deberán implementar mecanismos de seguridad para poder restringir el acceso a determinadas páginas de Internet, a determinadas personas, a determinadas estaciones de trabajo o autorizar el acceso a unos pocos [34].

Si no cuenta con un filtro para Internet puede usar las restricciones del navegador Explorer en donde puede elegir diferentes niveles de lenguaje, desnudos, sexo y violencia permitidos. Los padres o los supervisores pueden establecer contraseñas para permitir el acceso a cualquier página Web o impedir el acceso de los usuarios a las páginas Web que no tienen restricciones. Podrá acceder a esta configuración, desde el menú Herramientas, Opciones de Internet. En la ficha contenido aparece un índice que define opciones sobre las páginas que pueden o no ser vistas [20].

El uso del Internet no siempre se hará de una manera profesional. Si se considera el hecho de que los usuarios podrán acceder libremente a cualquier página disponible de la red, se debe tener en cuenta que existen serias amenazas como virus y spyware. Para evitar posibles ataques resulta necesario vigilar el correcto uso de Internet. Uno de los métodos más sencillos es el que nos ofrece el navegador Internet Explorer. A partir de aquí, se deben considerar mecanismos más especializados como los filtros para Internet.

4.7.4.1 Filtros para Internet

Los filtros para Internet surgen de la mala utilización de este servicio en las empresas y en el sector académico. Algunos estudios señalaron que las páginas más visitadas fueron las de tipo pornográfico, seguidas de las

páginas de juegos, música, viajes y horóscopos. Las consecuencias son las siguientes: problemas de saturación de la red de las empresas y, sobre todo, descenso de la productividad. Algunas empresas ya han encontrado la solución: implementar un filtro de acceso a Internet en sus equipos y limitar así la entrada a las páginas no deseadas desde las computadoras de sus empleados [47].

Los filtros para Internet son programas que mantienen un registro permanente de las páginas visitadas por los usuarios que utilizan las computadoras en donde son implementados. Existen varios tipos de filtros (ver Anexo 1). Actualmente, resultan una herramienta de gran importancia, ya que nos permiten tener un control sobre el uso que los usuarios harán de la red organizacional. El poseer mecanismos como éste harán que la productividad aumente dentro de la empresa así como evitar riesgos de ataques informáticos.

4.8 Recuperación en caso de desastres

Los desastres de pérdidas de datos son cosas que ocurren. Aceptarlo es el primer paso en la preparación de un plan completo para casos de desastre. Cuando ocurre un desastre, el equipo de TIC's siempre va a contrarreloj, por lo que contar con un plan para estos casos es esencial para lograr el éxito.

He aquí algunas de las acciones recomendadas a realizar:

- Cuando proceda a recuperar un desastre, no restaure los datos en el mismo servidor que los perdió. Restáurelos en otro servidor o destino.
- En fallos de Microsoft Exchange o SQL, no intente reparar el almacén de información ni los archivos de bases de datos originales; trabaje con copias.
- En casos de datos borrados, apague inmediatamente la computadora. No cierre Windows; así evitará que los datos se sobrescriban.
- Use regularmente un desfragmentador de volúmenes.
- Si en un sistema **RAID** falla una unidad de disco, no la sustituya por otra que haya formado parte de un sistema RAID anterior; antes de usar una unidad de recambio, póngala a cero.

- Si una unidad hace ruidos mecánicos extraños, apáguela inmediatamente y busque ayuda.
- Hágase con una copia de seguridad válida antes de hacer cambios de hardware o software.
- No ejecute herramientas de reparación de volúmenes en unidades que crea que puedan estar estropeadas.
- No ejecute herramientas desfragmentación en unidades que crea que puedan estar estropeadas.
- En una situación de pérdida de corriente con un sistema RAID, si el sistema de archivos no es de confianza, o no es montable, o no se puede acceder a los datos una vez recuperada la corriente, no ejecute utilidades de reparación de volúmenes [35].

Toda organización debe poseer planes de contingencia en caso de que ocurrieran desastres de cualquier tipo. Se debe saber qué hacer ante siniestros como incendios, inundaciones o sismos; así como también contra robos o modificaciones no autorizadas de datos. El realizar las acciones correctas traerán como consecuencias la recuperación de la información que es vital para toda organización ya que actualmente todas ellas dependen en gran manera de sus sistemas de bases de datos.

4.8.1 Sistemas RAID

Básicamente el RAID es un sistema el cual permite almacenar información en una cantidad n de discos, de tal forma que agilice el proceso máquina-disco. El sistema RAID evitará en lo más posible la pérdida de datos de la siguiente manera: Los discos optimizados para RAID poseen circuitos integrados que detectan si el disco está fallando, de ser así este circuito se encargará de sacar la información y almacenarla en los otros discos. (Figura 4.16). Una de las ventajas del sistema RAID es la posibilidad, con los discos **hot swap**, de conectarlos y desconectarlos en "caliente", es decir, que si un disco falla no hará falta el apagar el sistema para remplazarlo; además de que permite la reconstrucción y regeneración cuando un disco falla y la información redundante en los discos y los datos en los discos buenos son usados para regenerar la información de disco averiado [37].

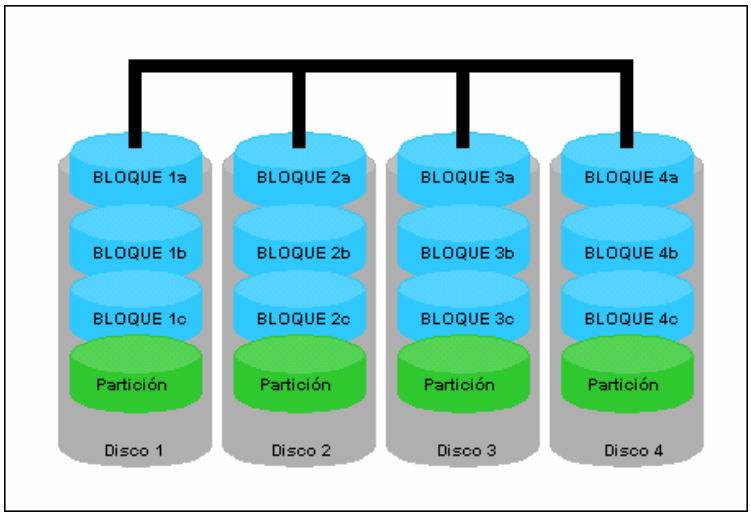

Figura 4.16 Funcionamiento del sistema RAID

Los sistemas **RAID**[19] ofrecen una serie de ventajas bastante importantes en lo que a seguridad de información se refieren. Sabemos que en cualquier momento los componentes físicos de las computadoras pueden fallar. Si esto llegara a ocurrir, los equipos que cuentan con este sistema se encargarán de almacenar la información en un dispositivo alterno que no presente fallas mientras que se trata de reparar el daño que se pudiera tener.

4.8.2 DRP (Disaster Recovery Plan)

Los continuos avances de la misma tecnología y de las necesidades particulares de cada empresa, hace que el modelo de disaster recovery sea un proceso cíclico con continuos ajustes y revisiones. Esta idea se muestra en la figura 4.17 [36].

El plan DRP es una herramienta que en últimas fechas está tomando una fuerza considerable. Se debe tener en cuenta que todo sistema implementado tiene un ciclo de vida, por lo que es necesario contar con un mecanismo que indique las acciones a realizar en cada fase del ciclo de vida del sistema.

[19] Redundant Array of Inexpensive Disks.

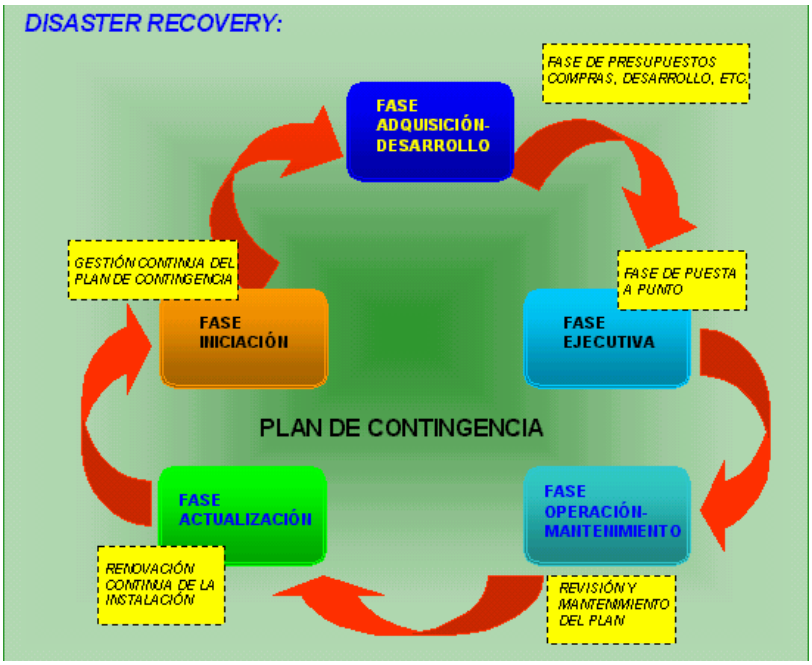

Figura 4.17 El ciclo del Disaster Recovery Plan

Este plan se orienta hacia la puesta en marcha de sistemas de computación. Comprende una serie de acciones a seguir cuando se poseen sistemas de seguridad dentro de los equipos de cómputo. Como puede verse en el diagrama anterior, lo primero consiste en contar con un sistema de seguridad; posteriormente viene su implementación, seguida de una fase de operación y mantenimiento. Una vez hecho estas acciones se procede a actualizar el sistema en caso de ser necesario. Si, por el contrario, se determina que no cumple las expectativas de seguridad de la organización, se procede a gestionar un nuevo sistema para su posterior desarrollo. Como puede observarse, el ciclo inicia nuevamente. Se pone de manifiesto la importancia de contar siempre con sistemas eficaces que garanticen en todo momento la seguridad de la información que se tiene dentro de la organización.

Capítulo 5.

Reglamento de seguridad

5.1 Fundamentos del reglamento

El reglamento que a continuación se gestiona ha sido formado a partir de:

- Reglamento interno de la dirección general de telecomunicaciones de la UAEH.
- Reglamento interno del CECA.

Del mismo modo, la normativa contenida en el reglamento ha sido formulada a partir del análisis realizado a los riesgos informáticos y a los elementos de seguridad vistos en el capítulo tres y cuatro respectivamente. Ambos han sido traducidos en una serie de normas que tendrán por objetivo garantizar la seguridad de todo lo que engloban cada uno de ellos así como evitar cualquier tipo de contingencia o ataque a la información.

5.2 Reglamento de seguridad

5.2.1 Disposiciones generales

Artículo 1. Este reglamento tiene por objeto establecer las normas de funcionamiento y uso de los equipos de cómputo dentro de la organización, en relación a los estándares que rigen los diferentes dispositivos eléctricos y electrónicos orientándolo hacia la función informática.

Artículo 2. Todos los usuarios tienen la obligación de observar y cumplir el presente reglamento.

Artículo 3. Para los efectos de este reglamento se entenderá por:

I. *Equipo de cómputo.* Es el conjunto de dispositivos físicos y lógicos que en conjunto realizan operaciones determinadas.
II. *Usuario.* Es una persona, organización u otra entidad.
III. *Seguimiento.* La acción de verificar que los lineamientos establecidos se lleven a cabo.
IV. *Respaldo.* Consiste en realizar una copia de seguridad de información en un dispositivo de almacenamiento secundario.

V. *Comunicaciones.* Son las diferentes tecnologías empleadas por las computadoras teniendo como objetivo el intercambio de información con otras computadoras.
VI. *Control de acceso.* Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.
VII. *Autenticación.* Procedimiento de comprobación de la identidad de un usuario.
VIII. *Identificación.* Procedimiento de reconocimiento de la identidad de un usuario.
IX. *Sistema de información.* Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
X. *Incidencia.* Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
XI. *Instalaciones físicas.* Lugar físico en donde se encuentran las diferentes áreas departamentales de la organización.

5.2.2 De las instalaciones físicas

Artículo 4. Las instalaciones deberán contar con una puerta de acceso físico y una salida de emergencia ambas blindadas y con sus respectivas cerraduras, así como una ventilación e iluminación adecuada.

Artículo 5. La instalación eléctrica deberá contar sin excepción con tierra física.

Artículo 6. El cableado eléctrico de la instalación será de calibre 12 y para el site donde se encuentren equipos especiales como UPS será de calibre 8.

Artículo 7. Se deberá contar con extintores de CO2, reguladores de clima artificial y detectores de humo fotoeléctricos, con la finalidad de hacer el área de trabajo más agradable y segura en caso de alguna contingencia.

Artículo 8. El cableado de red para las estaciones de trabajo será de tipo UTP categoría cinco.

Artículo 9. Las llaves de la puerta de acceso físico al área de cómputo y al site estarán en poder del área de cómputo.

Artículo 10. El área de cómputo deberá contar con manuales de organización y procedimientos para cada una de las actividades que ahí se realicen.

Artículo 11. Las instalaciones contarán con los siguientes señalamientos:

I. Prohibido fumar.
II. Extintor.
III. Salida de emergencia.
IV. Prohibido introducir alimentos.
V. Uso del gafete obligatorio.
VI. Solo personal autorizado.

Artículo 12. El área de cómputo deberá contar con una planta de energía eléctrica en caso de una falla de corriente prolongada.

Artículo 13. El cableado deberá ser transportado a través de canaletas colocadas en los techos y pared del edificio.

5.2.3 Del hardware

Artículo 14. El equipo de cómputo deberá contar con su número de inventario correspondiente.

Artículo 15. Si el equipo de cómputo presenta daños de fabricación, deberá ser reportado inmediatamente al responsable del área de cómputo con el fin de comunicarlo al proveedor del equipo.

Artículo 16. El equipo de cómputo deberá contar con sus seguros respectivos.

Artículo 17. El equipo de cómputo deberá contar con su mobiliario especial y éste deberá tener su número de inventario.

Artículo 18. Toda pérdida o daño al equipo causada por el usuario deberá ser repuesta o reparada por él mismo en un lapso no mayor a cinco días contados a partir del día del incidente.

Artículo 19. Todo equipo de cómputo deberá contar con su regulador de voltaje.

Artículo 20. Los equipos concentrados dentro del site deberán contar con sistemas UPS.

5.2.4 Del software

Artículo 21. Todo el software deberá contar con sus respectivas licencias.

Artículo 22. Todo equipo de cómputo deberá contar con su software antivirus correspondiente.

Artículo 23. Todo equipo de cómputo deberá contar con programas anti spyware.

Artículo 24. Todo equipo de cómputo deberá contar con sus respectivas ventanas de contraseñas de acceso.

5.2.5 De los sistemas

Articulo 25. El mantenimiento a los sistemas instalados dentro de la red será en un lapso de tres meses por el personal del área de cómputo y deberá ser documentado.

Artículo 26. Sólo usuarios autorizados tendrán acceso especial al código fuente de los sistemas implementados.

Artículo 27. El sistema deberá contar con su respectiva clave de acceso para su posterior utilización.

5.2.6 De las comunicaciones

Artículo 28. Todas las estaciones de trabajo deberán contar con firewalls con el objeto de aumentar la seguridad de la información.

Artículo 29. No se permitirá el uso de la red de la organización como medio de distribución de información dañina como virus, caballos de Troya, gusanos o cualquier otro tipo de código malicioso.

Artículo 30. No se permitirá el uso de programas ajenos a la red de la organización que puedan afectar el rendimiento y el comportamiento de la misma, como programas relacionados con spyware, sniffers y spammers; así como aplicaciones "peer to peer" como kazaa.

Artículo 31. No se permitirá el acceso a páginas con material pornográfico, de juegos o de música.

Artículo 32. La información que se intercambie por correo electrónico deberá responder a un comportamiento completamente profesional.

5.2.7 De los usuarios

Artículo 33. El área de cómputo permanecerá abierta en el horario definido por el área administrativa.

Artículo 34. Durante el tiempo de operación del área de cómputo solamente tendrán acceso para su uso:

VII. El personal de la organización.
VIII. Los usuarios a quienes se refiere el artículo 3 fracción II de este reglamento.

Artículo 35. Quedará estrictamente prohibido el acceso a personas en estado de ebriedad o bajo el efecto de estupefacientes.

Artículo 36. El usuario deberá portar en todo momento su gafete de identificación, el cual le será proporcionado por la organización.

Artículo 37. El usuario deberá contar con su respectiva clave de identificación para tener acceso al site.

5.2.8 De los respaldos

Artículo 38. Toda información técnica perteneciente a los equipos de cómputo y al área informática es parte integral de los mismos y disponible para su consulta en el momento en que se le solicite.

Artículo 39. Los backups de información deberán ser alojados en un lugar seguro fuera de la organización siendo actualizados periódicamente.

5.2.9 De las sanciones

Artículo 40. Será acreedor a las sanciones por:

I. Por el grado de incidencia.
II. Por la gravedad de la falta cometida.
III. Por el tipo de acción cometida dentro de la red de la organización.

Artículo 41. Cualquier usuario que realice actividades indebidas en la red como consultar páginas pornográficas, de juegos, o música será acreedor a las siguientes sanciones:

I. Suspensión temporal del acceso al área de cómputo.
II. Desconexión del nodo de la red por un tiempo indefinido.
III. Separado del cargo según la gravedad de la falta y el grado de incidencia.

Artículo 42. El usuario que trafique dentro de la red con programas maliciosos como spyware será separado del cargo.

Artículo 43. El usuario que sea sorprendido haciendo uso de software pirata será suspendido temporalmente del cargo.

5.2.10 De los planes de contingencia

Artículo 44. Los equipos especiales concentrados en el site deberán contar con sistemas RAID que entren en operación cuando ocurra algún fallo en dichos equipos.

Artículo 45. Toda la organización deberá estar bajo la implementación del plan DRP para así tener el todo momento los sistemas íntegros y funcionales.

5.3 Alcances del reglamento

El reglamento ha sido orientado hacia la regulación de la función informática utilizando y aprovechando las TIC's. El reglamento anteriormente descrito cubre a cada uno de los departamentos y áreas de trabajo de la organización puesto que actualmente el procesado y manipulación de datos se ha extendido por toda ella. En consecuencia, el reglamento gestionado será de uso general en toda la organización.

Conclusiones

La creciente mejora de las operaciones de intercambio de información y procesamiento de datos a través de Internet, ha aumentado significativamente la amenaza en contra de la seguridad de la información. Los sistemas informáticos son cada vez más complejos, pero a su vez, presentan mayores vulnerabilidades debido simplemente a su mayor dimensión.

Como hemos podido ver, las TIC's han redefinido los procesos de generación, manipulación e intercambio de datos dentro de las organizaciones que hoy día resultan de mucha importancia para todas ellas. Del mismo modo, aplicando técnicas de seguridad informática tomando en cuenta el análisis a la seguridad actual realizado por las TIC's generan un punto de trascendencia considerable para el buen desempeño de todas las funciones e interacciones que se deban hacer dentro de la organización y con el exterior.

Con lo anterior, en primera instancia se ha conocido la manera en como las TIC's han transformado la manera de trabajar con los datos dentro de la organización, generalizando lo que anteriormente era tarea solo de unos cuantos, pocos y muy especializados.

El presente trabajo de investigación ha realizado análisis a los riesgos y a los elementos de seguridad informática. Se han conocido cada una de las amenazas a las que puede estar expuesta la información, usuarios y sistemas. De este mismo modo, el haber conocido los elementos de seguridad que evitan la puesta en marcha de cualquier tipo de amenaza lleva a la gestión de mecanismos de control que tengan por meta regular el como

saber hacer con el diario hacer de las organizaciones, es decir, el mecanismo de control gestionado ha de ponerse en práctica en la realidad, dentro de las organizaciones que así lo requieran.

Así, un resultado de esta sinergia ha sido la generación de un reglamento el cual contiene los elementos de seguridad por medio de una serie de normas a cumplir mencionando lo que se debe hacer, como se debe trabajar y bajo que circunstancias, describiendo además que operaciones resultarían ilícitas de realizar y gestionando acciones necesarias para mantener en la medida de todo lo posible la seguridad del software, hardware, comunicaciones, usuarios, sistemas y datos de la organización.

Glosario de términos

A

Archivo. Agrupación de información que puede ser manipulada de forma unitaria por el sistema operativo de un ordenador. Un fichero puede tener cualquier tipo de contenido (texto, ejecutables, gráficos, etc.) y posee una identificación única formada por un "nombre" y un "apellido", en el que el nombre suele ser de libre elección del usuario y el apellido suele identificar el contenido o el tipo de fichero.

ARPANET. Red pionera de larga distancia financiada por ARPA (antigua DARPA). Fue la base inicial de la investigación sobre redes y constituyó el eje central de éstas durante el desarrollo de Internet. ARPANET estaba constituida por ordenadores de conmutación individual de paquetes, interconectados mediante líneas telefónicas de la que posteriormente derivó Internet.

Automatización. Ejecución automática de tareas industriales, administrativas o científicas haciendo más ágil y efectivo el trabajo y ayudando al ser humano.

B

Backup. Copia de ficheros o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

C

Copia de seguridad. Es una copia de los programas o de los datos, que se hace como prevención ante posibles pérdidas que podrían llegar a ser irreparables.

Cracker. Un cracker es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y pueden disponer de muchos medios para introducirse en un sistema. Individuo con amplios conocimientos informáticos que produce daños en sistemas o redes.

Criptografía. Del griego *kryptos* (ocultar) y *grafos* (escribir), literalmente escritura oculta, la criptografía es el "arte de escribir con clave secreta o de un modo enigmático". En otras palabras es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Criptología. Es la parte de la criptografía que tiene por objeto el descifrado de criptogramas cuando se ignora la clave.

D

Desfragmentador. Herramienta incluida en la mayoría de los sistemas operativos, aunque se puede adquirir de forma individual. Su función es desfragmentar la unidad de almacenamiento. Básicamente intenta agrupar toda la información almacenada, que se encuentra fragmentada por toda la unidad.

E

Encriptar. Es una manera de codificar la información de un archivo o de un correo electrónico de manera que no pueda ser leído en caso de ser interceptado por una tercera persona mientras viaja por la red. Sólo la persona o personas que tienen el tipo de software de descodificación adecuado pueden descifrar el mensaje.

Ethernet. Sistema de red de área local de alta velocidad. Se ha convertido en un estándar de red corporativa.

F

Firewall. Dispositivo que se coloca entre una red local e Internet y cuyo objetivo es asegurar que todas las comunicaciones entre los usuarios de dicha red e Internet se realicen conforme a las normas de seguridad de la organización que lo instala.

Firma digital. Código digital que se puede adjuntar a un mensaje transmitido por medios electrónicos y que identifica de manera exclusiva al remitente. Al igual que las firmas comunes en papel, el objetivo de las firmas digitales es garantizar que la persona que envía el mensaje es realmente quien dice ser. Las firmas digitales son particularmente importantes en el comercio electrónico y constituyen un elemento clave de la mayoría de los procesos de autenticación.

FTP. (File Transfer Protocol). Protocolo que permite a un usuario de un sistema acceder a, y transferir desde, otro sistema de una red. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo.

H

Hacker. Experto en informática capaz de entrar en sistemas cuyo acceso es restringido no necesariamente con malas intenciones. Una persona que goza alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de un ordenador o de una red de ordenadores. Este término se suele utilizar indebidamente como peyorativo, cuando en este último sentido sería más correcto utilizar el término cracker. Los hackers proclaman tener una ética y unos principios contestatarios e inconformistas pero no delictivos.

Hardware. Componentes físicos de una computadora o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.

Hoja de cálculo. Programa que permite manipular números dispuestos en forma de tablas. Habitualmente es posible realizar cálculos complejos con fórmulas y funciones así como dibujar distintos tipos de gráficas.

Hot Swap. Procedimiento para cambiar los componentes de una computadora sin necesidad de apagar el mismo.

I

Información. Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. La información ha sido siempre un recurso muy valioso, revalorizado hoy más aún por el desarrollo y la expansión de las tecnologías de la información y comunicaciones.

Internet. Internet es una red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).

Intranet. Una intranet es una red local que utiliza herramientas de Internet. Se puede considerar como una Internet privada que funciona dentro de una organización. Normalmente, dicha red local tiene como base el protocolo TCP/IP de Internet y utiliza un sistema firewall (cortafuegos) que no permite acceder a la misma desde el exterior.

K

Kernel. En informática, el kernel (también conocido como núcleo) es la parte fundamental de un sistema operativo. Es el software es el responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora. Como hay muchos programas y el acceso al hardware es limitado, el núcleo también se encarga de decidir qué programa podrá hacer uso de un dispositivo de hardware y durante cuánto tiempo, lo que se conoce como multiplexado. Acceder al hardware directamente puede ser realmente complejo, por lo que los núcleos suelen implementar una serie de

abstracciones del hardware. Esto permite esconder la complejidad, y proporciona una interfaz limpia y uniforme al hardware subyacente, lo que facilita su uso para el programador.

L

LAN. Local Area Network (Red de Área Local). Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden optimizarse los protocolos de señal de la red para llegar a velocidades de transmisión de Gbps (gigabits por segundo).

M

Mainframe. Nombre que se da a las grandes computadoras, capaces de atender a miles de usuarios y miles de programas "al mismo tiempo" asignándole un periodo muy pequeño a la atención de cada programa. Su capacidad de trabajo es muy alta, por lo que normalmente se encuentran en empresas de gran tamaño. Sus programas están compuestos por cientos de miles o millones de líneas de código.

Malware. La palabra malware proviene de una agrupación de las palabras malicious software. Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

Microcomputadora. Una computadora pequeña (computadora de escritorio, o también llamada computadora personal).

Microprocesador. Circuito integrado en un soporte de silicio, formado por transistores y otros elementos electrónicos miniaturizados. Son uno de los elementos esenciales de una computadora y de cada vez más aparatos electrónicos de todo tipo.

MIME. (Multipurpose Internet Mail Extensions). Extensiones Multipropósito que permiten que cuando enviemos un e-mail con un fichero binario vinculado, éste fichero llegue en su formato original. Conjunto de especificaciones Internet de libre distribución que permiten tanto el intercambio de texto escrito en lenguajes con diferentes juegos de caracteres como el intercambio de ficheros de diversos formatos entre ordenadores y aplicaciones que sigan los estándares de correo Internet.

Modelo OSI. El modelo OSI (Open Systems Interconection) es la propuesta que hizo la ISO (International Standards Organization) para estandarizar la interconexión de sistemas abiertos. Un sistema abierto se refiere a que es independiente de una arquitectura específica. Se compone el modelo, por tanto, de un conjunto de estándares ISO relativos a las comunicaciones de datos.

N

Nodo. Unidad de conexión de una computadora o conjunto de computadoras que reciben la llamada del usuario y la dirigen hacia el servicio solicitado donde se encuentre.

O

Ordenador. Máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas. Es el sinónimo más común de computadora.

P

Password. Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

Periférico. Un periférico es un dispositivo hardware de una computadora que potencia la capacidad de ésta y permite la entrada y/o salida de datos. El término suele aplicarse a los dispositivos que no forman parte indispensable

de una computadora y que son, en cierta forma, opcionales. Aunque también se suele utilizar habitualmente para definir a los elementos que se conectan externamente a un puerto de la computadora.

Procesador de texto. Aplicación informática que permite escribir textos de todo tipo, desde cartas hasta libros. Hoy en día es frecuente que permitan usar distintos tipos de letra, incluir imágenes y tablas de datos, escribir en columnas, añadir ecuaciones matemáticas, etc.

Procesamiento de datos. Conjunto de diferentes operaciones en secuencia sistemática sobre los datos, las cuales se basan en la elaboración, manipuleo y tratamiento de los mismos, mediante máquinas automáticas para producir los resultados esperados.

Programas agentes. Son programas inteligentes que se diferencian de los programas ordinarios porque van a tener entidad independiente, autónomos, ser robustos y adaptables, capaces de aprender de la experiencia, capaces de responder a situaciones imprevistas, capaces de percibir el estado actual del ambiente y capaces de desenvolverse para progresar hacia su objetivo. Los investigadores de inteligencia artificial han venido persiguiendo métodos más complejos de construcción de agentes, a estos se les dota de información relativa a las tareas que se deben llevar a cabo, el programa interfiere cual ha de ser la respuesta idónea para la situación dada.

Protocolo. Conjunto de normas técnicas que regulan las comunicaciones entre computadoras. Lista de comandos estandarizada a la que responde un servidor.

R

Reingeniería. Conjunto de actividades tendientes a reformular de manera integral, los procesos organizacionales, administrativos, financieros y contables de una empresa, lo que implica una reconversión, transformación y adaptación a los cambios tecnológicos, y a nuevos modelos estructurales empresariales, con la finalidad de incrementar su productividad, eficiencia y eficacia, procurando su mejora continua y modernización.

Respaldo. Consiste en guardar en un medio extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema. Esta se puede realizar tanto en ordenadores personales como en servidores. Este medio puede ser un disco duro externo, un CD-ROM grabable, cintas de datos (DAT), discos ZIP o JAZ o magneto-ópticos.

S

Servidor. Sistema que proporciona recursos (por ejemplo, servidores de ficheros, servidores de nombres). En Internet este término se utiliza muy a menudo para designar a aquellos sistemas que proporcionan información a los usuarios de la red.

SI. Siglas con las que se conoce al término sistema de información, el cual se define como el conjunto de elementos, ordenadamente relacionados entre sí que aporta al sistema objeto, es decir, a la organización a la cual sirve y le marca directrices de funcionamiento, la información necesaria para el cumplimiento de sus fines, para lo cual tendrá que recoger, procesar y almacenar la información, facilitando la recuperación de la misma.

Sinergia. Es la integración de elementos que da como resultado algo más grande que la simple suma de éstos, es decir, cuando dos o más elementos se unen creando un resultado que aprovecha y maximiza las cualidades de cada uno de los elementos.

Sistema RAID. Es una forma de almacenar los mismos datos en distintos lugares (por tanto de modo redundante) en múltiples discos duros. Al colocar los datos en discos múltiples, las operaciones de entrada y salida pueden superponerse de un modo equilibrado, mejorando el rendimiento del sistema.

SMTP. (Simple Mail Transfer Protocol). Protocolo para transferir correo electrónico a través de Internet. Definido en STD 10, RFC 821, que se usa para transferir correo electrónico entre ordenadores. Es un protocolo de servidor a servidor, de tal manera que para acceder a los mensajes es preciso utilizar otros protocolos.

SNMP. (Simple Network Management Protocol). Protocolo que se encarga del direccionamiento de red, se utiliza para grandes redes.

Software. Programas o elementos lógicos que hacen funcionar una computadora o una red, o que se ejecutan en ellos, en contraposición con los componentes físicos de la computadora o la red. Series de instrucciones codificadas que sirven para que la computadora realice una tarea. Son los programas de la computadora.

Spyware. Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos.

SSL. Protocolo creado por Netscape con el fin de posibilitar la transmisión cifrada y segura de información a través de la red. Permite que la información (normalmente datos económicos) viaje encriptada evitándose que pueda ser leída. Garantiza una seguridad alta en el comercio electrónico.

T

TCP/IP. (Transmission Control Protocol/Internet Protocol): Sistema de protocolos en los que se basa en buena parte Internet. El primero se encarga de dividir la información en paquetes en origen, para luego recomponerla en el destino. El segundo la dirige adecuadamente a través de la red.

Tecnología. Conjunto de los conocimientos propios de un oficio mecánico o arte industrial o del funcionamiento o proceso de máquinas.

U

Unix. Sistema operativo especializado en capacidades de multiusuario y multitarea el cual fue la base inicial del Internet desarrollado en principio por

un grupo de empleados de los laboratorios Bell de AT&T. Entre sus características más importantes se encuentran: redireccionamiento de entrada/salida, interfaz simple e interactiva con el usuario y alta portabilidad lo que lo hace independiente del hardware.

UPS. Sistema de alimentación ininterrumpida (Uninterruptible Power Supply, en español abreviado como SAI).

Usuario. En informática, navegante que accede a un servicio, contenido o página determinada.

V

VPN. Virtual Private Network, (Red Privada Virtual). Se refiere a una red en la cual algunas partes se conectan usando Internet público, pero los datos enviados por Internet se cifran de manera que toda la red es "virtualmente" privada. Un ejemplo típico es la red de una compañía donde hay dos oficinas en ciudades diferentes. Usando Internet, las dos oficinas fusionan sus redes en una sola, pero se une el tráfico que usa Internet.

Vulnerabilidad. En informática, es la condición expuesta a una amenaza en la que se encuentran los dispositivos físicos, lógicos y de comunicaciones de un sistema computacional.

W

WAN. Wide Area Network o Redes de Area Ancha. Un tipo de red que interconecta computadoras con un espectro amplio de cobertura, a nivel de un país o grupo de países. Internet puede considerarse como la más eficaz de la WAN actualmente existente.

Bibliografía:

[1] REBOLLOSO, Gallardo Roberto. La globalización y las nuevas tecnologías de información, Primera Edición, Editorial Trillas, México (2000)

[2] ZOLONDZ, Vogel Alfredo. Nuevas Tecnologías de Información, Editorial EDAMEX, México (2001)

[3] ALCALDE, Eduardo y García Miguel. Informática básica, Segunda Edición, Editorial Mc. Graw Hill, México (2001)

[4] Centro de Computación Profesional de México (CCPM). Aplicación práctica de la computadora, Editorial Mc. Graw Hill, México (2000)

[5] BEEKMAN, George. Computación & Informática hoy, una mirada a la tecnología del mañana, Editorial Addison Wesley Iberoamericana, S. A. México (1998)

[6] NORTON Peter. Introducción a la computación, Tercera Edición, Editorial Mc. Graw Hill, México (2000)

[7] PIATTINI, Velthuis Mario G., García Rubio Félix O. Calidad en el desarrollo y mantenimiento del software, Editorial Alfaomega Grupo Editor, México (2003)

[8] ESCAMILLA, de los Santos José Guadalupe. Introducción al uso de la computadora e Internet, Primera Edición, Editorial Trillas, México (2000)

[9] H. Fine Leonard, Seguridad en Centros de Cómputo, Segunda Edición 1990, Primera Reimpresión, Editorial Trillas, México (1994)

[10] GRATTON, Pierre. Protección Informática, Primera Edición, Editorial Trillas, México (1998)

[11] TAPSCOTT, Don, Caston Art. Cambio de paradigmas empresariales, Primera Edición, Editorial Mc. Graw Hill, México (1996)

[12] LONG, Larry. Introducción a las computadoras y al procesamiento de información, Segunda Edición, Editorial Prentice Hall, México (1990)

Referencias Electrónicas:

[13] NAVARRETE, Carrasco Roberto Clemente. ¿PARA QUÉ SIRVEN LAS TECNOLOGÍAS DE INFORMACIÓN? [en línea]. (Madrid, España): [citado 2 marzo 2005]. Disponible en World Wide Web:
<http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/usoti.htm#lati>

[14] Definición.org. Tecnologías de la Información [en línea]. [citado 4 marzo 2005]. Disponible en World Wide Web:
<http://www.definicion.org/tecnologias-de-la-informacion>

[16] jungla.dit. Seguridad de las Tecnologías de Información [en línea]. [citado 5 marzo 2005]. Disponible en World Wide Web:
<http://jungla.dit.upm.es/~pepe/libros/aenor2003.htm>

[17] Centro Nacional de Tecnologías de Información. El software y la Seguridad Nacional [en línea]. [citado 6 marzo 2005]. Disponible en World Wide Web:
<http://www.cnti.ve/fundamentos_sl2.html>

[19] SESMERO, Enrique. ¿IMPORTAN REALMENTE LAS TIC? [en línea]. [citado 8 marzo 2005]. Disponible en World Wide Web:
<http://www.gestiopolis.com/Canales4/ger/importic.htm>

[20] COMNET. Uso de restricciones para limitar el acceso a Internet [en línea]. [citado 12 mayo 2005]. Disponible en World Wide Web:
<http://www.comnet.com.ar/ie50.asp>

[21] zonavirus.com. zona virus la historia interminable - la génesis y el devenir de los virus [en línea]. [citado 7 diciembre 2005]. Disponible en World Wide Web:
<http://www.zonavirus.com/datos/articulos/20/LA_HISTORIA_INTERMINABLE_-_G%E9nesis_el_Devenir_Virus.asp>

[22] BIOCOM. SEGURIDAD INFORMÁTICA PARA LOS SISTEMAS DE INFORMACIÓN COMPUTARIZADOS [en línea]. [citado 9 marzo 2005]. Disponible en World Wide Web:
<http://www.biocom.com/informatica_medica/pgp.html>

[23] AQUINO, Luna Rubén. Importancia de la seguridad en Cómputo [CD-ROM]. México, D.F.: Departamento de Seguridad en Cómputo, UNAM 2003.

[24] ÁLVAREZ, Marañón Gonzalo. Amenazas deliberadas a la seguridad de la información [en línea]. [citado 10 marzo 2005]. Disponible en World Wide Web:
<http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html>

[25] LÓPEZ, Hernández José María. Seguridad física COMO [en línea]. [citado 12 marzo 2005]. Disponible en World Wide Web:
<http://es.tldp.org/Manuales-LuCAS/doc-como-seguridad-fisica/COMO-seguridad-fisica.html#INTRODUCCION>

[26] gratisweb.com. Seguridad Informática [en línea]. [citado 2 marzo 2005]. Disponible en World Wide Web:
<http://www.gratisweb.com/auditoriainformatica/seginfo1.htm>

[27] CÁRDENAS, Alanis Claudia del Carmen. Índice de Seguridad en Tecnologías de Información [en línea]. [citado 2 marzo 2005]. Disponible en World Wide Web:
<http://www.monografias.com/trabajos16/tecnologiasinformacion/tecnologias-informacion.shtml>

[28] PONS, Martonell Manuel. Seguridad en Correo Electrónico [en línea]. Enero 2000 [citado 7 mayo 2005]. Disponible en World Wide Web:
< http://www.criptored.upm.es/guiateoria/gt_m013b.htm >

[29] MORENO, José. La crisis y la oportunidad, más allá del lugar común [en línea]. [citado 15 marzo 2005]. Disponible en World Wide Web:
<http://www.chein.com.mx/articulos/2may-2002.htm>

[30] CANCELADO, G. Alberto. SISTEMA DE ADMINISTRACIÓN DE RIESGOS EN TECNOLOGÍA INFORMÁTICA [en línea]. [citado 18 marzo 2005]. Disponible en World Wide Web: <http://www.gestiopolis.com/recursos/documentos/fulldocs/ger1/sistecinfor.htm>

[31] OSORIO, Cuitláhuac. Seguridad en áreas de computación [Disquete]. México, D.F. [citado 5 abril 2005].

[32] Wikipedia, la Enciclopedia Libre. Pretty Good Privacy [en línea]. [citado 12 abril 2005]. Disponible en World Wide Web: <http://es.wikipedia.org/wiki/PGP>

[33] Seguridadysistemas.com, Noticias. La necesidad de proteger nuestros datos [en línea]. [citado 6 abril 2005]. Disponible en World Wide Web: <http://www.seguridadysistemas.com/modules.php?name=Sections&op=viewarticle&artid=42>

[34] Canal Hanoi. Seguridad en Internet [en línea]. (Madrid, España): [citado 7 abril 2005]. Disponible en World Wide Web: <http://www.iespana.es/canalhanoi/internet/segurida.htm>

[35] Kroll Ontrack Inc. Recuperar su servidor no tiene porque ser una pesadilla [en línea]. [citado 18 abril 2005]. Disponible en World Wide Web: <http://www.ontrack.es/biblioteca/articulos/serverNightmaresES_0304.asp>

[36] Fibernet. Disaster Recovery Plan [en línea]. [citado 19 abril 2005]. Disponible en World Wide Web: <http://www.fibernet.es/disaster.htm>

[37] DUEÑAS, Rodríguez Francisco Armando. Sistemas Raid [en línea]. [citado 19 abril 2005]. Disponible en World Wide Web: <http://www.ilustrados.com/publicaciones/EpZVVpykAuidvChMff.php#raid>

[38] TURMO, Sierra Emilio. NTP 215, detectores de humo [en línea]. [citado 20 abril 2005]. Disponible en World Wide Web: <http://www.mtas.es/insht/ntp/ntp_215.htm>

[39] EROSKI. Detectores de humo [en línea]. [citado 20 abril 2005]. Disponible en World Wide Web: <http://revista.consumer.es/web/es/20041001/practico/consejo_del_mes/>

[40] REYES, Mendoza José Alejandro. Preservación de equipo de cómputo [en línea]. [citado 22 abril 2005]. Disponible en World Wide Web: <http://personales.com/mexico/monterrey/preservaciondeequipodecomputo/>

[41] Diseño de páginas web, alojamiento, posicionamiento y dominios en Alicante, España. Definición y explicación del spyware [en línea]. (Alicante, España): [citado 13 abril 2005]. Disponible en World Wide Web: <http://www.masadelante.com/faq-que-es-spyware.htm>

[42] Diseño de páginas web, alojamiento, posicionamiento y dominios en Alicante, España. Programas para eliminar spyware [en línea]. (Alicante, España): [citado 13 abril 2005]. Disponible en World Wide Web: <http://www.masadelante.com/faq-programas-antispyware.htm>

[43] LIMANCHE, T. Germán F. SEGURIDAD DEL HARDWARE [en línea]. [citado 26 abril 2005]. Disponible en World Wide Web: <http://personales.com/bolivia/lapaz/grupo4CPD/politicas.htm>

[44] Wikipedia, la Enciclopedia Libre. Antivirus [en línea]. [citado 3 mayo 2005]. Disponible en World Wide Web: <http://es.wikipedia.org/wiki/Antivirus>

[45] NÚÑEZ, Sandoval Alejandro. Tecnologías de Seguridad en Redes [CD-ROM]. México, D. F.: Departamento de Seguridad en Cómputo UNAM-DGSCA, Abril 2003.

[46] 34TELECOM. VPN: definición básica [en línea]. [citado 11 mayo 2005]. Disponible en World Wide Web: <http://www.34t.com/Oferta/ayuda/VPN%20Definici%C3%B3n%20B%C3%A1sica.html>

[47] Belt Ibérica S. A. Las empresas ponen filtros a Internet [en línea]. [citado 12 mayo 2005]. Disponible en World Wide Web: <http://www.belt.es/noticias/2002/02_diciembre/23_27dediciembre/23dediciembre/23_filtros_internet.htm>

[48] Catholic.net. Filtros de Internet [en línea]. [citado 12 mayo 2005)]. Disponible en World Wide Web: <http://es.catholic.net/temacontrovertido/327/635/articulo.php?id=3289>

Anexo 1

Programas anti-spyware

- *Ad-Aware.* Es un programa de Lavasoft que detecta y elimina spyware. También detecta marcadores de teléfono, troyanos y otros.
- *Spybot.* También conocido como Spybot-S&D, es un programa gratuito de Microsoft Windows que detecta y elimina spyware. Incluye un "inmunizador" que permite bloquear la instalación de spyware.
- *Spy Sweeper*. Es un programa de Microsoft para eliminar spyware. Está considerado uno de los mejores programas para la eliminación de spyware pero su compra proporciona una licencia de sólo un año [42].

Firewalls filtrado de paquetes

Los firewalls filtrado de paquetes son los más rápidos actualmente ya que las reglas de filtrado son aplicadas directamente sobre los paquetes TCP/IP, es decir, el control o aplicación de reglas se realiza entre las capas de red y transporte del modelo OSI. Este tipo de firewalls regularmente se encuentran integrados dentro del núcleo del sistema operativo en aquellos sistemas con capacidad de firewall (Linux) [45].

Firewalls Proxies

Los proxies es software que opera en la capa de sesión y aplicación del modelo OSI. Esta característica hace que estos firewalls requieran de más recursos de cómputo en contraste con los firewalls filtrado de paquetes. Sin embargo, tienen la ventaja de establecer mecanismos más robustos de autenticación [45].

Filtros para Internet

Existen diferentes tipos de filtros. Algunos bloquean el acceso a sitios que contienen determinadas palabras o imágenes, otros restringen completamente el acceso, mientras que algunos más monitorean sitios ya

visitados así como los diálogos en el chat y en el correo electrónico. La elección correcta del filtro, debe ser aquella que mejor se adapte a las necesidades, circunstancias y economía de la familia o la organización.

Tenemos las siguientes opciones de filtros:

- *Chibrow.* Proporciona a los padres o directores de comunidad el control completo de designar los sitios apropiados y seguros que pueden consultar sus hijos o sus miembros.
- *Cyber Patrol.* Permite personalizar el acceso para cada miembro de la familia u organización. Bloquea sitios inapropiados así como permite el acceso a sitios predeterminados de una lista que los padres o directores pueden editar.
- *Disk Tracy.* Bloquea la entrada a sitios con contenidos indeseables y deja un historial de los sitios visitados.
- *The Internet Filter.* Es un programa de filtro y monitoreo tanto de sitios indeseables como de entrada a chats. Manda un correo electrónico a los padres o administradores del filtro cuando ocurre una irregularidad.
- *IamBigBrother.* Monitorea y guarda las actividades y conversaciones en las áreas de chats así como los sitios visitados. Captura imágenes de la pantalla y de los chats. Filtra y bloquea los sitios indeseados.
- *Net Nanny.* Uno de los mejores y más completos filtros que existen, ya que cuenta con un sistema de opciones muy flexible que se adapta a las necesidades de cada miembro de la familia y de cada organización. Cuenta con un sistema tanto de bloqueo como de filtro y monitoreo, así como de límite de tiempo en el uso de Internet con opción a personalizar las cuentas de hasta 12 usuarios.
- *We-Blocker.com.* Programa que bloquea sitios con material pornográfico.
- *Tuk Companion.* Permite la definición de sitios permitidos y restringidos, horarios de navegación y chat y el bloqueo de la ejecución de programas [48].