UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN REDES CON SISTEMAS WINDOWS NT

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

P R E S E N T A :

GABRIELA CAMACHO VILLASEÑOR
MARCO ANTONIO GUEVARA SANTISTEBAN

DIRECTOR DE TESIS: ING. NOÉ CRUZ MARÍN

CIUDAD UNIVERSITARIA **2005**

DEDICATORIA

A Mis Padres

Telma Villaseñor Santoyo
Miguel Ángel Camacho González

A Mis Abuelos †

Teresa Santoyo García
David Villaseñor León

Cruz González
Gabriel Camacho

Porque Donde Quiera Que Este Se Que Me Cuidan Y Me Guían.

A Mi Hermana y a mi Cuñado
Sandra Camacho Villaseñor
Juan José Aranda

A Toda La Familia Villaseñor Y A La Familia Camacho

A Mi Novio
Daniel Figueroa Sánchez

A Mis Jefes
Cruz Sergio Aguilar Díaz
Francisco Javier Montoya

A Mis Amigos, Compañeros De Escuela Y Sobretodo De UNICA

GABRIELA CAMACHO VILLASEÑOR

AGRADECIMIENTOS

A Dios
Por Darme La Fuerza Para Concluir Esta Tesis.

A La UNAM Y a la Facultad de Ingeniería.
Por Ser Mi Alma Mater Y Brindarme Todo Su Apoyo.

A Mis Padres
Telma Villaseñor Santoyo
Miguel Ángel Camacho González.
Por Nunca Perder La Confianza En Mí, En Apoyarme En Todas Mis Cosas, Por Darme La Fuerza Y El Ejemplo Para Superarme Y Ser Mejor. Los Amo Mucho A Los Dos Sobretodo Muchas Gracias Por Ser La Luz, La Guía En Mí Camino. Mamá Gracias Por Darme La Vida Y Ser Mi Fuerza Y Papá Por Ser El Ejemplo En Mi Vida.

A Mis Abuelos
Gracias Abuelitos Por Quererme, Apoyarme Y Sobretodo Tú Abuelita Teresa Por Cuidarme,

Educarme, Ayudarme Y Llevarme Al Kinder. Te Amo Y Te Extraño Mucho.

A Mi Hermana
Sandra Camacho Villaseñor.
Gracias Chaparrita Por Ser Como Eres, Tú Forma De Ser Me Ha Ayudado, Por Esa Fuerza Y El Empeño Con El Que Haces Las Cosas Y Sobretodo Por Los Buenos Momentos Que Hemos Pasado Juntas.

A Mi Novio
Daniel Figueroa Sánchez
Gracias Amor Por Todo Tú Apoyo, Por Ayudarme A Concluir Este Trabajo, Por Darme La Fuerza Para No Dejarme Vencer. No Sabes Como Te Lo Agradezco Este Es Un Triunfo De Los Dos, Sobretodo Por Todo Tú Amor Y Paciencia. Gracias También A Tú Mamá Por Su Apoyo. Te Amo Chiquito Precioso.

A Mi Cuñado Pepe
Muchas Gracias Por Todo Tú Apoyo Y Ejemplo Para Seguir Adelante.

A Mi Tía Elvia
Gracias Vivi Por Estar Conmigo, Quererme, Apoyarme, Aconsejarme Y Llevarme Contigo A Dar Tus Clases Me Sirvieron Mucho. Te Quiero Mucho Tía.

A Mis Jefes
Ing. Cruz Sergio Aguilar Díaz
Ing. Francisco Javier Montoya

Gracias A Ambos Por Todo Su Apoyo, Por La Confianza Brindada, Por Sus Consejos, Enseñanzas, La Ayuda Y Facilidades Para Concluir Esta Tesis.

A Unica, A La Ing. Beatriz,
Ing. Rosario Y Al Ing. Barranco
Por Su Apoyo Y Confianza Brindada.

Ing. Noé Cruz Marín
Por Ser Nuestro Asesor De Tesis, El Apoyo. La Confianza, La Ayuda Y Orientación Para Concluir Esta Tesis.

A Él Ing. Rafael Sandoval
Por Su Amistad, Apoyo, Colaboración En La Realización De Esta Tesis. Gracias Rafa Por Todas Tus Enseñanzas Me Sirvieron De Mucho.

A Mi Compañero De Tesis
Marco Antonio Guevara S.
Gracias Por Tú Amistad Y Colaboración
Para Concluir Esta Tesis

A Todos Mis Amigos Y Profesores
Xochitl, Ema, Rubio, Anabel, Ignacio, Carlos, Ángel, David, Omar, Alejandro, Reynaldo, La Elite, Gonzalo, al Transporte Puma, Yesenia, Arturo, Ing. Maria Sara Valentina, Lic. Claudia Loreto Y A Todos Aquellos Por Falta De Memoria. No Quisiera Omitir, Gracias Por Su Apoyo, Amistad Y Paciencia.

Y A Todos Aquellos Que Me Dieron Su Apoyo Y Me Dijeron "Y Tú Para Cuando..."

GABRIELA CAMACHO VILLASEÑOR

Agradecimientos

Universidad Nacional Autónoma de México
Por brindarme la oportunidad de desarrollarme en el ámbito profesional y así poder alcanzar un objetivo más en mi vida.

Ing. Noe Cruz Marín
Por sus valiosos consejos, por su ayuda y sobretodo por el tiempo dedicado para la elaboración de esta tesis.

Gabriela Camacho Villaseñor
Por tu apoyo, comprensión y tiempo para la culminación de este trabajo de tesis, pero sobretodo por tu amistad durante más de seis años, gracias por todo Gaby.

Ing. Francisco Javier Montoya, Ing. Sergio Aguilar e Ing. Rafael Sandoval
Por toda su ayuda y consejos que me brindaron para la realización de esta tesis.

Marian Aburto
Por tu apoyo y fortaleza que me has brindado siempre, para seguir adelante. Al cariño y comprensión que has tenido conmigo, te quiero mucho Marian, por todos los momentos que hemos pasado juntos.

Ing. Rigel Gámez Leal
Por siempre apoyarme y motivarme para poder alcanzar este sueño, por ser más que un jefe conmigo, siempre has sido un gran amigo. Nunca olvidaré toda la ayuda que me has brindado Rigel, gracias.

Ing. Elizabeth Aguirre, Ing. Gabriel Jaramillo y Leticia Flores
Por sus enseñanzas, por su amistad y por su ayuda en todo momento.

A mis amigos:
David, Araceli, Hugo, Yezmin, Claudia, Andrea, Cristina, Ismael, Luz, Rogelio, Gregorio, Jeanette, Elizabeth, José Luis, Alma, Guadalupe, Nadia, Ema, Luis, Omar, Misao, Antonia, Libertad, Alfredo, Felipe, Margarita, Yesenia, Daniel, Marcela, Fabiola, Angélica, Esther, Miguel, Nubia, Joel, Rosalba, Rosario, Gloria, Hatziri, y a todos los que me faltaron perdón por omitir algunos nombres, pero a todos GRACIAS por su amistad, confianza y por todos esos grandes momentos que hemos pasado juntos.

Y a todas las personas que han sido muy especiales para mi y que de alguna manera me han ayudado con sus comentarios y sus sugerencias en cualquier situación, a lo largo de mi vida.

Marco Antonio Guevara Santisteban

Dedicatorias

Este trabajo esta dedicado con todo mi corazón, mi cariño y mi amor,
a las personas más importantes de mi vida,
gracias por todo lo que me han dado,
ya que esto es posible gracias a ellos.

A mis Padres
Rocío Santisteban Téllez y Marco Antonio Guevara Montes de Oca *por ser mis papás, por quererme, ayudarme y apoyarme en mi vida.*
Por su amor, cariño, comprensión, y paciencia que siempre han tenido conmigo, pero sobretodo por siempre confiar y creer en mi, no tengo palabras para agradecerles todo lo que han hecho por mi, todo lo que soy es por ustedes, este trabajo es suyo, es para mis papas que los quiero mucho.

A mi Hermana
Rocío Guevara Santisteban *por ser mi hermanita a la que quiero mucho, gracias por quererme, ayudarme y apoyarme cuando he necesitado de ti, porque más que mi hermana has sido una amiga en todo momento. Todo mi cariño para ti y a seguir adelante contadora que siempre podrás contar conmigo.*

A mi Familia
A mis abuelitas, abuelitos †, tías, tíos, primas y primos, por siempre apoyarme y ayudarme cuando he necesitado de alguno de ellos; por brindarme su cariño y comprensión siempre que los he necesitado, gracias a todos y recuerden que siempre pueden contar conmigo.

Y a todas aquellas personas que me han ayudado poquito o mucho en todos los aspectos de mi vida, ya que a todos siempre los llevo en mi corazón.

Marco Antonio Guevara Santisteban

ÍNDICE GENERAL

CAPÍTULO 1 ANTECEDENTES

CAPÍTULO 2 TEORÍA DE SEGURIDAD

CAPÍTULO 3 SEGURIDAD FÍSICA (HW)

CAPÍTULO 4 SEGURIDAD LÓGICA (SW)

CAPÍTULO 5 MEDIDAS DE SEGURIDAD Y SANCIONES

CAPÍTULO 6 IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN REDES CON SISTEMAS WINDOWS NT CASO: LABORATORIO DE LA UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO DE LA FACULTAD DE INGENIERÍA DE LA UNAM

OBJETIVOS

OBJETIVO GENERAL

El objetivo principal de esta tesis es el establecer estrategias, procedimientos y políticas de seguridad implementadas a nivel físico, lógico y administrativas en la Unidad de Servicios de Computo Académico (UNICA), en la División de Ciencias Básicas de la Facultad de Ingeniería, UNAM, para mejorar el proceso de detección y corrección de vulnerabilidades, con el fin de proteger la integridad, confidencialidad y disponibilidad de información contra incidentes de seguridad.

OBJETIVOS PARTICULARES

- A NIVEL LÓGICO se busca explotar las herramientas con las que se cuenta los propios sistemas operativos instalados en la sala de cómputo, aprovechar las nuevas tecnologías y servicios para obtener mayor seguridad en la transmisión de información, así como proponer algunas herramientas de seguridad que hagan menos vulnerable los sistemas.

- A NIVEL FÍSICO se propone implementar medidas de seguridad que permitan la manera de controlar los recursos adecuando las necesidades de los usuarios, instalaciones y del personal.

- A NIVEL ADMINISTRATIVO proponer procedimientos preventivos que ayuden a minimizar los incidentes y amenazas de seguridad, las cuales indiquen que hacer antes, durante y después de un incidente o amenaza, además de llevar bitácoras de eventos donde se registren los acontecimientos, así como llevar el control tanto de equipos como de software, infraestructura en general, además de reforzar las políticas existentes de seguridad en la sala de UNICA, en la División de Ciencias Básicas.

Y así ser capaz de mantener en permanente operación el Laboratorio de la Unidad de Servicios de Computo Académico. Para que soporte las actividades del laboratorio y ofrecer un mejor servicio a la comunidad universitaria de la Facultad de Ingeniería.

INTRODUCCIÓN

INTRODUCCIÓN

La información es un insumo esencial para las actividades en la vida universitaria, de ahí la necesidad de fortalecer el desarrollo del laboratorio de cómputo donde la Unidad de Servicios de Cómputo Académico (UNICA) juega un papel central y muy importante.

El objetivo principal de UNICA es cumplir con los requerimientos de sus clientes en el área de cómputo, teniendo como meta elevar la calidad de los productos y servicios. Su misión es la de proporcionar, en el ámbito institucional, los servicios de apoyo en cómputo que la comunidad de la Facultad de Ingeniería requiere, recursos de cómputo comerciales y de alta especialización que el avance de la educación, el desarrollo de la informática y el ejercicio profesional demanden.

La tecnología informática es una herramienta de gran utilidad para el logro de objetivos, donde el volúmen del tráfico de información, es cada vez mayor y a la vez más usuarios tienen acceso a la misma.

Es importante señalar que una adecuada planeación permite una eficiente coordinación, así como el control y la racionalización de actividades y recursos informáticos de la sala de cómputo de la División de Ciencias Básicas de la Facultad de Ingeniería (a nivel software y hardware), lo que consecuentemente ayuda a cubrir con los objetivos del laboratorio.

En los últimos años el uso de las redes de área local han tenido una gran evolución y demanda en empresas públicas y privadas, instituciones educativas principalmente a la necesidad de compartir recursos informáticos y tener una transmisión más segura y eficiente.

El presente trabajo de tesis, esta dedicado a la implementación de medidas de seguridad. Como bien sabemos las computadoras juegan un papel muy importante y hasta crucial, para cualquier trabajo en este tiempo.

La seguridad en un sistema informático, se puede llegar a pensar que es lo primordial mantener una privacidad en la información, por lo que en este tema trabajamos en las medidas que hay que cubrir en cuestión de seguridad, ya que no sólo es a nivel físico, lógico, si no también se toca el nivel administrativo, ya que las personas son las más

involucradas en mantener la seguridad de los sistemas. Ya que son un elemento primordial, para cumplir y hacer cumplir las políticas de seguridad aquí recomendadas.

Esta tesis consta de seis capítulos, los primeros cinco conforman un marco teórico y el último es el caso práctico y la implementación de las medidas de seguridad y de las aportaciones a las políticas de seguridad. Describiremos a continuación una breve síntesis de cada capítulo.

Capítulo 1. "Antecedentes", En este capítulo se habla acerca de los conceptos básicos de redes y de seguridad.

Capítulo 2. "Teoría de Seguridad", En este capítulo profundiza lo que es la seguridad, sus conceptos e importancia, así como de los modelos de seguridad y cuál fue el que se aplicó en esta tesis.

Capítulo 3. "Seguridad Física (Hardware)", Se detalla más medidas de seguridad física que se deben tomar en cuenta en un laboratorio de cómputo.

Capítulo 4. "Seguridad Lógica (Software)", Al igual que en el capítulo anterior también se toca el tema de las medidas pero a nivel lógico que se tienen que llevar en un laboratorio de cómputo.

Capítulo 5. "Medidas de Seguridad y Sanciones", En este capítulo se habla de las políticas de respaldo, así como de los planes de contingencia que deben existir en dicho laboratorio y cuáles son las leyes aplicables y sanciones.

Capítulo 6. "Caso: Laboratorio de la Unidad de Servicios de Cómputo Académico de la Facultad de Ingeniería de la UNAM, División de Ciencias Básicas", En este capítulo se proponen e implementan las medidas y herramientas de seguridad ya estudiadas en los capítulos anteriores, las aportaciones que se realizaron en cuestiones de políticas de seguridad, tener un mejor control con el formato de prestamos de equipos y de software, llevar una bitácora de incidencias, checar las medidas de seguridad físicas, la capacitación del personal para UNICA, Ciencias Básicas.

Todas estas aportaciones y recomendaciones que hacemos a UNICA, esperemos que también puedan servir como referencia para otras instituciones o laboratorios de cómputo y que puedan hacer conciencia de la importancia que tiene la seguridad en todos los aspectos.

Finalmente exponemos nuestras conclusiones del presente trabajo de tesis.

CAPÍTULO 1

ANTECEDENTES HISTÓRICOS

1.1 Antecedentes de Seguridad en Cómputo

Desde los comienzos de la computación, los sistemas se han visto expuestos a una serie de peligros o riesgos que de igual forma han ido aumentando conforme se globalizan las comunicaciones entre los sistemas.

Inicialmente la seguridad fue enfocada al control de acceso físico ya que para acceder a una computadora se requería la presencia física del usuario frente al sistema. A finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadoras. Mientras que por una parte Internet iba creciendo exponencialmente con redes importantes que se adherían a ella, como *BITNET o HEPNET*, por otra parte la informática tenía factores técnicos que iban produciendo piratas informáticos.

Así, comienzan a crecer los sistemas multiusuario en los cuales un recurso computacional era compartido por varios usuarios, surgen nuevos riesgos como la utilización del sistema por personas no autorizadas, manipulación de información o aplicaciones por suplantación de usuarios, aparece un primer esquema de protección basado en Códigos de usuarios y Contraseñas (passwords) para restringir el acceso al sistema, además se establecen distintas categorías de control de acceso a los recursos. Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso *worm* o gusano de Internet. Miles de computadoras conectados a la red se vieron inutilizados durante días, y las pérdidas se estiman en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor muy importante por los responsables o los administradores de los sistemas informáticos. Poco después de este incidente, y a la vista de los peligros que podía causar un fallo o un ataque a los sistemas informáticos estadounidenses (en general, a los sistemas de cualquier país) la agencia DARPA (*Defense Advanced Research Projects Agency*) creó el CERT (*Computer Emergency Response Team*), un grupo formado en su mayor parte por voluntarios calificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten al *host* de Internet.

Los sistemas siguen evolucionando y se inicia la computación en red, en la cual además de los riesgos asociados a los sistemas multiusuarios, aparece un nuevo tipo de vulnerabilidad, básicamente en el proceso de transmisión de la información; aunque las primeras redes estaban aisladas del mundo exterior estaban expuestas a los posibles atacantes internos.

Con la evolución de la tecnológica se inicia el proceso de interconexión de las distintas redes aisladas de una empresa para configurarse en redes corporativas, donde aumentan considerablemente los riesgos ya que es más difícil controlar la totalidad de la red.

Han pasado diez años desde la creación del primer CERT “Equipo de Respuesta a Incidentes de Seguridad en Cómputo”, y cada día se hace patente la preocupación por los temas relativos a la seguridad en la red y a sus equipos, también se hace patente la necesidad de esta seguridad. Además de los piratas informáticos, ha habido nuevas generaciones de intrusos que forman grupos, con un objetivo principal: compartir conocimientos. Hoy en día cualquiera tiene a su disposición gigabytes de información electrónica publicada en Internet; cualquier aprendiz de pirata puede conectarse a un servidor *web*, descargar un par de programas y ejecutarlos contra un servidor desprotegido, tanto así, que esa misma persona puede conseguir el control total sobre un servidor Unix, probablemente desde su PC con Windows 98 y sin saber nada sobre Unix. Por si esto fuera poco, presumen, a través de sistemas de conversación como el IRC (*Internet Relay Chat*), donde en canales como #hack o #hackers jactan de sus logros ante sus colegas.

Quizás hoy en día estamos en la fase en la cual la mayoría de las redes es están siendo conectadas a redes públicas como Internet, CompuServer, BitNet, etc., en las cuales la seguridad se ha convertido en un gran problema, pero a pesar de que las oportunidades han sido ampliadas a millones de clientes, desgraciadamente los atacantes también han crecido en forma considerable.

Es responsabilidad de los diseñadores y administradores de sistemas, el proveer la suficiente garantía y confiabilidad que permita operar en las mejores condiciones y lograr un funcionamiento continuo de los sistemas bajo el mejor clima de confianza de nuestros usuarios, garantizando el respeto por niveles adecuados de confidencialidad e integridad de la información que procesamos.

Aunque inicialmente el interés de entrar ilegalmente a los sistemas fue el reto técnico de lograrlo, el número de incidentes y ganancias por la entrada ilegal ha aumentado considerablemente. Incidentes como el robo de información, espionaje industrial, estafas, extorsión, daño de sistemas, terrorismo, etc. se cuentan como los nuevos objetivos de ataques a los sistemas utilizados.

Entre los aspectos más relevantes de preocupación en los sistemas de seguridad se encuentra todo lo relacionado con:

1) Los servidores con sistemas operativos como UNIX, DEC, NT, Netware, etc; los cuales, de alguna forma, representan grandes riesgos.

2) Los protocolos de comunicaciones, representan uno de los puntos de vulnerabilidad más utilizado en las redes.

3) Las aplicaciones del sistema o de los usuarios.

4) Bases de datos, entre otros tópicos.

Definitivamente si para minimizar los riesgos “nunca hay un sistema 100% protegido”, es necesario tomar conciencia del problema y adoptar una metodología o guías para enfrentarlo. Con el conocimiento profundo de nuestra red, un análisis de amenazas y riesgos, la adopción de políticas de seguridad y finalmente la utilización de las tecnologías adecuadas, se podrá obtener un sistema seguro, además de incorporar herramientas de criptografía, cortafuegos (Firewalls), monitoreo, realizar auditorías y hasta esquemas proactivos que para poder anticipar ataques y prevenirlos.

1.2 Problemas de Seguridad

Existen muchos problemas de seguridad tanto a nivel lógico como físico y estos problemas son ocasionados por las diferentes amenazas y ataques que existen, para lo cual es necesario conocerlos.

Un sistema informático es un conjunto de elementos hardware, software, datos/información y personal que hacen posible el almacenamiento, proceso y transmisión de la información con el objetivo de realizar una determinada tarea. Todos estos elementos son susceptibles de ser atacados y sobre ellos tenemos una serie de amenazas, estas amenazas son problemas que pueden ser lógicos como físicos.

La mayoría de los problemas son a nivel lógico y aunque son varios los elementos que conforman un sistema informático, será la *información* el recurso más preciado sobre el cual se pone un mayor énfasis para tener un nivel aceptable de seguridad.

Los objetivos básicos de la seguridad de la información son:

- Confidencialidad: Asegurar que la información no es expuesta o revelada a personas no autorizadas.

- Integridad: Asegurar consistencia de datos, en particular prevenir la creación, alteración o borrado de datos de entidades no autorizadas.

- Disponibilidad: Asegurar que los usuarios legítimos no tengan acceso restringido a su información y recursos

- Uso legítimo: Asegurar que los recursos no son usados por personas no autorizadas o en formas no autorizadas.

Para soportar estos objetivos necesitamos definir las Políticas de Seguridad que regirán nuestro dominio de seguridad. Estas políticas deben ser definidas en varias categorías: acceso físico, seguridad en la comunicación, computadoras, sistemas operativos, bases de datos, aplicaciones, personal, ambiente natural, respaldos, planes de contingencias, y más.

Una amenaza es una persona, entidad, evento o idea que plantea algún daño a un activo.

Un ataque es una realización de una amenaza.

Una protección son los controles físicos, mecanismos, políticas y procedimientos que protegen nuestros activos o recursos de las amenazas (problemas).

Una vulnerabilidad es el debilitamiento o ausencia de una protección en un recurso o activo.
Un riesgo es una medida del costo de una realización de una vulnerabilidad que incorpora la probabilidad de éxito de un ataque. El riesgo es alto si el valor del activo vulnerable es alto y la probabilidad de éxito de un ataque es alto.

Las amenazas pueden ser clasificadas en intencionales y accidentales siendo las primeras las más peligrosas. Las amenazas intencionales lo cual se convierte en un ataque, puede ser pasivo o activo.

Un *ataque pasivo* es aquel que no causa modificación o cambio en la información o recurso, son los más peligrosos ya que los fines que se alcanzan son más letales y beneficiosos para el que los comete. "Quizás en este momento en su red tenga un intruso invisible".

Los *ataques activos*, son aquellos que producen cambios en la información o en el comportamiento del sistema.

1.2.1 Clasificación de las amenazas

Podemos clasificar las amenazas en:

1. Amenazas fundamentales: Afectan directamente los cuatro objetivos básicos de la seguridad: Fugas de información, violación a la integridad, no disponibilidad de servicios y uso ilegítimo.

2. Amenazas habilitadoras primarias: Son importantes porque la realización de cualquiera de estas amenazas puede conducir directamente a la realización de las amenazas fundamentales. Éstas son:

    1) Suplantación
    2) Sobrepasar los controles
    3) Violación con autorización
    4) Caballo de Troya
    5) Puerta trasera
    6) Bombas lógicas
    7) Virus

3. Amenazas subyacentes: Si analizamos cualquiera de las amenazas fundamentales o de habilitación de las primarias en un ambiente dado, podemos identificar amenazas subyacentes particulares cualquiera de las cuales puede habilitar las amenazas fundamentales. Por ejemplo si consideramos la amenaza fundamental de Fugas de información podemos encontrar varias amenazas subyacentes, tales como:

    - Escuchar sin autorización.
    - Análisis de tráfico.
    - Indiscreción por personal.
    - Reciclaje de medios.

Según estadísticas obtenidas, las siguientes amenazas o tipos de ataque más predominantes son:

- Violación con autorización.
- Suplantación.
- Sobrepasar los controles.
- Caballos de Troya y puertas traseras.

Además a todo esto tenemos que agregar los problemas físicos que se pueden presentar, como las catástrofes (naturales o artificiales) son las amenazas menos probables contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos y más en una gran urbe como la ciudad de México, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que si se produjeran generarían los mayores daños.

Un subgrupo de las catástrofes es el denominado de riesgos poco probables. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la del resto de catástrofes) que nadie toma, o nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son un ataque nuclear contra el sistema, el impacto de un satélite contra la sala de operaciones. Nada nos

asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

Como ejemplos de catástrofes se encuentran los terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que se piensa); los riesgos poco probables los trataremos como algo anecdótico. De cualquier forma, vamos a hablar de estas amenazas sin extendernos mucho, ya que el objetivo de este proyecto no puede ser el proporcionar las directrices para una construcción de edificios a prueba de terremotos, o un plan formal de evacuación en caso de incendio.

1.3 Niveles de Seguridad

Existen diferentes sistemas o mecanismos de seguridad, que pueden ser implantados en hardware, software o sistemas de seguridad (dispositivos, programas y aplicaciones en conjunto). La elección de la seguridad que se requiere en cada caso depende de qué tan importante es la información que le maneja. Se han establecido criterios de niveles de seguridad para la evaluación de sistemas entre ellos se encuentran TCSEC (Trust Computer System Evaluation Criteria) en Estados Unidos, CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) en Canadá e ITSEC (Information Tecnology Security Evaluation) el cual es un acuerdo entre países europeos: Alemania, Inglaterra, Francia y Holanda. Sin embargo, cada uno de ellos presenta diferencias entre sus niveles de seguridad.

Todos los criterios de seguridad consideran importante el diseño del producto hasta los últimos niveles, pero otro aspecto a considerar es la evaluación de servicios y aplicaciones, por lo que se debe estudiar las técnicas de seguridad más convenientes para lo que se desea proteger.

Para nuestro país existe una situación muy preocupante con respecto a la seguridad, ya que parece que proteger la información manejada en las redes de comunicaciones no era de mucha importancia, incluso no existía ninguna ley que penalizará los delitos electrónicos. Debido a esta situación algunas empresas principalmente los bancos, han recurrido a mecanismos como el cifrado para garantizar que las transacciones realizadas no sean alteradas. Es necesario que tanto organismos gubernamentales como privados establezcan estrictos sistemas de seguridad, para esto se propone para México los siguientes niveles de seguridad de acuerdo a los criterios que otros países han utilizado tanto a nivel software como a nivel hardware para tener redes más seguras. A continuación se presentan estos niveles de seguridad:

Nivel 0

No existe ninguna forma de seguridad por lo que no es confiable el sistema entero. No hay dispositivos ni programas que limiten a usuarios ajenos el uso del sistema. Un ejemplo de este nivel es la instalación de un sistema que no es capaz de monitorear o detectar el usuario que esta operando.

Nivel 1

Se emplean sistemas de autentificación como por ejemplo palabra clave (password) que sólo conoce el usuario y determina los derechos de acceso a programas e información que tiene dentro del sistema, así como también la ejecución de ciertos comandos. Cada usuario puede proteger su información mediante el establecimiento de los permisos que especifique. Sin embargo el control de este sistema lo tiene el administrador el cual puede acceder a todos los programas e información sin existir una vigilancia en sus acciones. La evaluación de las aplicaciones que se encuentra en esta categoría será aprobada cuando las tareas que especifican sean cumplidas durante su ejecución en un sistema comercial.

Nivel 2

Se incluye el nivel uno y la creación de niveles de autorización en el sistema. El sistema debe manejar una seguridad multinivel y no todos los usuarios tienen derecho a ejecutar ciertos comandos, o que el administrador pueda hacer uso con toda libertad de la información perteneciente a usuarios del sistema. En este último caso interviene el sistema de auditoria que registra tanto las acciones de los usuarios como el administrador que esta a cargo del control de la red.

En este nivel todavía se habla de aplicaciones, considerando más restricciones de seguridad. Para hacer efectivas las técnicas de seguridad, éstas deben implantarse desde el momento del diseño de la aplicación y evaluarlas para garantizar su nivel.

Nivel 3

Además de dejar a cargo el monitoreo y control de las acciones de usuarios al sistema, existe otro mecanismo de protección para el manejo de información como lo es la codificación.

Nivel 4

Contiene los anteriores niveles y la implementación de dispositivos, por ejemplo: los firewalls, conocidos también como cortafuegos. Estos dispositivos solamente filtran la información, deciden que servicios pueden ser accesados desde el exterior de una red privada, por quienes pueden ser ejecutados y también que servicios pueden hacer uso los usuarios del exterior.

Nivel 5

En este nivel se debe pensar en seguridad de dominios mediante la instalación de sistemas de seguridad. El sistema debe especificar detalladamente su funcionalidad, diseños de hardware y deben contener funciones de prueba que lo validen.

Nivel 6

Es el nivel de seguridad más efectivo pero el más costoso, puesto que se necesita implantar herramientas de seguridad cuyo análisis debe considerar todo el sistema que se requiere asegurar. Para su validación se requiere del diseño de la arquitectura, el diseño de implantación, documentos de su funcionalidad, las garantías que establece. Debe probarse su funcionalidad y a su vez buscar puntos vulnerables que pudiera tener.

Estos niveles de seguridad son una propuesta que sirven para establecer un criterio de seguridad para nuestro país; que consisten en siete niveles de acuerdo a los establecidos por Estados Unidos, Canadá y los países europeos, con el fin de abarcar los aspectos más importantes de seguridad del software y del hardware.

Se proporcionan en la actualidad diferentes productos de software y hardware que brindan seguridad en la información que se maneja en la red de los diversos usuarios, aunque es necesario que se estén actualizando los diferentes sistemas de seguridad tanto para el aspecto físico como lógico.

1.4 Fundamentos de las Redes de Computadoras

1.4.1 Definición de Red.

Una red son computadoras conectadas entre sí, con el fin de compartir recursos e información y son capaces de realizar comunicaciones electrónicas.

Uno de los principales objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. Otro de los objetivos consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro.

Los elementos para crear una red es interconectar físicamente las computadoras. Para eso se utiliza una tarjeta de red, cables y concentradores. Una vez resuelta la comunicación física, se debe instalar el sistema operativo de red en los servidores, haciéndolos responsables de la distribución y del control de los servicios disponibles. Además del software, existe también un conjunto de programas ejecutados en las estaciones de trabajo, que junto con la tarjeta de red permiten establecer la comunicación con el servidor.

1.4.2 Tipo de Redes

LAN.-Redes de área local. 10 m. - 10 Km.

Es una red que cubre una extensión reducida como una empresa, una universidad, un colegio, etc. No habrá por lo general dos ordenadores que disten entre sí más de un kilómetro.

Una configuración típica en una red de área local, es tener una computadora llamada servidor de archivos en la que se almacena todo el software de control de la red, así como el software que se comparte con las demás computadoras de la red.

Las computadoras que no son servidores de archivos reciben el nombre de estaciones de trabajo. Éstos suelen ser menos potentes y tienen software personalizado por cada usuario. La mayoría de las redes LAN están conectadas por medio de cables y tarjetas de red, una en cada equipo.

MAN.-Redes de área metropolitana. 10 Km. – 100 Km.

Las redes de área metropolitana cubren extensiones mayores como pueden ser una ciudad o un distrito. Mediante la interconexión de redes LAN se distribuyen la informática a los diferentes puntos del distrito. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

WAN.-Redes de área amplia. 100 Km. - 1000 Km.

Las redes de área extensa cubren grandes regiones geográficas como un país, un continente o incluso el mundo. Cable transoceánico o satélites se utilizan para enlazar puntos que distan grandes distancias entre sí. En conclusión una Red WAN es una red en la cual pueden transmitirse datos a larga distancia, interconectando facilidades de comunicación entre diferentes localidades de un país.

Redes según su conexión

- Redes dedicadas o exclusivas.

Son aquellas que por motivo de seguridad, velocidad o ausencia de otro tipo de red, conectan dos o más puntos de forma exclusiva. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

- Redes punto a punto

Permiten la conexión en línea directa entre terminales y computadoras. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión y la seguridad que presenta. Su desventaja sería el precio muy elevado de este tipo de red.

- Redes multipunto.

Permite la unión de varios terminales a su correspondiente computadora compartiendo una única línea de transmisión. La ventaja consiste en el abaratamiento de su costo, aunque pierde velocidad y seguridad. Este tipo de redes requiere amplificadores y difusores de señal o de multiplexores que permiten compartir líneas dedicadas.

- Redes compartidas

Son aquellas a las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con transmisiones de otras naturalezas. Las redes más usuales son las de conmutación de paquetes y las de conmutación de circuitos.

- Redes digitales de servicios integrados (RDSI)

Se basan en desarrollos tecnológicos de conmutación y transmisión digital. La RDSI es una red de uso general capaz de integrar una gran gama de servicios como son la voz, datos, imagen y texto. La RDSI requiere de la instalación de centrales digitales.

1.4.3 Topología de Redes

Una red esta formada por cables que conecta las computadoras entre sí, y a la forma en que se distribuye el cableado y los componentes de la red se le llama topología, es la manera en que trabajan las máquinas, ya sea física o lógicamente en la red. Las topologías se clasifican de la siguiente manera:

1.4.3.1 Topología de bus

En esta topología todas las computadoras y/o dispositivos están conectados a un mismo cable llamado *bus*. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red. Todos los Nodos de la Red están unidos a este cable. Este cable recibe el nombre de "Backbone Cable" (bus de difusión). Se denomina *bus de difusión* ya que las señales que transmite la computadora para comunicarse por la red con otras máquinas son señales eléctricas (corrientes y/o voltajes) éstas se "difunden" o "dispersan" por todo el cable. Su principal característica consiste en que la única manera en que deja de trabajar la red es abriendo el medio, en el bus de difusión, en cualquier otro caso como si el cable que une el servidor o a las terminales con el bus se rompe, la red sigue funcionando, sólo se desconecta de la red el equipo al que estaba conectado con dicho

cable. El bus debe tener terminadores en los extremos, esto con el fin de eliminar las señales que se difunden por el cable. Tanto Ethernet como Local Talk pueden utilizar esta topología. Además si algún equipo deja de funcionar, la red sigue funcionando. A continuación se muestra en la figura 1.1 la topología de bus:

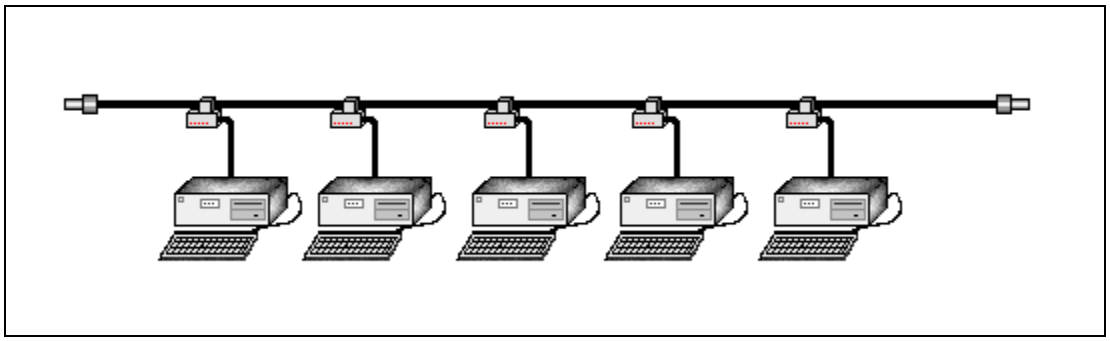


Figura 1.1 Topología de Bus

Ventajas

- Es más fácil conectar nuevos nodos a la red.
- Requiere menos cable que una topología estrella.

Desventajas

- Toda la red se cae si hay una ruptura en el cable principal.
- Se requiere de terminadores.
- Es difícil detectar el origen de un problema cuando toda la red cae.
- No se debe utilizar como única solución en un gran edificio.

1.4.3.2 Topología de Anillo

En esta topología, la información lleva un sólo sentido; esto se consigue poniendo las computadoras sobre el bus obligando a la señal a llevar un sentido. Los nodos de la red se disponen en un anillo cerrado conectado a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el nodo principal es quien gestiona conflictos entre nodos al evitar la colisión de tramas de información. En este tipo de topología, un fallo en un nodo afecta a toda la red aunque actualmente hay tecnologías que permiten mediante unos conectores especiales, la desconexión del nodo averiado para que el sistema pueda seguir funcionando. La topología de anillo esta diseñada como una arquitectura circular, con cada nodo conectado directamente a otros dos nodos. Toda la información de la red pasa a través de cada nodo hasta que es tomado por el nodo apropiado.

A continuación se muestra en la figura 1.2 la topología de anillo:

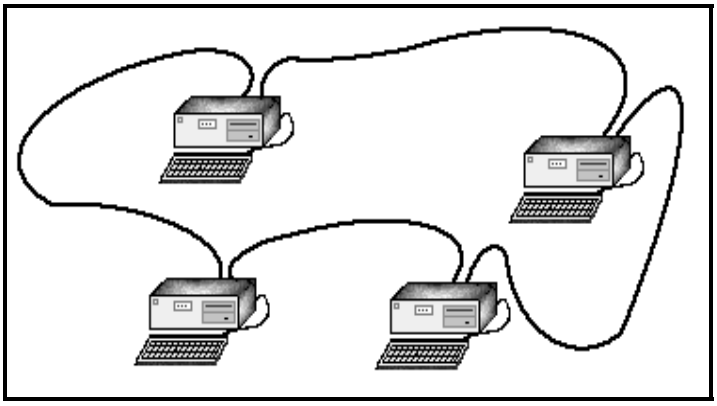


Figura 1.2 Topología de Anillo.

1.4.3.3 Topología de Estrella

Es una topología estrella todos y cada uno de los nodos de la red, estos se conectan a un concentrador o hub. Los datos de estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos. En ésta topología toda la información pasa por el centro. La única manera de que deje de trabajar la red es al fallar el hub, en cualquier otro caso la red sigue funcionando (como lo es la desconexión o falla de algún equipo o dispositivo conectado al hub). A continuación se muestra en la figura 1.3 la topología de estrella:

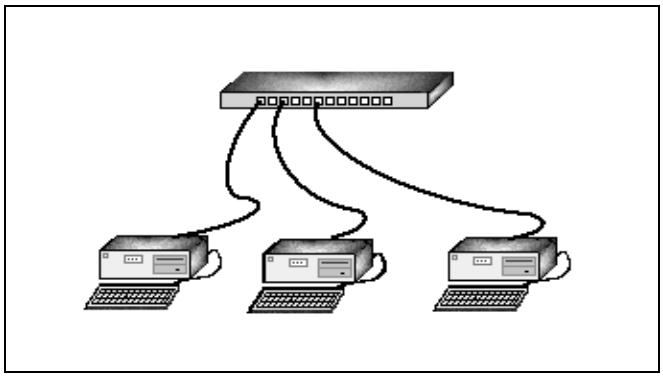


Figura 1.3 Topología de estrella.

Ventajas

- Gran facilidad de instalación.
- Posibilidad de desconectar elementos de red sin causar problemas.
- Facilidad para la detección de fallo y su reparación.

Desventajas

- Requiere más cable que la topología de bus.
- Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados.
- Se han de comprar hubs o concentradores.

1.4.3.4 Topología de Árbol

La topología de árbol combina características de la topología de estrella con la BUS. Consiste en un conjunto de subredes estrella conectadas a un BUS. Esta topología facilita el crecimiento de la red. A continuación se muestra en la figura 1.4 la topología de árbol:

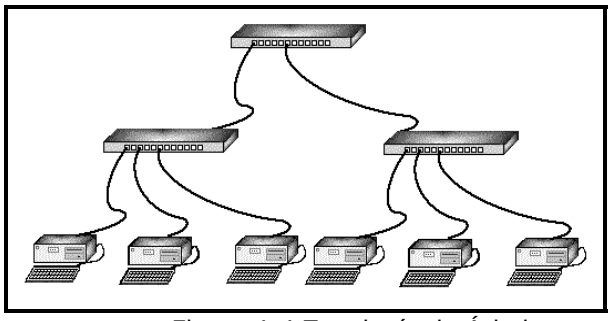


Figura 1.4 Topología de Árbol.

Ventajas

- Cableado punto a punto para segmentos individuales.
- Soportado por multitud de vendedores de software y de hardware.

Desventajas

- La medida de cada segmento viene determinada por el tipo de cable utilizado.
- Si deja de funcionar el segmento principal todo el segmento también lo hace.
- Es más difícil su configuración.

Tipo Malla

En esta topología, todos los nodos se conectan con todos los nodos. El inconveniente radica en la cantidad de cable usado para unir todos los dispositivos. La principal ventaja consiste en que si algún equipo falla o algún cable se rompe no se cae la red. Ni en ningún otro caso (sólo el extremo de que todos fallen).

1.4.3.5 Topologías Híbridas

- Topología de Estrella Cableada

Físicamente parece una topología estrella pero el tipo de concentrador utilizado, la MAU se encarga de interconectar internamente la red en forma de anillo. Esta topología es la que se utiliza en redes Token Ring.

- Jerárquica

Los equipos se conectan de grado de potencia.

- Anillo Doble

En esta topología, se parece a la tipo anillo, pero si algún equipo deja de funcionar, se desconecta o se rompe un cable, la señal se regresa. Esta topología es utilizada en la Interfase de Distribución de Datos por Fibra (FDDI).

- Mejoras al anillo o estrella anillo

Esta topología, físicamente parece estrella, pero realmente trabaja como anillo. Al dispositivo que une las terminales se denomina MAU (Unidad de Acceso Multiestación).

- Bus-estrella

Esta topología, físicamente parece estrella pero lógicamente es un BUS. Al dispositivo que une las terminales se denomina concentrador (Hub).

1.4.4 Medios de Transmisión

Medios de transmisión guiados

En medios guiados, el ancho de banda o velocidad de transmisión dependen de la distancia y de sí el enlace es punto a punto o multipunto.

Par trenzado

Es el medio guiado más usado. Consiste en un par de cables, embutidos para su aislamiento, para cada enlace de comunicación. Debido a que puede haber acoples entre pares, estos se trenza con pasos diferentes. La utilización del trenzado tiende a disminuir la interferencia electromagnética. Este tipo de medio es el más utilizado debido a su bajo coste, pero su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance. Con estos cables, se pueden transmitir señales analógicas o digitales. Es un medio muy susceptible a ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas.

VENTAJAS

- Fácil instalación.
- Es económico.

- Se pueden transmitir señales analógicas o digitales.

DESVENTAJAS

- Susceptible al ruido.
- Susceptible a las interferencias.
- Poca velocidad de transmisión.
- Corta distancia de alcance.

Cable coaxial

Consiste en un cable conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre por otra capa aislante que es la funda del cable. Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones. Se utiliza para transmitir señales analógicas o digitales. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor por cada kilómetro.

Ventajas

- Es económico.
- No es necesario utililizar demasiados repetidores.
- Soporta conexiones de banda ancha y en banda base.
- Se utiliza para varias señales (voz, video y datos)

Desventajas

- Difícil manejo por su grosor.
- Atenuación.
- Ruido térmico.
- Ruido de ínter modulación.

Fibra óptica

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta que se encarga de aislar el contenido de aplastamientos, abrasiones, etc. Es un medio muy apropiado para largas distancias e incluso últimamente para LAN'S.

Ventajas

- Permite mayor ancho de banda.
- Menor tamaño y peso.
- Menor atenuación.
- Aislamiento electromagnético.
- Mayor separación entre repetidores.
- Su rango de frecuencias es todo el espectro visible y parte del infrarrojo.

Desventajas

- Sólo pueden suscribirse las personas que viven en las zonas de la ciudad por las cuales ya esté instalada la red de fibra óptica.
- El coste es alto en la conexión de fibra óptica, las empresas no cobran por tiempo de utilización sino por cantidad de información transferida al computador, que se mide en megabytes.
- El coste de instalación es elevado.
- Fragilidad de las fibras.
- Disponibilidad limitada de conectores.
- Dificultad de reparar un cable de fibras roto en el campo.

1.4.5 Clases de Cableado

- Clase A

Soporta aplicaciones hasta de 100 Khz. Incluye telefonía y otras aplicaciones de poco ancho de banda pensadas para distancias de campus. Se utiliza en centrales privadas de comunicación, redes punto a punto entre otros.

- Clase B

Soporta aplicaciones de 1Mhz.Comprende aplicaciones que trabajan a moderada rapidez de aplicación y sobre distancias de campus.

- Clase C

Soporta aplicaciones de hasta 16Mhz. Incluye alta rapidez de transmisión de bits para cortas distancias.

- Clase D

Soporta aplicaciones que trabajan hasta 100Mhz. Comprende muy altas velocidades de transmisión binaria a cortas distancias.

- Clase óptica

Ofrece la mayor velocidad posible.

Características	Coaxial thinnet (10Base2)	Coaxial thicknet (10Base5)	Par trenzado (10BaseT)	Fibra óptica
Costo del cable	Más caro que el par trenzado	Mayor que el tinte	Menos caro	Más caro
Máxima longitud del cable	185 metros (607 pies)	500 metros (1640 pies)	100 metros (328 pies)	2 kilómetros (6562 pies)
Rango de transmisión	10 Mbps.	10 Mbps.	10 Mbps.-100 Mbps.	100 Mbps. o más
Flexibilidad	Bastante flexible	Menos flexible	El mas flexible	No flexible
Facilidad de instalación	Fácil de instalar	Fácil de instalar	Muy fácil de instalar	Difícil de instalar
Susceptibilidad de interferencia	Buena resistencia a la interferencia	Buena resistencia a la interferencia	Susceptible a la interferencia	No susceptible a la interferencia
Características especiales	Componentes electrónicos menos caros que el par trenzado	Componentes electrónicos menos caros que el par trenzado	El mismo cable que el del teléfono. A menudo preinstalado en los edificios	Soporta voz, datos y video.
Preferencia de usos	Sitios medianos a grandes con necesidades de alta seguridad	Se usa en conexiones de punto a punto y en redes Thinnet	UTP en sitios con pequeño presupuesto. STP Token Ring de cualquier tamaño	Cualquier tamaño de instalación que requiera alta velocidad de datos, así como seguridad.

Tabla 1.1 Comparación de Cables.

1.4.6 Modelo OSI

La necesidad de la normalización de las redes condujo a la Organización Internacional de Normalización (I.S.O.) a la creación del subcomité de sistemas abiertos (OSI) en 1977.

El modelo OSI es utilizado por todas las redes del mundo y consisten en siete capas o niveles donde cada una de ellas define las funciones que deben proporcionar los protocolos con el propósito de intercambiar información. Cada nivel depende de los que están por debajo de él, y a su vez proporciona alguna funcionalidad a los niveles superiores.

OSI en realidad no es una arquitectura particular, porque no especifica los detalles de los niveles, sino que los estándares de ISO existen para cada nivel.

- *Nivel físico*. Cuestiones: los voltajes, la duración de un bit, el establecimiento de una conexión, el número de polos en un enchufe, etc.
- *Nivel de enlace.* El propósito de este nivel es convertir el medio de transmisión crudo en uno que esté libre de errores de transmisión.

    - El remitente parte los datos de entrada en marcos de datos (algunos cientos de bytes) y procesa los marcos de acuse.

    - Este nivel maneja los marcos perdidos, dañados, o duplicados.

    - Regula la velocidad del tráfico.

    - En una red de broadcast, un subnivel (el subnivel de acceso medio, o medium access sublayer) controla el acceso al canal compartido.

- *Nivel de red.* Determina el ruteo de los paquetes desde sus fuentes a sus destinos, manejando la congestión a la vez. Se incorpora la función de contabilidad.

- *Nivel de transporte*. Es el primer nivel que se comunica directamente con su par en el destino (los de abajo son de máquina a máquina. Provee varios tipos de servicio (por ejemplo, un canal punto-a-punto sin errores). Podría abrir conexiones múltiples de red para proveer capacidad alta. Se puede usar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples entrando en una máquina. Provee el control de flujo entre los hosts.

- *Nivel de sesión*. Parecido al nivel de transporte, pero provee servicios adicionales. Por ejemplo, puede manejar tokens (objetos abstractos y únicos) para controlar las acciones de participantes o puede hacer checkpoints (puntos de recuerdo) en las transferencias de datos.

- *Nivel de presentación*. Provee funciones comunes a muchas aplicaciones tales como traducciones entre juegos de caracteres, códigos de números, etc.

- *Nivel de aplicación*. Define los protocolos usados por las aplicaciones individuales, como e-mail, telnet, etc.

Ventajas del modelo OSI

- OSI define claramente las diferencias entre los servicios, las interfaces, y los protocolos.

    - Servicio: lo que un nivel hace

    - Interfaz: cómo se pueden accesar los servicios

    - Protocolo: la implementación de los servicios

- Porque OSI fue definido después de implementar los protocolos, los diseñadores no tenían mucha experiencia, como en donde se debieran ubicar las funcionalidades, y algunas otras faltan. Por ejemplo, OSI originalmente no tiene ningún apoyo para broadcast.

- OSI no tuvo éxito debido a:

- Mal momento de introducción: insuficiente tiempo entre las investigaciones y el desarrollo del mercado a gran escala para lograr la estandarización.

- Mala tecnología: OSI es complejo, es dominado por una mentalidad de telecomunicaciones sin pensar en computadores, carece de servicios sin conexión, etc.

- Malas implementaciones

- Malas políticas: investigadores y programadores contra los ministerios de telecomunicación.

1.4.7 Protocolos

Un protocolo es un conjunto de normas que rigen la comunicación entre las computadoras de una red. Estas normas especifican que tipo de cables se utilizarán, que topología tendrá la red, que velocidad tendrán las comunicaciones y de que forma se accederá al canal de transmisión.

1.4.7.1 Protocolo TCP/IP

TCP/IP es un conjunto de protocolos de comunicación, entre los cuales los más importantes son el TCP y el IP, de ahí toma su nombre.

- Tiene como objetivos la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida.

- La red es packet-switched y está basada en un nivel de internet sin conexiones. Los niveles físico y de enlace (que juntos se llaman el "nivel de host a red" aquí) no son definidos en esta arquitectura.

- Nivel de internet. Los hosts pueden introducir paquetes en la red, los cuales viajan independientemente al destino. No hay garantias de entrega ni de orden. Este nivel define el Internet Protocol (IP), que provee el ruteo y control de congestión.

- Nivel de transporte. Permite que pares en los hosts de fuente y destino puedan conversar. Hay dos protocolos:

    - Transmission Control Protocol (TCP). Provee una conexión confiable que permite la entrega sin errores de un flujo de bytes desde una máquina a alguna otra en la internet. Parte el flujo en mensajes discretos y lo monta de nuevo en el destino. Maneja el control de flujo.

    - User Datagram Protocol (UDP). Es un protocolo no confiable y sin conexión para la entrega de mensajes discretos. Se pueden construir otros protocolos de aplicación sobre UDP. También se usa UDP cuando la entrega rápida es más importante que la entrega garantizada.

- Nivel de aplicación. No se usan niveles de sesión o presentación.

TCP/IP no define la capa de enlace ni la física, esto produce que TCP/IP es independiente de la arquitectura de la red.

Todos los protocolos están definidos en una de las capas de TCP/IP.

1.4.7.2 Protocolo TCP

Significa Protocolo de Control de Transmisión. La principal función de TCP es que los datos lleguen a su destino. Es un protocolo altamente confiable, el cual tiene:

1. Sistema de Transferencia básico.

Son dos modos:

- Modo Stream (flujo): Se basa en que TCP corta y encapsula los paquetes de información.

- Modo Orientado a Carta (registro): Se manejan bloques de información donde cada bloque se llama carta o registro. El corte lo hace la capa de aplicación.

2. Confiabilidad.

Se tiene la certeza que el paquete de información (denominado segmento) ha llegado a su destino; esto lo hace por medio de diferentes mecanismos:

a) Número de Secuencia: Es un número que se asigna de forma consecutiva a cada byte que se transmite.

b) ACKnowledgement (ACK): Bandera de confirmación de la llegada del paquete a su destino. Por cada paquete que envía el origen, el destino debe enviar un mensaje ACK con su número ACK (número de secuencia del siguiente byte que espera recibir). Si llegase al destino un paquete que no es el que espera, entonces no envía el ACK.

c) Check Sum: Es una fórmula matemática que nos permite transformar un flujo de bits de información en un número el cual es enviado en la cabecera del paquete. La máquina destino los compara (aplicando al paquete que llega la misma ecuación) y si son iguales es que es la misma información que salió, y si son diferentes es debido a que se alteró la información, en tal caso se desecha ese paquete y se espera a que vuelva a enviar el origen el mismo paquete a falta de señal ACK por parte del destino.

3. Control de Flujo.

Este sistema permite regular la cantidad de información que se transmitirá en base al número de señales ACK recibidas. Aquí se introducirá el concepto de ventana. Que es la cantidad de datos que un equipo puede enviar antes de llegar una confirmación ACK. Por ejemplo: Si la ventana es de 5000, quiere decir que al llegar a 5000 datos deja de transmitir sin que halla llegado una confirmación.

4. Multiplexación.

Al igual que en el multiplexor, se selecciona de varias entradas una salida hacia un puerto (número que se asigna a cada uno de los protocolos de la capa de aplicación). La variable en la que lleva la información es de 2 bytes, por lo que puede haber en un equipo hasta 65536 puertos corriendo al mismo tiempo (lo que es 2^{16}).

De los 2^{16} puertos se distinguen 2 bloques:

a) Puertos Bien Conocidos: Son los puertos que se usan más y que tienen mayor utilidad.

b) Puertos Libres: Cada usuario puede asignar para su uso personal.

5. Conexión.

En este contexto, TCP es un protocolo orientado a conexión, o sea, abre, mantiene y cierra una sesión.

Puerto Fuente		Puerto Destino	
Número de Secuencia			
Data offset	Reservado	Códigos de Bits	Ventana
Check Sum	Puntero de urgencia	Opciones	Relleno
Datos			

Tabla 1.2 Encabezado TCP.

Segmento TCP

Los componentes que integran el encabezado TCP son los siguientes:

a) Data Offset (desplazamiento de datos): Indica el tamaño del encabezado y donde empiezan los datos.

b) Puntero de Urgencia: Indica que datos son urgentes y hay que procesar primero.
c) Bandera:

- URI: Urgencia.
- ACK: Si está en nivel lógico alto es que está confirmado.
- EOL: Fin de carta.
- FPC.
- PSH.
- RST: Vuelve a empezar la sesión (se inicializa).
- SJN: Se utiliza al inicio de la sesión.
- FIN: Se inicia el proceso de cierre de sesión.

1.4.7.3 Protocolo UDP.

Significa Protocolo de Datagrama de Usuario. Su función es proveer de un medio de envío de mensajes entre aplicaciones. Diseñado para pequeños mensajes.

Características:

- Es un protocolo muy simple.
- No es confiable (no hay garantía de que llegue la información).
- Es un protocolo sin conexión (no inicia, ni mantiene ni cierra la sesión).
- Tiene un encabezado pequeño.
- No ordena ni reordena los datos.

Puerto Fuente	Puerto Destino
Largo	Check Sum
Datos	

Tabla 1.3 Encabezado UDP.

1.4.7.4 Protocolo IP

Significa Protocolo Internet.

Funciones:

- Rutear los datagramas hacia los equipo remotos, ya que se encuentran en la capa de red.
- Define su propio esquema de direccionamiento.
- Fragmenta y defragmenta los datagramas (en UDP se consideran como datagramas los paquetes de información).

Características:

- Es un protocolo sin conexión.
- Es un protocolo no confiable (no sabe si llega o no llega la información).

Definición del esquema de direccionamiento.

Es determinar cómo se identifican los equipos dentro de la red. Cada dirección en ethernet es de 32 bytes por lo que se pueden tener hasta exp48. Dichas direcciones se representan en hexadecimal. Arcnet usa 1 byte para direccionar. Las redes Token Ring usan 2 o 6 bytes. La dirección se encuentra en la tarjeta, dicha dirección es puesta por el fabricante. Estas direcciones se denominan físicas ya que trabajan a nivel físico del modelo OSI; también son llamadas direcciones MAC.

1.4.7.5 Protocolo ARP.

Sus siglas significan Protocolo de Resolución de Direcciones. Se encarga, en base a una dirección IP, cuál es la dirección física que le corresponde. Cuando a ARP le llega una solicitud para localizar una dirección física a partir de una dirección IP los pasos son los siguientes:

1. Busca en su tabla de ARP la dirección IP solicitada. Si la localiza lee cual es la dirección física que le corresponde y la manda como respuesta.

2. Una vez teniendo la dirección física se procesa el paquete y se envía al equipo.

3. Si no encuentra la dirección IP en su tabla se da a la tarea de localizar la dirección física de la dirección solicitada, para ello:

- ARP genera un mensaje de petición que se envía a la red mediante una señal Broadcast para que todos los equipos en la red la escuchen. Entre los parámetros que tiene este mensaje están: La dirección IP y física del equipo fuente y la dirección IP del equipo destino.

- Cuando el paquete está en la red le llega a todos los equipos y todos los procesan por ser un mensaje de broadcast.

- Al procesar el mensaje se dan cuenta que es una petición de ARP en la cual se solicita la dirección física de la dirección IP destino.

- Únicamente el quipo que tenga la dirección IP destino solicitada es la que va a responder generando un mensaje de respuesta de ARP. En este mensaje el equipo va a colocar su dirección física que es la solicitada, este mensaje es enviado a la máquina que lo solicitó cuando la máquina que envió el mensaje de solicitud le llega el mensaje de respuesta, lo analiza y guarda en la tabla de ARP la dirección IP y física del equipo destino de esta forma localiza la dirección física a partir de la dirección IP y cuando llegue otro mensaje para dicha dirección IP simplemente tomará la dirección física de la tabla de ARP. La tabla ARP es dinámica.

1.4.7.6 Protocolo ICMP

Significa Protocolo de Mensajes de Control de Internet. Se encuentra dentro de IP como una sub-rutina, pero trabaja como una capa superior a IP. Se usa para reportes de error y mensajes. El formato ICMP varía con respecto al mensaje pero el más usado es:

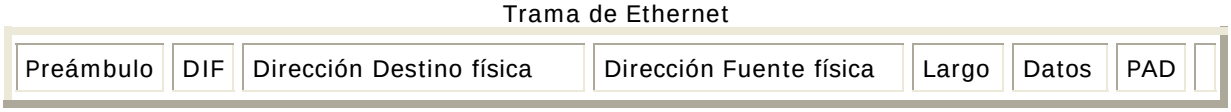
Tipo	Código	Check Sum
Sin usar		
Encabezado IP + 64 bits de datos del mensaje que ocasionó el error.		

Tabla 1.4 Formato ICMP.

1. Tipo: Aquí se aloja el motivo por el cual no se logró llegar al destino como pueden ser: De saturación, equipo inalcanzable, red inalcanzable, etc.

2. Código: Destino que no se alcanzó.

Trama de Ethernet



1. DIF: Delimitador de Inicio de Frame.

2. PAD: Relleno.

3. Largo: Parecido al Check Sum.

4. Preámbulo: Envía una señal a la tarjeta para no perder información.

1.4.7.7 Otros protocolos de red.

IPX/SPX

Internet Packet eXchange/Sequenced Packet eXchange. Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

DECnet

Es un protocolo de red propio de Digital Equipement Corporation (DEC), que se utiliza para las conexiones en red de los ordenadores y equipos de esta marca y sus compatibles. Está muy extendido en el mundo académico. Uno de sus componentes, LAT (Local Area Transport, transporte de área local), se utiliza para conectar periféricos por medio de la red y tiene una serie de características de gran utilidad como la asignación de nombres de servicio a periféricos o los servicios dedicados.

X.25

Es un protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

AppleTalk

Este protocolo está incluido en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo. Existen tres formas básicas de este protocolo:

- LocalTalk

Es la forma original del protocolo. La comunicación se realiza por uno de los puertos serie del equipo. La velocidad de transmisión no es muy rápida pero es adecuada para los servicios que en principio se requería de ella, principalmente compartir impresoras.

- Ethertalk

Es la versión de Appletalk sobre Ethernet. Esto aumenta la velocidad de transmisión y facilita aplicaciones como la transferencia de ficheros.

- Tokentalk

Es la versión de Appletalk para redes Token Ring.

- NetBEUI

NetBIOS Extended User Interface (Interfaz de usuario extendido para NetBIOS). Es la versión de Microsoft del NetBIOS (Network Basic Input/Output System, sistema básico de entrada/salida de red), que es el sistema de enlazar el software y el hardware de red en los PCs. Este protocolo es la base de la red de Microsoft Windows para Trabajo en Grupo.

1.4.7.8 Redes de transmisión FRAME RELAY

Es un protocolo para la transmisión de información que permite establecer redes nacionales para la interconexión internacional y a su vez establecer puntos alternos para una mayor seguridad en su red. El cliente puede programar canales permanentes, logrando tener una comunicación mediante un solo enlace a varios países para el intercambio de información corporativa.

Características:

- Diseñado para aplicaciones interactivas.
- Soporta tráfico en ráfagas por manejar multiplexación estadística.
- Optimiza el ancho de banda.
- Adaptable a nuevas tecnologías.
- Independencia del protocolo.
- Tecnología comprobada.

Beneficios:

- Optimización de recursos de Telecomunicaciones, se traduce en un menor costo para el operador y para el cliente.
- Facilidad en la administración.
- Disminución de la probabilidad de falla en los enlaces.
- Desarrollo continuo de nuevas opciones para el manejo de nuevas aplicaciones.
- Permite la interconexión de sistemas de cómputo y redes Lan a alta velocidad, sin tener que intervenir en equipos de conversión de protocolos e integrarlos con otros servicios de telecomunicaciones.
- Reducción de costos con respecto a líneas dedicadas, cuando se necesita la conexión de tres o más puntos. Por lo tanto, se disminuye el presupuesto de gastos con respecto a las comunicaciones corporativas.

- Transparencia en el transporte de los protocolos utilizados y por lo tanto agilidad en la implementación de proyectos.

- Posibilidad de concentración de varios puntos en un punto principal utilizando planta externa mínima, lo que se refleja en disminución de gastos en comunicaciones.

- Generación de estadísticas para el control y supervisión de gastos en cada punto de la red privada. Lo cual provee mayor inteligencia en la administración de la red.

Ventajas:

- Asignación del ancho de banda por demanda, Esto hace que la plataforma sea el medio idóneo para el transporte de información que se transmite por ráfagas como:

- Correo electrónico, transferencia de archivos, aplicaciones cliente/server, voz y video.

- Costos flexibles: Cuando se necesita la comunicación con muchos puntos, el costo resulta más beneficioso que el de adquirir una topología similar utilizando líneas dedicadas.

- Integración de aplicaciones: A través de Frame Relay se puede establecer un enlace físico entre dos o más puntos, utilizando diferentes rutas virtuales, cada uno de ellos con la capacidad de transportar diferentes protocolos.

- Ancho de Banda Garantizado: Al usuario se le asegura un ancho de banda mínimo.

- Estadísticas: De ser requerido por el cliente, Frame Relay es capaz de generar estadísticas para el control, y mejoramiento del ancho de banda utilizado.

- Transparencia al Protocolo: Frame Relay está diseñado para transportar sobre una misma plataforma, diferentes protocolos.

- Notificación de Congestión: La red puede notificar a los usuarios, con el fin de que el dispositivo del cliente disminuya su razón de transmisión de información, ya que esta experimentando problemas de congestión, y/o que otro usuario está excediendo su tráfico en la red.

1.4.8 Estándares y Normas IEEE de Redes

La IEEE ha creado una serie de estándares para el correcto uso de la redes a nivel mundial, estas están contempladas en la norma 802 de dicha institución. Los comités 802 del IEEE definen las normas sobre redes de área local. La mayoría de ellas se estableció en los años 80. Muchas de la normas 802 del IEEE son también normas 802 del ISO. Las normas 802 hacen referencia sobre todo a los niveles 1 y 2 según la pila del modelo OSI de la ISO, es decir Los niveles físicos y de enlace, tratan aspectos como el acceso de las tarjetas de red o Network Inteface Card (NIC) al medio físico, etc.

- 802.1: Norma IEEE que define la relación entre las normas 802 del IEEE y el modelo OSI.

- 802.1B: Norma del IEEE que define una arquitectura y protocolo de alto nivel para la gestión de LAN'S IEEE 802.

- 802.2: Norma IEEE que define el protocolo de control de enlaces lógicos LLC (Logical Link Control). En el modelo OSI de la ISO el nivel Dos o de enlace se divide en dos subniveles, el nivel de control de acceso al medio MAC (Media Access Control) y el LLC.
- 802.3: Norma IEEE para redes de tipo CSMA/CD.
- 802.3 U: Es una red 802.3 con autonegociación para la selección automática de velocidad.
- 802.4: Norma IEEE para redes en bus con Paso de Testigo (Token Bus).
- 802.5: Norma IEEE para redes en anillo con Paso de Testigo (Token Ring).
- 802.6: Norma IEEE para redes de área metropolitana (MAN).
- 802.7: Grupo Asesor del IEEE para técnicas de banda ancha.
- 802.8: Grupo Asesor del IEEE para técnicas de fibra óptica.
- 802.9: Grupo de trabajo del IEEE para la integración del tráfico de voz, datos y video en LANS 802 y en redes RDSI.
- 802.10: Grupo asesor del IEEE para técnicas de seguridad en la red.
- 802.11: Comité del IEEE que define normas para las redes inalámbricas.
- 802.12: Comité del IEEE que define la norma Ethernet a 100 Mbs con el método de acceso de prioridad bajo demanda propuesto por Hewlett Packard y otros fabricantes. Son redes 100 VG Anylan.

Los estándares más populares son:

- Ethernet
- Local Talk
- Token Ring
- FDDI

1.4.8.1 Ethernet

Ethernet es hoy en día el estándar para la redes de área local. Tanto Ethernet (Versión 2) como el muy similar estándar IEEE802.3 definen un modo de acceso múltiple y de detección de colisiones, es el conocido Carrier Sense Multiple Access/Collision Detection (CSMA/CD). Cuando una estación quiere acceder a la red escucha si hay alguna transmisión en curso y si no es así transmite. En el caso de que dos redes detecten probabilidad de emitir y emitan al mismo tiempo se producirá una colisión pero esto queda resuelto con los sensores de colisión que detectan esto y fuerzan una retransmisión de la información. Ethernet es generalmente disponible. Como la más nueva tecnología en la familia Ethernet, es relativamente costosa.

1.4.8.1.1 Tipos de Ethernet

Existen actualmente tres tipos de Ethernet, distinguidos por su velocidad de transmisión:

- Standard Ethernet: Transfiere datos a un máximo de 10 Mbps. Para un pequeño grupo de trabajo con necesidades de interconexión en red limitada (por ejemplo, impresión compartida y un pequeño bit de archivo compartido); standard Ethernet es una solución de interconexión en red bastante económica.
- Fast Ethernet: Transfiere datos a un máximo de 100 Mbps. Los costos son de dos a tres veces más que la standard Ethernet pero decrecen rápidamente.

- Gigabit Ethernet: Transfiere datos en un máximo de 1Gbps.

Tipo de Ethernet	Velocidad (Mbps)	Distancia (m)	Media
10Base5 (IEEE 802.3)	10	500	Coaxial Grueso
10Base2 (IEEE 802.3)	10	185	Coaxial Delgado
10BaseT (IEEE 802.3)	10	100	UTP
10BaseF(IEEE 802.3)	10	2000	Fibra Óptica

Tabla 1.5 Cableados y velocidades de transmisión.

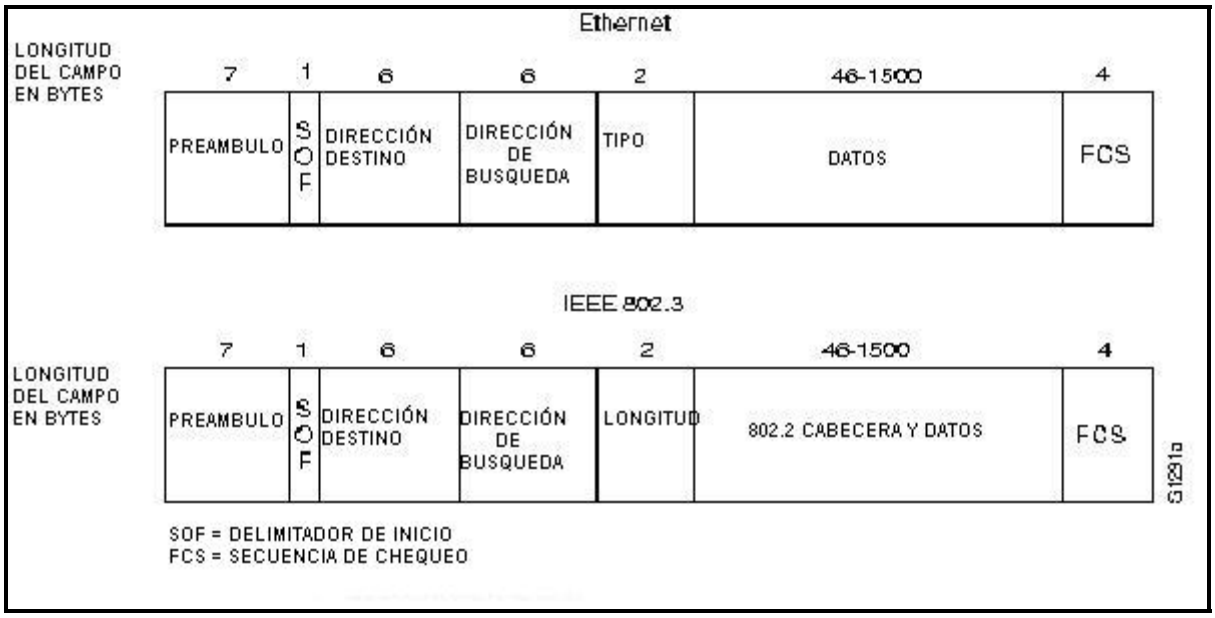


Tabla 1.6 Formatos de trama Ethernet IEEE 802.3

Ethernet define de qué manera se introducirán los datos en la red. Donde se indicará el receptor, el emisor donde irán los datos, donde irá el checksum, etc. Esto se define en la trama Ethernet. En la figura superior se puede ver la distribución de la información en cada paquete enviado. Se comienza con un preámbulo que termina al que sigue la trama en sí. El inicio de la trama es la información de la dirección de destino seguido de la dirección de procedencia a lo que sigue el tipo o la longitud de la información los datos y el checksum de la trama. El checksum (FCS) se comprueba en la llegada para asegurarse de la correcta recepción de la información.

Fast Ethernet

Para aumentar la velocidad de la red de 10Mbs a 100Mbs se han definido nuevos estándares de Ethernet denominados en conjunto FastEthernet (IEE802.3u).Tres nuevos tipos de redes Ethernet han visto la luz. Las topologías posibles quedan reducidas a la topología estrella.

Tipo de Ethernet	Velocidad (Mbps)	Media
100BaseTX (IEEE 802.3u)	100	UTP de categoría 5
100BaseFX (IEEE 802.3u)	100	Fibra óptica
100BaseT4 (IEEE 802.3u)	100	UTP de categoría 3 modificado *

Tabla 1.7 Estándares de Ethernet.

* Se añaden dos líneas al cable UTP de categoría 3.

Gigabit Ethernet

Gigabit Ethernet es una extensión a las normas de 10 Mbps y 100 Mbps IEEE 802.3; además del cable UTP categoría 6. Nos ofrece un ancho de banda de 1000 Mbps y mantiene compatibilidad completa con la base instalada de nodos Ethernet.

Gigabit Ethernet soporta nuevos nodos de operación Full-Dúplex para conexiones compartidas que usan repetidores y los métodos de acceso CSMA / CD.

Las implementaciones iniciales de Gigabit Ethernet emplearán cableados de fibra de gran velocidad, los componentes ópticos para la señalización sobre la fibra óptica.

1.4.8.2 LocalTalk

El protocolo LocalTalk fue desarrollado por Apple Computer, Inc. para ordenadores Macintosh. El método de acceso al medio es el CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Este método, similar al de Ethernet (CSMA/CD) se diferencia en que el ordenador anuncia su transmisión antes de realizarla. Mediante el uso de adaptadores LocalTalk y cables UTP especiales se puede crear una red de ordenadores Mac a través del puerto serie. El sistema operativo de estos establece relaciones punto a punto sin necesidad de software adicional aunque se puede crear una red cliente servidor con el software AppleShare.

Con el protocolo LocalTalk se pueden utilizar topologías bus, estrella o árbol usando cable UTP pero la velocidad de transmisión es muy inferior a la de Ethernet.

1.4.8.3 Token Ring

El protocolo Token Ring fue desarrollado por IBM a mediados de los 80. El modo de acceso al medio esta basado en el traspaso del testigo (token passing). En una red Token Ring los ordenadores se conectan formando un anillo. Un testigo (token) electrónico pasa de un ordenador a otro. Cuando se recibe este testigo se está en disposición de emitir datos. Estos viajan por el anillo hasta llegar a la estación receptora. Las redes Token Ring se montan sobre una topología estrella cableada (star-wired) con par trenzado o fibra óptica. Se puede transmitir información a 4 ó 16 Mbs. Cabe decir que el auge de Ethernet está causando un descenso cada vez mayor del uso de esta tecnología.

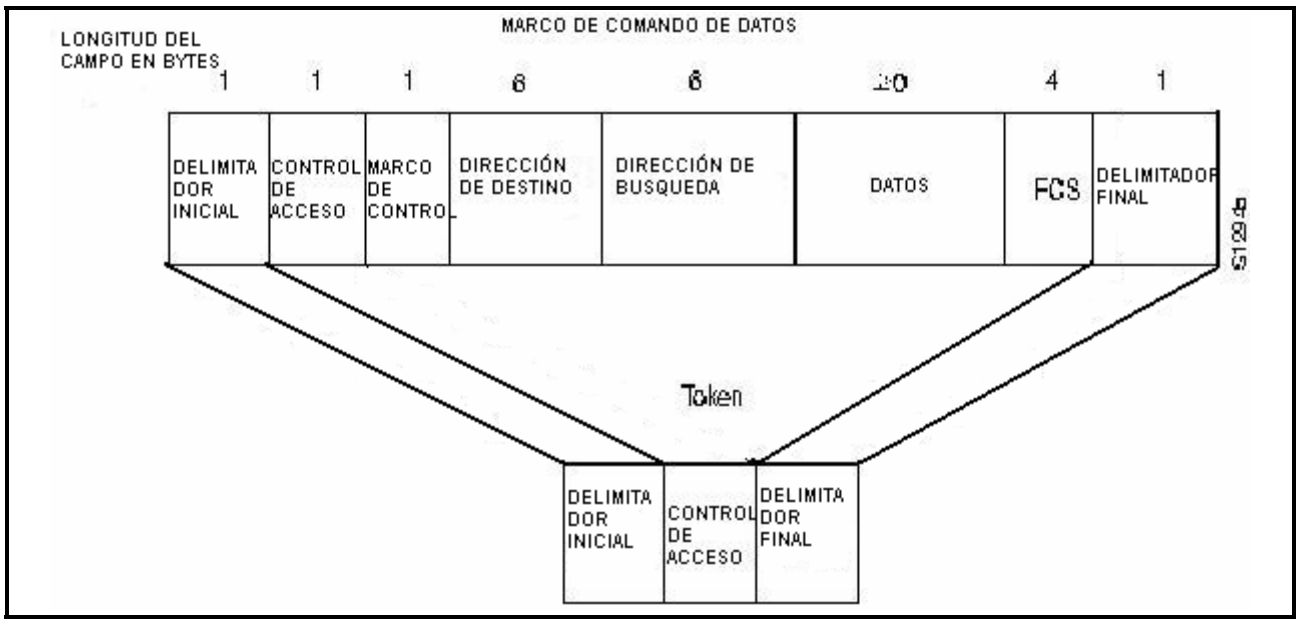


Fig. 1.5 Formatos de Trama en Token Ring.

Como se puede ver, la trama de Token Ring es similar a la de Ethernet, la principal diferencia consiste en que a los datos se le agrega un Token, que es el que marca la prioridad de transmisión.

1.4.8.4 FDDI

Este protocolo de red se utiliza principalmente para interconectar dos o más redes locales que con frecuencia distan grandes distancias.

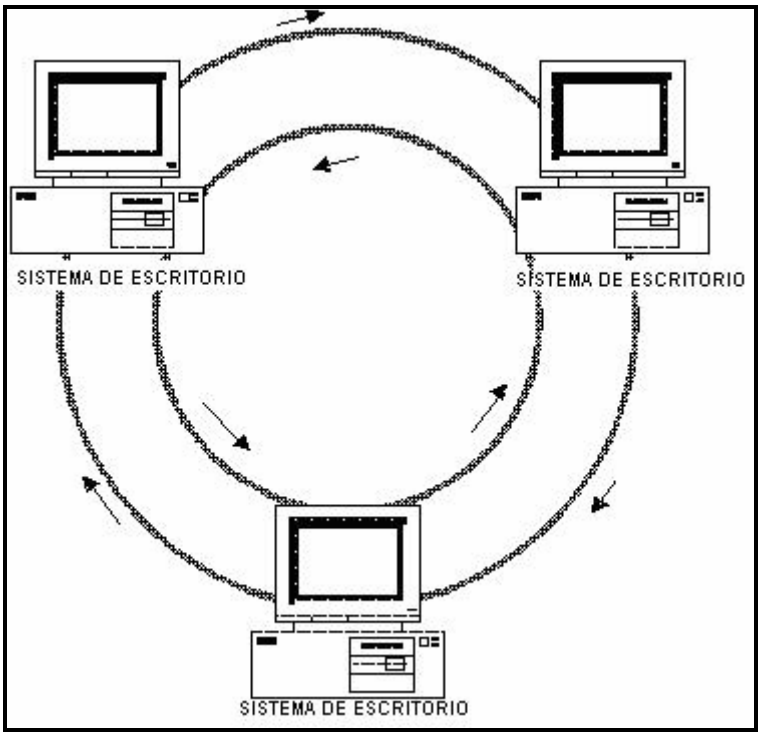


Figura 1.6 Fiber Distributed Data Interface.

El método de acceso al medio utilizado por FDDI está basado también en el paso de testigo. La diferencia es que en este tipo de redes la topología es de anillo dual. La transmisión se da en uno de los anillos pero si tiene lugar un error en la transmisión el sistema es capaz de utilizar una parte del segundo anillo para cerrar el anillo de transmisión. Se monta sobre cables de fibra óptica y se pueden alcanzar velocidades de 100 Mbps.

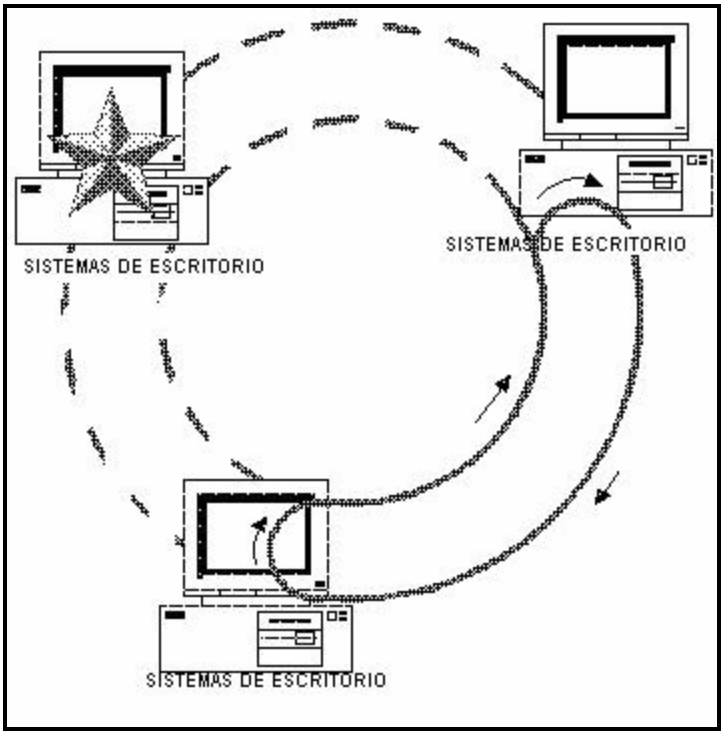


Figura 1.7 Topología FDDI.

En la siguiente tabla se muestra un resumen de los estándares anteriormente mencionados:

Estándar	Cable	Velocidad	Topología
Ethernet	Par trenzado, coaxial, fibra óptica	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Par trenzado, fibra óptica	100 Mbps	Star
Gigabit Ethernet	Par trenzado, fibra óptica	1000 Mbps	Star
Local Talk	Par trenzado	.23 Mbps	Linear Bus o Star
Token Ring	Par trenzado	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fibra óptica	100 Mbps	Anillo Duall Ring

Tabla 1.8 Estándares de Tecnologías.

1.4.8.5 RDSI: estándar universal

RDSI (o bien ISDN en inglés) permite la conexión de una amplia gama de terminales como teléfonos, computadoras, centrales PBX, etc., en donde la red proporciona una gran variedad de servicios entre los que se incluyen voz, datos e imágenes. La RDSI se presenta como la bandera de las redes RDI, aunque su oferta es diferente:

- Audio de 7 Khz de ancho de banda, en vez de los 3.1 Khz de la red telefónica actual.
- Canales digitales de 64 kbps de velocidad en vez de las que se alcanzan utilizando módems que difícilmente llegan a los 40 kbps.
- Mayor funcionalidad y servicios gracias al canal común de señalización.
- Un único y estandarizado método de acceso que da paso a toda una red de área extensa, con posibilidad de transferir información tanto en modo circuito como en modo paquete.

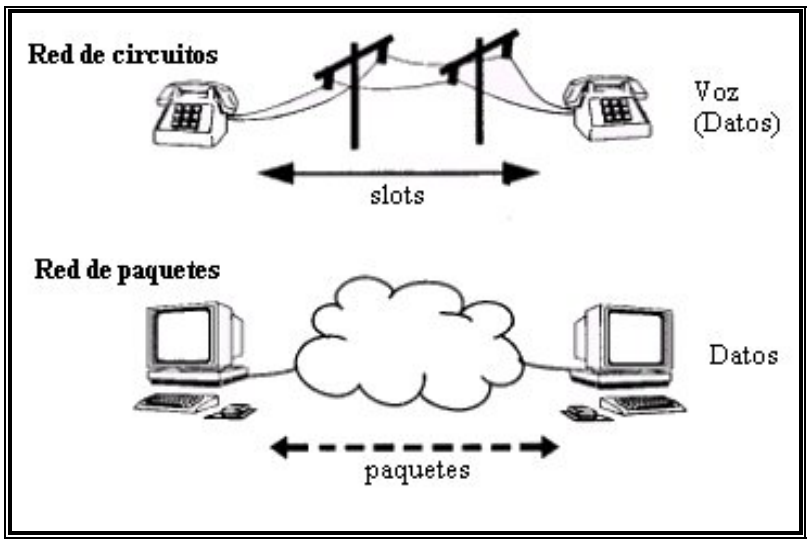


Figura 1.8 RDSI-BE

La RDSI-BE integra redes de circuitos y redes de paquetes permitiendo el soporte eficiente de voz, datos e imágenes en baja definición.

LA RDSI DE BANDA ESTRECHA (RDSI-BE)

Las comunicaciones se configuran como un conjunto de redes separadas:

- Red X.25 para datos.
- Redes de conmutación de circuitos para voz y datos.
- Redes para transmisión de la señal de TV.
- Redes de área local (LAN).
- Redes metropolitanas (MAN).

No existe una red universal donde podamos conectar indistintamente el teléfono, los terminales X.25, ni por supuesto un receptor de TV. Cada uno de estos dispositivos requiere

un tipo específico de servicio, contratado, instalado y gestionado por separado. La RDSI pretende ser la gran integradora de los servicios que hasta ahora proporcionaban las compañías telefónicas: desde la red conmutada para voz, redes de paquetes, hasta los enlaces digitales punto a punto, pasando por la mayoría de redes especializadas en dar un solo servicio. La integración de las LAN y circuitos de TV quedan como objetivo para una futura RDSI en banda ancha. En principio, la RDSI convivirá y permitirá la conectividad con el resto de redes públicas, aunque éstas progresivamente irán siendo integradas o sustituidas por la RDSI hasta llegar a constituirse en red única. Para permitir la interconexión de terminales actuales, que no soportan de forma nativa protocolos RDSI, se han diseñado los denominados Adaptadores de Terminal (TA). Los TA garantizan de esta forma la conexión de la mayoría de recursos de comunicaciones existentes sin necesidad de cambios notables.

1.4.8.6 Modo de Transferencia Asíncrono – ATM

ATM y la Red Óptica Sincronía (SONET) forman la base de la Red Digital de Servicios Integrados de Banda Ancha (B-ISDN), un nuevo estándar en desarrollo para la integración en red de: Datos, Voz, Imagen y Vídeo, a velocidades de transmisión desde 34 Mbps hasta 622 Mbps aproximadamente.Emplea el concepto de Conmutación de Celdas (Cell Switching), el cual combina los beneficios de la Conmutación de Paquetes tradicionalmente utilizada en redes de datos, y la Conmutación de Circuitos utilizada en redes de voz.
ATM se basa en el concepto de Conmutación Rápida de Paquetes (Fast Packet Switching) en el que se supone una fiabilidad muy alta a la tecnología de transmisión digital, típicamente sobre fibra óptica, y no necesita la recuperación de errores en cada nodo. Ya que no hay recuperación de errores, no son necesarios los contadores de número de secuencia de las redes de datos tradicionales, tampoco se utilizan direcciones de red ya que ATM es una tecnología orientada a conexión, en su lugar se utiliza el concepto de Identificador de Circuito o Conexión Virtual (VCI).

ATM ha sido definido para soportar de forma flexible, la conmutación y transmisión de tráfico multimedia comprendiendo datos, voz, imágenes y vídeo. En este sentido, ATM soporta servicios en modo circuito, similar a la conmutación de circuitos, y servicios en modo paquete, para datos (Fig. 1.9).

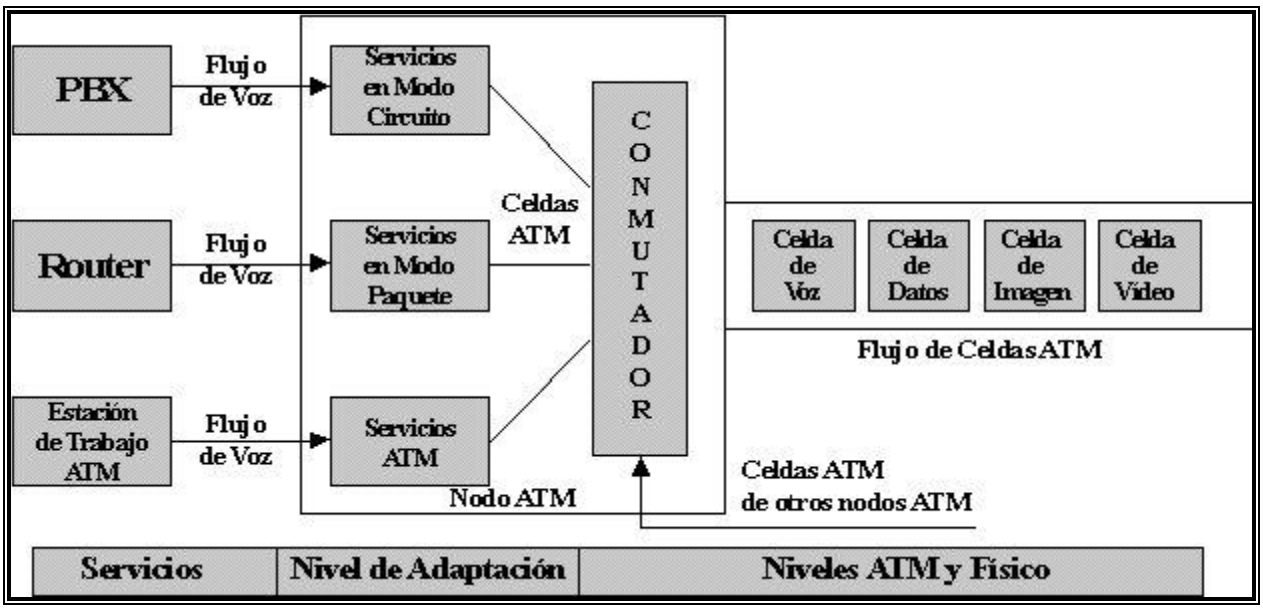


Figura 1.9 Funcionamiento de un Nodo ATM.

Sin embargo, a diferencia de la conmutación de circuitos, ATM no reserva "slots" para la conexión. En su lugar, una conexión obtiene "slots" o celdas, sólo cuando está transmitiendo información. Cuando una conexión está en silencio no utiliza "slots" o celdas, estando estas disponibles para otras conexiones.

En una red ATM, donde las celdas no están reservadas sino asignadas bajo demanda, el conmutador receptor no puede determinar por adelantado a que canal corresponde cada celda. La Celda ATM a diferencia del Time Slot en STM, debe transportar la identificación de la conexión a la que pertenece, de esta forma no existirán Celdas vacías ya que serán utilizadas por conexiones pendientes. Esta es una diferencia fundamental del ATM frente al STM. La cabecera presente en cada celda, consume aproximadamente un 9.5% del ancho de banda, siendo este el precio que hay que pagar por la capacidad para disponer de ancho de banda bajo demanda, en lugar de tenerlo permanentemente reservado y eventualmente desperdiciado.

1.4.9 Dispositivos de Interconexión de Redes

En este apartado se analizan los diferentes tipos de dispositivos de interconexión de redes, que se pueden dividir genéricamente en cuatro categorías: repetidores, bridges (puentes), routers (ruteadores) y gateways (compuertas). Cada uno de los cuales está asociado a uno o varios de los niveles OSI. Los repetidores están asociados al Nivel 1 (nivel físico), los bridges al Nivel 2 (nivel de enlace), los routers o encaminadores al Nivel 3 (nivel de red) y los gateways o convertidores de protocolos a los niveles superiores (Transporte, sesión, presentación y aplicación).

1.4.9.1 Repetidor

Es un dispositivo que regenera la señal de una red y la retransmite. Operan en el nivel más bajo del modelo OSI. Se emplean para ampliar la cobertura de una red, conectando dos o más LAN's. El número de repetidores depende de la red. Se usan para redes del mismo tipo, con igual protocolo, medio de acceso, y topología. Operan amplificando todas las señales eléctricas que reciben, es decir son transparentes hasta los protocolos más altos. No proporciona ningún tipo de aislamiento entre redes. Sólo pueden proporcionar una gestión de redes simple. Es extremadamente rápido ya que no analiza la señal sólo la toma y la regenera; por lo que es el dispositivo menos inteligente. Es transparente para la red: A nivel de software no se da uno cuenta de que existe, solo físicamente. Toda la red sabe de la existencia de la señal, solo que la procesa a quien va dirigida. Se puede poner en cualquier parte de la red.

Su mayor ventaja es poder conectar redes con diferente medio de transmisión como por ejemplo ethernet sobre cable coaxial a ethernet sobre fibra óptica. Más que repetidores lo que se suele utilizar son regeneradores que no solo amplifican, que supone amplificar la señal con el ruido adicional, sino que devuelven la señal digital original eliminando el ruido.

1.4.9.2 Bridges (Puentes)

Un bridge es un dispositivo usado para interconectar redes de área local (LAN).Es un dispositivo que hace la misma función que el repetidor, pero lo hace mejor. A diferencia del repetidor, el puente es más inteligente ya que determina a que computadora va y determina si pasa o no pasa la señal. Es más lento que el repetidor. El puente puede cambiar de método de acceso, o sea, si se unen 2 redes con igual protocolo y diferente método de acceso (reglas para poner la información en el medio de transmisión). Generalmente se usa para dividir una red de gran tráfico en 2 de menor tráfico. Los bridges reciben todos los paquetes enviados por cada red acoplada a él, y los reenvían selectivamente entre las LAN's,

utilizando solo las direcciones del nivel 2 (de enlace) para determinar donde retransmitir cada paquete. Los bridges reenvían solo aquellos paquetes que están destinados a un nodo del otro lado del bridge, descartando (filtrando) aquellos que no necesitan ser retransmitidos.

Los bridges locales conectan LAN's las cuales no están colocadas en sitios diferentes. Por ejemplo aquellas que son adyacentes a lo largo de su longitud. Los bridges locales permiten a un edificio grande o un campus compacto tener una única red "lógica" más larga que la que podría ser con un solo segmento de cable y proporciona algún aislamiento eléctrico y de tráfico entre segmentos.

Los bridges remotos conectan LAN's de lugares distantes. Estos bridges se usan en pares; cada bridge remoto se conecta a una LAN y a otro bridge remoto mediante un enlace remoto. Como los bridges no necesitan tener enlaces con la misma velocidad en ambos lados, pueden ser utilizados para interconectar LAN's vía enlaces de telecomunicaciones de baja velocidad.

La mayoría de los bridges actuales son capaces de aprender automáticamente la topología de la red (learning bridges), examinando cada paquete que reciben anotando la dirección fuente de tales paquetes. Cualquier dirección fuente que el bridge no haya visto antes será almacenada en su tabla interna para referencias futuras. Cuando un bridge recibe de un nodo un paquete que tiene una dirección destino desconocida, envía el paquete a todas los otros puertos para asegurar que el paquete alcanzará su destino. A notar que en el futuro cualquier paquete recibido con ese nodo como destino, el bridge conocerá su localización. Los bridges proporcionan mejoras de tráfico y aislamiento que los repetidores entre segmentos de LAN, pero introducen algún retardo. También son más fáciles de instalar y manejar que los routers, pero no dan el alto grado de aislamiento de tráfico entre LAN de estos.

1.4.9.2.1 Bridges Multipuerto

Los bridges multipuerto son bridges con tres o más interfaces de enlace de datos o puertos. Se utilizan para conectar más de dos LAN en un único punto. Como resultado del mayor número de puertos y mejores prestaciones, un único bridge multipuerto puede ser usado para reemplazar varios bridges de dos puertos conectados conjuntamente por medio de segmentos o troncales de LAN. El bridge multipuerto también proporciona mejores prestaciones debido a que los paquetes son conmutados de una LAN a otra sobre su bus Entrada/Salida o su memoria, los cuales son mucho más rápidos que los segmentos de LAN. La operación de los bridges multipuerto es superior en el sentido de filtrar y reenviar paquetes, con la excepción de que la determinación de adonde deben ser enviados tales paquetes es más compleja.

1.4.9.3 Router (Ruteador)

Hace las funciones de un puente con la decisión de pasar o no pasar, cambio de método de acceso, mismo protocolo, etc. Además es más inteligente, si va a pasar la información determina el mejor camino para llegar a su destino. Entre ruteadores hay: El mismo protocolo de ruteo, tablas de ruteo (tabla que contiene la información de los ruteadores conectados a un ruteador). Hay protocolos de dominio público. Un ruteador podría soportar varios protocolos.

Debido al gran empuje que tienen hoy en día las tecnologías de hubs y conmutadores ATM, que ofrecen una alta variedad de prestaciones, los fabricantes de routers se están viendo

obligados a ampliar a marchas forzadas el horizonte de sus productos. De hecho la gran mayoría se apresta a abrazar ATM al tiempo que continua mejorando el rendimiento de sus soluciones mediante avances tan significativos como las arquitecturas multiproceso. Estas mejoras se producen justo en un momento en que los analistas predicen un futuro punto de convergencia entre los conmutadores ATM, los routers y los hubs inteligentes. La fusión entre Wellfleet y SynOptics constituye un ejemplo claro, aunque no el único de esta tendencia.

La elección de un ruteador determinado ha de tener en cuenta aspectos como la escalabilidad y flexibilidad para añadir interfaces LAN o WAN. Los fabricantes están lanzando una nueva generación de tarjetas de interfaz de alta velocidad, tanto para soportar conexiones LAN ATM como servicios WAN ATM. Otras nuevas interfaces proporcionan conexiones WAN de SMDS (Switched Multimegabit Data Service), Fast Ethernet y FDDI sobre par trenzado.

El ruteador tradicional incluye tres componentes clave: tarjetas de red, procesador de control y backplane (panel dorsal). Las tarjetas de red soportan protocolos e interfaces de LAN's y WAN's, mientras que el procesador de control efectúa cálculos de ruta y actualizaciones de topología. El backplane, finalmente, constituye el tejido de conmutación del equipo, proporciona el camino que han de seguir los datos y opera a la misma velocidad al menos que el cable de la red.

Tres son las funciones de tolerancia a fallos más importantes que han de ofrecer los ruteadores: redundancia a componentes críticos, capacidad de explorar rápidamente esa redundancia y reparación de fallos "en caliente". Una prestación importante en ese sentido es la conexión WAN redundante.

Tan importante como la tolerancia a fallos es el throughput (capacidad de procesamiento), cuya evaluación es una de las tareas más duras a la hora de seleccionar equipos. A pesar de los grandes pasos dados para desarrollar pruebas estándar, todavía algunos fabricantes sorprenden al usuario garantizando dudosos ratios de paquetes por segundo que, en los casos más llamativos, incluso superan los límites teóricos.

1.4.9.4 Bridge/Routers (Ruteadores) o Brouters

Aunque los ruteadores actuales son multiprotocolo, lo cual permite el encaminamiento sobre diferentes redes dentro de un único sistema, entre los diferentes niveles superiores de cada pila de protocolos puede haber alguno que sea desconocido para el router. En estos casos se requeriría colocar un bridge que no se ocupa de los protocolos de alto nivel, que es lo que se utiliza para protocolos no encaminables. Pero existe otra solución que es el bruouter.

Como sugiere el nombre, un bruoter (bridge/ruteador) es un sistema que combina simultáneamente las funciones de bridge y router, y que elige "la mejor solución de los dos". Brouters trabajan como router con los protocolos encaminables y como bridge con los que no lo son. Tratan estas funciones independientemente y proporcionan soporte de hardware para ambos.

Ventajas e Inconvenientes de los Bridge/Routers

Brouters ofrecen todas las ventajas de los routers para protocolos de router, y todas aquellas de los bridges para protocolos de bridge. Pensando que ellos son los sistemas más complejos de instalar, proporcionan el más alto grado de flexibilidad, lo que los hace ideales para rápidos cambios o expansiones de la red.

1.4.9.5 Gateways (Compuertas)

Los gateways -el sistema de interconexión de redes más complejo- funciona en los tres niveles más altos del modelo OSI (sesión, presentación y aplicación). Los gateways pueden conectar redes de arquitecturas (pila de protocolos) completamente diferentes. Para hacer esto, los gateways convierten una arquitectura de red en otra sin afectar a los datos transmitidos.

Los gateways proporcionan muchos servicios de gestión de red y al igual que bridges y routers (ruteadores) conectan tanto redes locales o redes extensas.

1.4.9.6 Transceivers

Permite una conexión rápida y fácil entre el cableado de red local y el puerto de AUI del dispositivo de sistemas o de red. Envían y reciben información, detecta coalisiones en la red, y protege la confiabilidad de redes monitoreando problemas de un mal funcionamiento entre el AUI y el Transceivers para una máxima flexibilidad; los transceivers son compatibles tanto con IEE 802.3, como con protocolos de Ethernet y son transparentes para los sistemas operativos de red. Cuentan con unos leds que proveen una evaluación visual rápida de la condición de la red.

1.4.9.7 Periféricos

Los periféricos fueron creados para que la computadora pueda interactuar y comunicarse con el mundo externo y también con otras computadoras. El teclado es la puerta de entrada de la computadora, a través de la cual se ingresan los datos necesarios para su funcionamiento. Los discos (rígido y flexible) son utilizados para almacenar todo lo que sea necesario, desde programas hasta los datos resultantes del procesamiento de la información. El monitor y la impresora nos permiten visualizar los resultados del procesamiento.

1.4.9.8 Las tarjetas

La tarjeta madre (o motherboard) de una computadora está compuesta por ranuras de expansión, que son simples conectores que posibilitarán la expansión de la capacidad de la computadora. Un tipo de tarjeta muy conocido es la de fax / módem. Con ésta es posible enviar y recibir mensajes de fax a través de una línea telefónica; conectarse con otra computadora para el intercambio de datos y la conexión con cualquier tipo de red, como Internet, Intranet y Extranet. Otro tipo de tarjeta muy utilizado es la de sonido, que compone los kits multimedia tan comunes y que permite al microprocesador transformar constantemente la información de muchas aplicaciones en sonidos estéreo.

Si una computadora tiene como función principal el desarrollo de diseños de alta definición, probablemente contará con el auxilio de una tarjeta aceleradora de video y de un escáner, otro dispositivo de entrada de información, una especie de lector de imágenes que funciona como una copiadora pero con la diferencia de que permite registrar y guardar la información a la que se ha accedido.

Tarjeta de Comunicación

Cuando sea necesario interconectar una computadora en red, habrá que contar con un componente adicional: una tarjeta de comunicación. Existen varias tarjetas de este tipo. Una de ellas es la tarjeta fax / módem. Cuando conectamos una computadora por medio de la

línea telefónica con un proveedor de acceso a Internet y utilizamos la red, literalmente establecemos una interconexión con millones de computadoras diferentes. Entramos en lo que se ha dado en llamar "La gran red".

Tarjetas de red

La tarjeta de red o NIC es la que conecta físicamente el ordenador a la red. Las tarjetas de red más populares son por supuesto las tarjetas Ethernet, existen también conectores Local Talk así como tarjetas TokenRing.

Tipos de tarjetas

Tarjeta Ethernet con Conectores Rj-45

Los conectores LocalTalk se utilizan para computadoras Mac, conectándose al puerto paralelo. En comparación con Ethernet la velocidad es muy baja, de 230KB frente a los 10 ó 100 MB de la primera. Las tarjetas de Token Ring, son similares a las tarjetas Ethernet aunque el conector es diferente, por lo general es un DIM de nueve pines.

Otras tarjetas

En una red con alcance local dentro de un mismo espacio físico, por lo general se emplea una tarjeta de comunicación conectada con otras computadoras utilizando un cable. Este tipo de tarjeta permite alcanzar una gran velocidad de transmisión y es más conocida como tarjeta de red. Las tarjetas de red más usadas para las comunicaciones locales son las que utilizan la tecnología de Ethernet y Token Ring.

Cables de conexión

Las tarjetas de red utilizan un cable especial para conectar una computadora con otra. Dentro de las opciones más utilizadas se encuentran el cable coaxial y el cable de pares trenzados. Con el cable coaxial es posible interconectar una computadora con otra. La red, desde el punto de vista del cable, tiene un inicio y un fin definidos.
El cable parte de un inicio preestablecido y pasa por todas las computadoras hasta llegar a la otra punta. Existen algunas reglas básicas que definen la cantidad de computadoras que puede estar conectadas, el tamaño máximo del cable coaxial y la manera en que se lo puede ampliar.

1.4.9.9 Concentradores (Hubs)

Existen concentradores con diversas capacidades. Los más básicos pueden conectar hasta ocho computadoras, es decir, tienen ocho puertos de comunicación desde donde es posible "colgar" hasta ocho computadoras utilizando el cable UTP de dos pares. Los concentradores más utilizados en instalaciones de medio y gran porte pueden soportar hasta 24 conexiones. Existe también la posibilidad de interconectar un concentrador con otro, ampliando la cantidad máxima de computadoras en la red.

1.4.9.10 Servidores

Los servidores de archivos conforman el corazón de la mayoría de las redes. Se trata de computadoras con mucha memoria RAM, un enorme disco duro o varios y una rápida tarjeta de red. El sistema operativo de red se ejecuta sobre estos servidores así como las aplicaciones compartidas.

Un servidor de impresión se encargará de controlar el trafico de red ya que este es el que accede a las demandas de las estaciones de trabajo y el que les proporcione los servicios que pidan las impresoras, archivos, Internet, etc. Es preciso contar con un ordenador con capacidad de guardar información de forma muy rápida y de compartirla con la misma rapidez.

1.4.9.11 Estaciones de trabajo

Son las computadoras conectadas al servidor. Las estaciones de trabajo no han de ser tan potentes como el servidor, simplemente necesita una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor. Una estación de trabajo puede carecer de unidad de disco flexible y de disco duro y trabajar directamente sobre el servidor. Prácticamente cualquier ordenador puede actuar como estación de trabajo.

1.5 Antecedentes de Windows NT, Windows 2000 y Windows 2003

1.5.1 Windows NT (Windows New Technology).

Es un sistema operativo de 32 bits desarrollado originalmente para que sea OS/2 3.0 antes que Microsoft e IBM discontinuaran su trabajo con OS/2. NT se diseñó para estaciones de trabajo avanzadas (Windows NT 3.1) y para servidores (Windows NT 3.1 Advanced Server).

Está basado en un microkernel, con un direccionamiento de hasta 4GB de RAM, soporte para sistemas de archivos FAT, NTFS y HPFS, soporte de red incorporado, soporte multiprocesador, y seguridad C2

NT está diseñado para ser independiente del hardware. Una vez que la parte específica de la máquina - la capa HAL (Capa de Abstracción de Hardware)- ha sido llevada a una máquina en particular, el resto del sistema operativo deberá compilar teóricamente sin alteración. Se lanzó una versión de NT para correr en máquinas Alpha de DEC. NT y necesita un 386, con al menos 12MB de RAM (preferible 16MB), y al menos 75MB de disco duro libre.

Windows NT 4**:** La nueva versión de Windows NT, denominada "Cairo" en su etapa de desarrollo. Presenta las mismas características de la interfaz de Windows 95. Tiene algunas modificaciones en su diseño con respecto a las porciones GDI y USER del sistema operativo.

Windows NT presenta una arquitectura del tipo cliente-servidor. Los programas de aplicación son contemplados por el sistema operativo como si fueran clientes a los que hay que servir, y para lo cual viene equipado con distintas entidades servidoras.

Uno de los objetivos fundamentales de diseño fue el tener un núcleo tan pequeño como fuera posible, en el que estuvieran integrados módulos que dieran respuesta a aquellas llamadas al sistema que necesariamente se tuvieran que ejecutar en modo privilegiado (también llamado modo kernel, modo núcleo y modo supervisor). El resto de las llamadas se expulsarían del núcleo hacia otras entidades que se ejecutarían en modo no privilegiado (modo usuario), y de esta manera el núcleo resultaría una base compacta, robusta y estable. Por eso se dice que Windows NT es un sistema operativo basado en micro-kernel.

Es por ello que en un primer acercamiento a la arquitectura distinguimos un núcleo que se ejecuta en modo privilegiado, y se denomina Executive, y unos módulos que se ejecutan en modo no privilegiado, llamados subsistemas protegidos.

Los programas de usuario (también llamados programas de aplicación) interaccionan con cualquier sistema operativo (SO) a través de un juego de llamadas al sistema, que es particular de cada SO. En el mundo Windows en general, las llamadas al sistema se denominan API (Application Programming Interfaces, interfaces para la programación de aplicaciones). En Windows NT y en Windows 95 se usa una versión del API llamada API Win32. Un programa escrito para Windows NT o Windows 95, y que por consiguiente hace uso del API Win32, se denomina genéricamente "programa Win32", y de hecho esta denominación es bastante frecuente en artículos y libros al respecto. Desgraciadamente, y conviene dejarlo claro cuanto antes, el término "Win32" tiene tres acepciones (al menos hasta ahora) totalmente distintas. Una es el API, otra es el nombre de uno de los subsistemas protegidos de Windows NT, y por último se denomina Win32s a una plataforma desarrollada por Microsoft, similar a Windows 3.1, pero que usa el API Win32 en vez del API Win16 del Windows 3.1.

Hechas estas aclaraciones, podemos continuar adelante. Algunas de las llamadas al sistema, debido a su naturaleza, son atendidas directamente por el Executive, mientras que otras son desviadas hacia algún subsistema. Esto lo veremos con detalle en breve.

El hecho de disponer de un núcleo rodeado de subsistemas que se ejecutan en modo usuario nos permite además añadir nuevos subsistemas sin producir ningún tipo de confrontación.

En el diseño de Windows NT han confluido aportaciones de tres modelos: el modelo cliente-servidor, el modelo de objetos, y el modelo de multiprocesamiento simétrico.

Modelo cliente-servidor. En la teoría de este modelo se establece un kernel que básicamente se encarga de recibir peticiones de procesos clientes y pasárselas a otros procesos servidores, ambos clientes y servidores ejecutándose en modo usuario. Windows NT pone el modelo en práctica pero no contempla el núcleo como un mero transportador de mensajes, sino que introduce en él aquellos servicios que sólo pueden ser ejecutados en modo kernel. El resto de servicios los asciende hacia subsistemas servidores que se ejecutan en modo usuario, independientes entre sí, y que por tanto pueden repartirse entre máquinas distintas, dando así soporte a un sistema distribuido (de hecho, el soportar los sistemas distribuidos fue otra de las grandes directivas de diseño de este SO).

Modelo de objetos. Decir que no implementa puramente la teoría de este modelo, sino que más bien lo que hace es simplemente contemplar los recursos (tanto internos como externos) como objetos. Brevemente, señalaremos que todo objeto ha de poseer identidad propia (es único y distinguible de todos los demás), y una serie de atributos (variables) y métodos (funciones) que modifican sus atributos. Los objetos interaccionan entre sí a través del envío de mensajes. No sólo existen en Windows NT objetos software (lógicos), sino que los dispositivos hardware (físicos) también son tratados como objetos (a diferencia de UNIX, que recordemos trataba a los dispositivos como ficheros).

Modelo de multiprocesamiento simétrico. Un SO multiproceso (o sea, aquel que cuenta con varias CPU y cada una puede estar ejecutando un proceso) puede ser simétrico (SMP) o asimétrico (ASMP). En los sistemas operativos SMP (entre los que se encuentran Windows NT y muchas versiones de UNIX) cualquier CPU puede ejecutar cualquier proceso, ya sea del SO o no, mientras que en los ASMP se elige una CPU para uso exclusivo del SO y el resto de CPU quedan para ejecutar programas de usuario. Los sistemas SMP son más complejos que los ASMP, contemplan un mejor balance de la carga y son más tolerantes a fallos (de manera que si un subproceso del SO falla, el SO no se caerá pues podrá ejecutarse sobre otra CPU, cosa que en los ASMP no sería posible, con lo que se bloquearía el sistema entero).

Comencemos describiendo los subsistemas protegidos, para seguidamente estudiar la estructura del Executive.

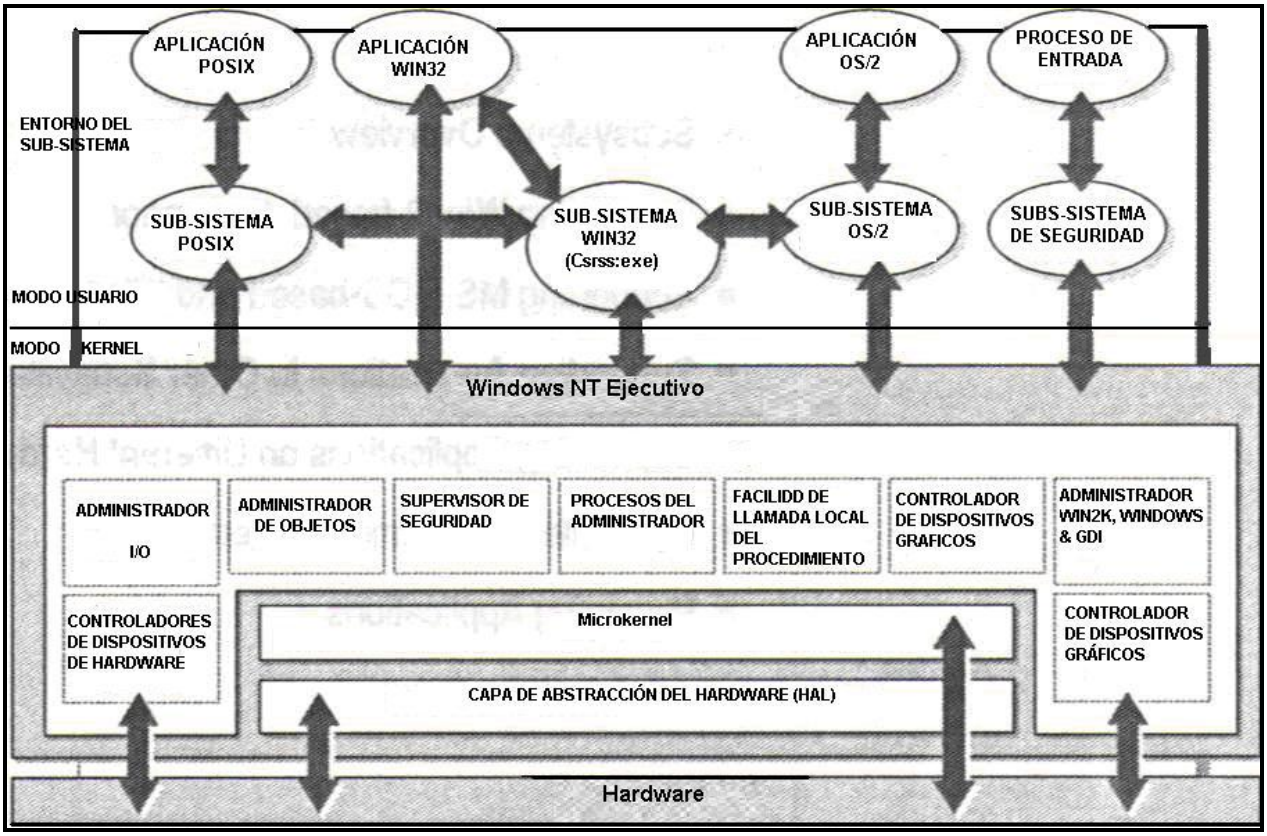


Figura 1.10 El núcleo se ejecuta en modo privilegiado (Executive) y en modo no privilegiado (subsistemas).

1.5.2 Windows 2000

Windows 2000 es un sistema operativo distinto a Windows 9x y Windows NT. Se sabia que Windows NT 5.0 estaba en proyecto, pero Windows 2000 llegó a resolver las dudas que se tenían, es la nueva versión de Windows NT 4.0 WorkStation y NT Server, pero también incorpora la sencillez de manejo de la serie 9x. Dicho en otras palabras, Windows 2000 ofrece lo mejor de ambos mundos: la solidez y la seguridad de NT, junto a la facilidad de manejo, soporte de hardware y multimedia de Windows 98.

La familia Windows 2000 está integrada por cuatro versiones:

- Windows 2000 Professional: Windows 2000 Pro, sucesor de NT Worksta-tion, está destinado a ser un cliente de red seguro y una estación de trabajo corporativa. Soporta hasta 2 procesadores y es útil, como sistema operativo autónomo, para correr aplicaciones de alta performance, especialmente en diseño gráfico, por ejemplo. Microsoft lo promociona como el principal sistema operativo de escritorio en un entorno de negocios.

- Windows 2000 Server: sucesor de NT Server, soporta hasta 4 procesadores y está destinado a ser el servidor de impresión, archivos, aplicaciones e, incluso, Web de una empresa pequeña a mediana.

- Windows 2000 Advanced Server: sucesor de NT Server Enterprise Edition, soporta hasta 8 procesadores y será el servidor departamental de aplicaciones en empresas medianas a grandes, con más de un dominio y tareas de misión crítica. Entre otras prestaciones, se incluye soporte para RAID y fault tolerance.

- Windows 2000 Data Center Server: soporta hasta 32 procesadores y sólo se entregará sobre pedido. Está destinado a grandes empresas que requieran data warehousing, análisis econométricos, simulaciones cientificas e ingenieriles a gran escala, etc.

Los requisitos del Hardware

Los requerimientos mínimos para Windows 2000 Professional son:

Pentium 166 MHz, 64 Mb de RAM y 2Gb de disco duro. Con espacio libre de al menos, 1 Gb.

Estas son algunas características para que el sistema W2000 Professional pueda funcionar. Las versiones Server y Advanced Server requieren procesadores más potentes y más RAM (al menos 256 Mb). En resumen, se recomienda que si deseas instalar W2000 y obtener un nivel aceptable de rendimiento (sobre todo para las versiones Server) optes por una máquina Pentium III 500 Mhz con 256 Mb de RAM como mínimo.

La confiabilidad del sistema.

La fiabilidad y la capacidad de gestión han mejorado con herramientas que ayudan a los usuarios y administradores de red a gestionar de forma más sencilla sus sistemas, empezando porque el laberinto de las DLLs parece resuelto. Windows 2000 permite que las DLLs (Dymanic Link Libraries) se instalen en los directorios de sus aplicaciones específicas, y eviten que se eliminen las DLLs compartidas.

La seguridad con la infraestructura.

Puesto que se trata de un sistema operativo orientado al trabajo en red y a la compartición de recursos, la familia Windows 2000 ha integrado sólidas tecnologías de seguridad. La intención es que cada usuario pueda comprender como funcionan estas tecnologías y controlarlas de forma cabal. Esta "infraestructura" de seguridad funciona en tres niveles:

- Local. Se refiere a la protección de datos en el ordenador. El sistema esta diseñado para evitar que usuarios no autorizados se "salten" el sistema de arranque y, por tanto, también las funciones de seguridad. Algunos fabricantes de hardware integran sistemas de "contraseña", una solución no muy adecuada para entornos de trabajo compartido. La encriptación de los datos en el disco NTFS es un servicio que se basa en la arquitectura CriptoAPI de Windows para implementar el sistema de llaves públicas. Cada archivo (incluyendo sus temporales de trabajo) se encripta a través de una llave generada aleatoriamente, utilizando algoritmos asimétricos. W2000 es el primer sistema operativo que implementa encriptación de 128 bits en un proceso transparente, ya que ENF encripta y desencripta los archivos localizando las llaves del usuario, bien desde el almacén del sistema o desde los dispositivos como los Smart Cards.

- Corporativo. Se refiere a la protección de datos en una red local. W2000 utiliza el protocolo de autentificación Kerberos versión 5, un estándar de seguridad en redes locales e intranets que verifica y hace un seguimiento de la actividad de cada usuario dentro de la red. Kerberos permite un control del acceso unificado a casi cualquier

entorno de red, eliminando la necesidad de obtener permisos y esperar la respuesta cada vez que un cliente desea acceder a un nuevo recurso de la red.

- Publico. W2000 utiliza también sistemas de llaves públicas y protocolos de autenticación para mantener la seguridad de las comunicaciones que se realizan por Internet, de forma que verifique la procedencia de mensajes de correo o garantice las fuentes de donde proceden las descargas. Por otra parte, incluye soporte para redes privadas virtuales (VPN), protocolos encapsulados que crean un "canal" de comunicación privado a través de redes públicas. El soporte VPN se realiza a través del protocolo PPTP (Point to Point Tunneling Protocol), Layer 2 Tunneling Protocol e IPSec, un protocolo que implementa una gama de funciones sobre una capa de red encriptada.

1.5.3 Windows 2003

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida.

• Está construido sobre la robustez y fiabilidad de Microsoft Windows 2000 Server.

• Las características mejoradas del Directorio Activo permiten realizar tareas más fácilmente, entre las que destacan la habilidad de renombrar dominios, la posibilidad de redefinir el esquema y una replicación más eficiente.

• Mayor disponibilidad a través del Windows System Resource Manager, de las actualizaciones del sistema automáticas y gracias a un servidor cuyos parámetros le confieren la máxima seguridad por defecto.

• Ofrece la mejor conectividad, facilitando al máximo la configuración de enlaces entre delegaciones, acceso inalámbrico seguro y acceso remoto a aplicaciones a través de los Terminal Services, así como en su integración mejorada con dispositivos y aplicaciones.

• Combinado con Visual Studio .NET 2003, se convierte en la plataforma más productiva para implementar, ejecutar y gestionar aplicaciones conectadas mediante la nueva generación de servicios Web basados en XML.

Ediciones Microsoft Windows Server 2003

- Microsoft Windows Server 2003 Standard Edition.
- Microsoft Windows Server 2003 Enterprise Edition.
- Microsoft Windows Server 2003 Datacenter Edition.
- Microsoft Windows Server 2003 Web Edition.

Seguro

Windows Server 2003 cuenta con la fiabilidad, disponibilidad, escalabilidad y seguridad que lo hace una plataforma altamente segura.

Disponibilidad. Windows Server 2003 ofrece una disponibilidad mejorada de soporte a clustering. Los servicios de clustering han llegado a ser esenciales para las organizaciones en cuanto a implementación de negocios críticos, comercio electrónico y aplicaciones de negocios en línea, porque proporcionan mejoras significativas en disponibilidad, escalabilidad y manejabilidad. La instalación y configuración de clustering es más fácil y más robusta en Windows Server 2003, mientras que algunas características de red mejoradas en el producto ofrecen mejor recuperación de fallos y un tiempo productivo alto del sistema.

La familia de Windows Server 2003 soporta clusters de servidor de hasta 8 nodos. Si uno de los nodos en un cluster no se puede usar debido a un fallo o por mantenimiento, inmediatamente otro nodo empieza a dar servicio, un proceso conocido como recuperación de fallos. Windows Server 2003 también soporta balanceo de carga de red, el cual nivela el tráfico de entrada dentro del Protocolo de Internet (IP), a través de los nodos en un cluster.

Escalabilidad. Windows Server 2003 ofrece escalabilidad a través de "Scale-up", habilitado por multiprocesamiento simétrico (SMP) y "Scale-out", habilitado por clustering. Pruebas internas indican que, comparado con Windows 2000 Server, Windows Server 2003 da hasta un 140 por ciento de mejor desempeño en la administración de archivos y un rendimiento más significativo en varias otras características incluyendo servicio Microsoft Active Directory, servidor Web y componentes Terminal Server así como servicios de red. Windows Server 2003 abarca desde soluciones de procesador únicas hasta sistemas de 32 vías. Esto soporta procesadores tanto de 32-bits como de 64 bits.

Fiabilidad. Los negocios han hecho crecer la tradicional red de área local (LAN) al combinar redes internas, externas y sitios de Internet. Como resultado de esto, el aumento de seguridad en los sistemas es ahora más crítica que antes. Como parte del compromiso de Microsoft de brindar computación segura, la compañía ha revisado intensamente la familia Windows para identificar posibles fallos y debilidades. Windows Server 2003 ofrece muchas mejoras y características nuevas e importantes de seguridad incluyendo:

El tiempo de ejecución. Esta función del software es un elemento clave de Windows Server 2003 que mejora la fiabilidad y ayuda a asegurar un entorno seguro. Esto reduce el número de fallos y huecos de seguridad causados por errores comunes de programación. Como resultado, hay menor vulnerabilidad de que ocurran ataques. El tiempo de ejecución de lenguaje común también verifica que estas aplicaciones puedan correr sin errores y chequea permisos de seguridad válidos, asegurando que el código realice solamente las operaciones correspondientes.

Internet Information Services 6.0. Para incrementar la seguridad del servidor Web, Internet Information Services (IIS) 6.0 está configurado para una máxima seguridad - la instalación por defecto está "asegurada". Características de seguridad avanzadas en IIS 6.0 incluyen: servicios de criptografía selectiva, advanced digest authentication, y acceso configurable de control de procesos. Éstas son algunas de las muchas características de seguridad en IIS 6.0 que le permiten llevar a cabo negocios con seguridad en la Web.

Productivo
En numerosas áreas, Windows Server 2003 tiene capacidades que pueden hacer que su organización y empleados sean más productivos, como:

Servicios de impresión y archivos. En el corazón de cualquier organización TI, la habilidad que se tenga de administrar eficientemente los recursos de archivo e impresión, es lo que permitirá que estos estén disponibles y seguros para los usuarios. Al aumentar las redes en tamaño con más usuarios localizados en sitios, en ubicaciones remotas, o en compañías de

socios, los administradores de TI enfrentan cada vez más carga pesada. La familia Windows ofrece servicios inteligentes de manejo de archivos e impresión con una funcionalidad y rendimiento elevado, permitiéndole reducir TCO.

Active Directory. Active Directory es un servicio de directorio de la familia de Windows Server 2003. Esto almacena información acerca de objetos en la red y hace que esta información sea fácil de encontrar por los administradores y usuarios - proporcionando una organización lógica y jerárquica de información en el directorio. Windows Server 2003 trae muchas mejoras para Active Directory, haciéndolo mas versátil, fiable y económico de usar. En Windows Server 2003, Active Directory ofrece una escalabilidad y rendimiento elevado. Esto también le permite mayor flexibilidad para diseñar, implementar y administrar el directorio de su organización.

Servicios de Administración. Mientras que la computación se ha proliferado en ordenadores de sobremesa y dispositivos portátiles, el coste real de mantenimiento de una red distribuida de ordenadores personales ha aumentado significativamente. Reducir el mantenimiento día a día a través de la automatización, es la clave para reducir costes de operación. Windows Server 2003 contiene varias herramientas importantes de administración automatizada como Microsoft Software Update Services (SUS) y asistentes de configuración de servidor para ayudar a automatizar la implementación. La Administración de Políticas de Grupo se hace más fácil con la nueva Consola para Administración de Políticas de Grupo (GPMC), permitiendo que más organizaciones utilicen mejor el servicio Active Directory para sacar beneficio de sus poderosas características de administración. En conclusión, las herramientas de líneas de comandos permiten que los administradores realicen la mayoría de las tareas desde la consola de comandos.

Administración de almacenamiento. Windows Server 2003 introduce características nuevas y mejoradas herramientas para la administración del almacenamiento, haciendo que sea más fácil y más seguro manejar y dar mantenimiento a discos y volúmenes, respaldar y recuperar datos, y conectarse a una red de almacenamiento (SANs).

Terminal Services. Terminal Services, componente de Microsoft Windows Server 2003, se construye en el modo de servidor de aplicaciones en Windows 2000 Terminal Services. Terminal Services le permite enviar aplicaciones en Windows, virtualmente a cualquier dispositivo incluyendo a aquellos que no pueden correr Windows.

Conectado Windows Server 2003 incluye características y mejoras nuevas para asegurarse de que su organización y usuarios permanezcan conectados:

Servicios Web XML. IIS 6.0 es un componente importante de la familia Windows. Los administradores y desarrolladores de aplicaciones Web demandan una plataforma Web rápida que sea tanto escalable como segura. Las mejoras significativas de arquitectura en IIS abarcan un modelo de procesos nuevo que en gran medida aumenta la fiabilidad, la escalabilidad y el desempeño. IIS está instalado predeterminadamente en estado seguro (Lock down). La seguridad se incrementa debido a que el administrador del sistema habilita y deshabilita funciones del sistema de acuerdo a requerimientos de la aplicación. En conclusión, el apoyo directo de edición de XML mejora la administración.

Comunicaciones y redes. Las comunicaciones y redes nunca han sido tan críticas para las organizaciones que enfrentan el reto de competir en el mercado global. Los empleados necesitan conectarse a la red desde cualquier lugar y cualquier dispositivo. Socios, vendedores y otros fuera de la red necesitan interactuar eficientemente con recursos clave, y la seguridad es más importante que nunca. Las nuevas características y mejoras en redes

en la familia de Windows Server 2003 incrementan la versatilidad, manejabilidad y fiabilidad de infraestructura de red.

Servicios empresariales UDDI. Windows Server 2003 incluye servicios empresariales UDDI, una infraestructura dinámica y flexible para servicios Web XML. Esta solución basada en estándares le permite a las compañías llevar a cabo sus propios servicios internos UDDI para redes de uso interno y externo. Los desarrolladores pueden encontrar y reutilizar fácil y rápidamente los servicios Web disponibles dentro de la organización. Los administradores TI pueden catalogar y administrar los recursos programables de su red. Con servicios empresariales UDDI, las compañías pueden crear e implementar aplicaciones más inteligentes y seguras.

Servicios de Windows Media. Windows Server 2003 incluye los servicios de medios digitales más poderosos de la industria. Estos servicios son parte de la nueva versión de la plataforma de tecnologías de Microsoft Windows Media que también incluyen un nuevo reproductor de Windows Media, un codificador de Windows Media, codecs de audio y video y un paquete para desarrollo de software de Windows Media.

Mejor economía Microsoft diseñó Windows Server 2003 para ayudar a las compañías a darle valor añadido a sus negocios al mantener costes bajos. La alta fiabilidad de Windows Server 2003 ayuda a controlar costes al reducir fallos y tiempo de inactividad. Windows Server 2003 tiene la flexibilidad de escalar según la demanda.

Las herramientas poderosas de administración y configuración en Windows Server 2003 le permiten a los negocios implementar y administrar sistemas tan fácil y eficientemente como sea posible. La compatibilidad con aplicaciones heredadas y productos de otras compañías hará que las organizaciones no pierdan su inversión de infraestructura existente. Con la familia de Windows Server 2003, las organizaciones se benefician de una plataforma poderosa y robusta que ayuda a darle a los negocios valor hoy en día y en el futuro.

.NET y los Servicios Web XML

Microsoft .NET está altamente integrado en la familia de Windows Server 2003. Permite un nivel sin precedentes de integración de software al usar servicios Web XML: aplicaciones discretas, con elementos básicos que se conectan entre sí - así como con otras aplicaciones más grandes - vía Internet. Al implantar en los productos la estructura de la plataforma de Microsoft, .NET brinda la posibilidad de crear, alojar, implementar y usar rápida y fiablemente soluciones seguras y conectadas a través de servicios Web XML. La plataforma Microsoft proporciona una serie de herramientas de desarrollo, aplicaciones cliente, servicios Web XML y de servidores necesarios para participar en este mundo conectado.

Estos servicios Web XML proporcionan componentes reciclables construidos en base a los estándares de la industria que integran capacidades de otras aplicaciones independientemente de como las aplicaciones fueron creadas, de su plataforma o sistema operativo o de los dispositivos usados para acceder a ellos.

Con servicios Web XML, los desarrolladores pueden integrar aplicaciones dentro de las empresas y a través de las fronteras de la red con socios y clientes. Este avance - abre la puerta a una colaboración federada y a relaciones de negocio a negocio y de negocio a cliente más eficiente - puede tener un impacto potencial significativo en las ganancias. Millones de otras empresas pueden usar estos componentes en varias combinaciones para producir experiencias altamente personales e inteligentes.

Otros beneficios de .NET en la familia de Windows Server 2003 para los desarrolladores de aplicaciones son:

Aprovechar sus inversiones existentes. Las aplicaciones existentes basadas en Windows continuarán corriendo en Windows Server 2003 y pueden ser fácilmente empaquetadas como servicios Web XML.

Escribir menos código y usar herramientas y lenguajes de programación que conozcan. Esto es posible por estar los servicios de aplicación creados en Windows Server 2003, tales como Microsoft ASP .NET, monitoreo de transacciones, mensajes en espera y acceso a datos.

Usar monitoreo de procesos, reciclaje e instrumentación integrada para dar fiabilidad, disponibilidad y escalabilidad a sus aplicaciones.

Todos estos beneficios están en la infraestructura básica mejorada del servidor de Windows y forman la base de .NET.

DIRECTORIO ACTIVO.

Destaca la nueva capacidad de renombrar dominios, la posibilidad de redefinir el esquema, de desactivar tanto atributos como definiciones de clase en el esquema, la selección múltiple de objetos sobre los cuales realizar cambios simultáneamente, y la de establecer relaciones de confianza en bosques cruzados, evitando problemas con políticas de usuarios y grupos.

El soporte de meta directorios y del inetOrgPerson permite la integración de información de identidades procedente de múltiples directorios, bases de datos y ficheros, así como la migración de objetos de un directorio LDAP al Directorio Activo. Las mejoras en la gestión de políticas de grupo, en el interfaz del usuario a través de la Microsoft Management Console (MMC), y en la conexión con oficinas remotas. En este último aspecto se ha optimizado la sincronización y replicación tanto del Directorio Activo como del Catálogo Global entre controladores de dominio, que puede ser verificada con nuevas herramientas como Health Monitor y cuya compresión puede ser ahora desactivada para disminuir la carga en la CPU a costa de consumir mayor ancho de banda en las comunicaciones.

• ADMINISTRACIÓN.

A través de la Consola de Gestión de Políticas de Grupo (GPMC) se mejora y facilita la administración, integrándose aún más con los servicios del Directorio Activo, con el consiguiente ahorro de costes. Se proporcionan herramientas y servicios de implementación más potentes, entre los que cabe citar Windows Management Instrumentation (WMI), Resultant Set of Policy (RsoP), las mejoras en los servicios de IntelliMirror y la nueva tecnología de Instalación Remota (RIS), con cuya implementación los usuarios pueden disponer de sus aplicaciones y datos sin importar desde donde se conecten a la red corporativa. Se ha potenciado la gestión a través de comandos, admitiendo scripting y facilitando la administración remota.

• SERVICIOS ARCHIVO E IMPRESIÓN.

Al mejorar la infraestructura del sistema de archivos (destacando las tecnologías DFS, EFS y el nuevo soporte de tecnologías Antivirus) ahora es más fácil utilizar, asegurar y almacenar tanto archivos como otros recursos esenciales, y acceder a la información con herramientas de indexación de contenidos más rápidas. Con el Automated System Recovery (ASR) es más sencillo recuperar el sistema, hacer copias de seguridad de los ficheros y mantener la

máxima disponibilidad, sin depender de la asistencia del departamento de TI. La conectividad se ve beneficiada con las características mejoradas de compartición de documentos a lo largo de toda la organización gracias al redirector WebDAV (Web Digital Authoring & Versioning). En lo que respecta a la impresión, además de contar con soporte a más de 3.800 periféricos, los servicios disponen de tecnología tolerante a fallos en cluster, aceptando tareas de otras plataformas como Macintosh, UNIX, Linux o Novell, así como Wireless LAN y Bluetooth. El monitor de estado aporta un mayor rendimiento y más información sobre la situación de los dispositivos, cuyas características (ubicación, color, velocidad, etc) se pueden publicar en el Directorio Activo para un mayor aprovechamiento de estos recursos.

• INTERNET INFORMATION SERVICES 6.0.

Totalmente rediseñado con el objetivo de mejorar la seguridad, fiabilidad y rendimiento, se instala completamente bloqueado por defecto.

Basado en una nueva arquitectura, las aplicaciones web en ejecución están aisladas una de la otra, permitiéndose la monitorización y administración proactiva de aplicaciones así como cambios de configuración en línea, reduciendo el tiempo que precisan los administradores para reiniciar servicios con el fin de mantener las aplicaciones operativas. IIS 6.0 ha demostrado su compatibilidad con miles de aplicaciones de clientes e ISVs, y opcionalmente puede ser configurado para funcionar en modo de aislamiento IIS 5.0, lo que asegura la máxima compatibilidad.

Además con el nuevo IIS 6.0 la replicación de configuraciones de servicio web en diferentes servidores se convierte en una tarea totalmente automatizada permitiendo a los administradores reducir el tiempo de implementación al mínimo.

• CLUSTERING.

Con características avanzadas de recuperación ante fallos y balanceo de carga, ofrecen la máxima disponibilidad 7x24. Integrándose en el Directorio Activo (en el que cada cluster es visto como un objeto "virtual") y con soporte tanto de 32 como de 64 bit, en Microsoft Windows Server 2003 se ha incrementado de 4 a 8 el número máximo de nodos por cluster, disponiendo así el administrador de más opciones para garantizar el servicio para las necesidades de la empresa.

Del Clustering cabe destacar la mayor facilidad de configuración (con pre-configuraciones y administración remota) y de administración de sus recursos (entre ellos el gestor de Balanceo de Carga), las métricas para análisis de disponibilidad, las capacidades mejoradas en seguridad (soporte de Kerberos, EFS e integración con Seguridad IP), de almacenamiento (con funciones específicas para redes SAN) y las destinadas a la recuperación de fallos, contribuyendo todo ello al máximo uptime.

• NETWORKING Y COMUNICACIONES.

Con ayuda de la Resultant Set of Policy se puede analizar el impacto de la implementación de políticas de red y comunicaciones, simplificando así la resolución de problemas. Mediante los servicios de Instalación Remota, las herramientas para migración de configuraciones de usuarios, el nuevo Windows Installer (con soporte de aplicaciones de 64 bit, así como de firmas digitales y CLR), el software Update Services para testar las actualizaciones de Windows Update antes de ser aplicadas en la organización y muchas otras nuevas características de Microsoft Windows Server 2003, se logra una mejor gestión centralizada

de recursos y servicios, contribuyendo así a la reducción del TCO y el aumento de la productividad de los usuarios.

• TERMINAL SERVICES.

Permiten disponer de aplicaciones Windows e incluso de los propios escritorios Windows en prácticamente cualquier dispositivo, incluyendo aquellos que ni siquiera funcionan bajo sistemas operativos Windows. Los nuevos Terminal Services, construidos sobre la base y la experiencia de los existentes en Microsoft Windows 2000 Server, ofrecen nuevas opciones para la implementación de aplicaciones, un acceso más eficiente a los datos con conexiones de menor ancho de banda, mayor número de usuarios concurrentes, y mediante Session Directory proporciona el soporte necesario para el balanceo de carga de red (tanto el desarrollado por Microsoft como el de otras tecnologías de terceros).

Además con el nuevo Terminal Server el usuario podrá ver sus unidades y dispositivos locales en sus sesiones remotas, así como recibir audio y video en diferentes calidades a su elección. La administración de sesiones se mejora permitiendo visualizar diferentes sesiones a la vez en consola por parte del administrador e interactuar con ellas aportando valor a la sesión.

• ADMINISTRACIÓN DE ALMACENAMIENTO.

Añade nuevas y mejoradas funcionalidades para la gestión del almacenamiento, haciendo más fácil y fiable la manipulación de discos y volúmenes, copias de seguridad y procesos de restauración, así como la conexión a redes SAN (Storage Area Networks). El IFS (Intelligent File Storage) protege los datos de los usuarios, facilita el acceso a redes complejas y proporciona una arquitectura de almacenamiento flexible. Shadow Copy Restore permite a los usuarios la recuperación de versiones previas de archivos sin interrumpir su trabajo y sin necesidad de intervención administrativa. DFS (Distributed File System) permite a los administradores asignar un único name-space, proporcionando a los usuarios un único acceso virtual a elementos agrupados de forma lógica, aunque estén almacenados en diferentes localizaciones físicas. La encriptación de datos de los usuarios (EFS, Encrypting File Systems) es ahora más sencilla e incluye la encriptación offline de carpetas y archivos, siendo particularmente beneficioso para los usuarios móviles.

• WINDOWS MEDIA SERVICES.

Los Windows Media Services ofrecen nuevas oportunidades de comunicación (eLearning y broadcasting, tanto comercial como corporativo), y eliminan el buffering para clientes que acceden a contenidos ricos en elementos multimedia, con lo que se puede dar soporte al doble de los usuarios actuales con Microsoft Windows 2000 Server. A esto contribuye también el Audio Acceleration, que da prioridad, a la carta, al tráfico multimedia sobre otros flujos de datos en servidores de acceso remoto, lo que proporciona un mejor rendimiento, beneficiando especialmente a las redes de baja velocidad.

• .NET FRAMEWORK.

El .NET Framework está formado por tres elementos principales: el runtime del lenguaje común (Common Language Runtime, CLR), un conjunto jerárquico de librerías de clases unificadas, y una versión avanzada de Páginas de Servidor Activas llamada ASP+. Integrando el entorno de desarrollo de aplicaciones .NET Framework en Microsoft Windows Server 2003, los desarrolladores ya no tendrán que escribir más código para resolver tareas de "fontanería informática", centrándose exclusivamente en crear valor en los procesos de

negocio. Además, los nuevos Enterprise UDDI Services permiten descubrir y reutilizar fácilmente servicios web dentro de la propia organización, ejecutándose el servicio UDDI para su uso en la intranet o la extranet, beneficiando así también a los desarrolladores.

• APPLICATION SERVICES.

Los avances en Microsoft Windows Server 2003 proporcionan numerosos beneficios para el desarrollo de aplicaciones, lo que redunda en una significativa reducción del TCO (Coste Total de Propiedad) y en un mejor rendimiento. Entre ellos destacan una integración e interoperabilidad más simplificada (con el soporte nativo de servicios Web XML, así como de los estándares UDDI, SOAP y WSDL), mejoras en la productividad (al incluir Microsoft .NET Framework, Message Queuing, COM+ y ASP .NET), una escalabilidad y eficiencia superiores (gracias a la integración de ASP .NET en IIS 6.0, al soporte asíncrono de .NET Framework y la memoria caché inteligente de ASP .NET), una seguridad garantizada end-to-end y a una implementación y gestión más eficientes con los servicios Windows Installer y nuevas herramientas como fusión, que soporta el versionado de DLLs side-by-side.

CAPÍTULO 2

TEORÍA DE SEGURIDAD

2.1 Conceptos de Seguridad

En este capitulo trataremos las diferentes definiciones que existen de Seguridad y para nuestro interés la seguridad informática.

Definición de Seguridad

Confianza tranquilidad de una persona procedente de la idea de que no hay ningún peligro. Es una cualidad o estado seguro.

Definición de Seguridad en Cómputo

Una versión acerca de un sistema completamente seguro se la atribuye a Gene Spafford[1], podría juzgarse de cómica pero nos refleja cuán difícil puede ser mantener un sistema confiable y seguro.

"*El único sistema que es completamente seguro es aquel que está apagado, desconectado, guarnecido en una caja fuerte de titanio, enterrado en una caja de concreto, rodeado de gas irritante y por unos guardias altamente armados (aún así yo no arriesgaría mi vida por él).*"

Con una definición más cercana a nuestras necesidades, encontramos que según Garfinkel[2] la seguridad en cómputo puede definirse en los siguientes términos:

"*Una computadora es segura si uno puede depender de ésta y su software, y si éstos funcionan como uno espera que lo hagan.*"

Si uno espera que los datos que hoy dejó en la máquina, en unas semanas sigan ahí sin que alguien más los haya leído, entonces la máquina es segura, a este concepto también se le conoce como "confiabilidad" (trust).

Esto nos lleva a identificar a la seguridad como protección, ahora nos falta especificar qué es lo que queremos proteger y de qué. Las tres áreas de protección que nos interesan son: Software, Hardware y los datos, de que los queremos proteger:

Hardware

- Protección de destrucción de hardware valioso.

Software

- Protección de destrucción de programas valiosos.

Datos

- Protección de destrucción de datos valiosos.

  Y para las tres áreas (Hardware, Software y Datos):

- Protección a cambios no autorizados.
- Protección a uso no autorizado.

[1] Garfinkel, Simson and Spafford, Gene. Practical UNIX Security. Ed. O'Reilly & Associates. Inc USA 1994
[2] N, Derek Arnold. UNIX Security a practical Tutorial. McGrawHill 1993, pags. 10 y 11.

2.2 Definiciones de Seguridad[3]

2.2.1 Seguridad en la Información (INFOSEC)

La protección en el proceso de la información se requiere por que la información puede ser comprometida por ignorancia, inadvertencia, accidentalmente o por malicia.

2.2.2 Seguridad en Cómputo (COMPUSEC)

El sentido general de "seguridad en cómputo" (COMPUSEC), será expuesto como el estado de certeza de que los datos computarizados y los archivos de programas no pueden ser accesados, obtenidos o alterados por personas no autorizadas.

2.2.3 Seguridad en los datos

Consiste de procedimientos y acciones diseñadas para prevenir la revelación no autorizada, transferencia, modificación o destrucción, accidental o intencional de los datos. Hoy en día el término de datos debe ser cambiado por información, simplemente por que cada vez más el tráfico de la red consiste de información en general, más que datos (incluyendo imágenes, fax, video, etc.)

2.2.4 Seguridad en Comunicaciones (COMSEC)

En los años recientes, el tema ha tomado la dirección de que la información "segura" fluye en redes y líneas de comunicación "seguras". La seguridad en comunicaciones COMSEC es, por lo tanto, la protección como resultado de la aplicación de "criptoseguridad", seguridad en la transmisión, la emisión de medida de seguridad a telecomunicaciones y de medidas de seguridad física a la información que se transmite por los distintos medios de comunicación.

2.2.5 Criptoseguridad

Es el componente de Seguridad en comunicaciones COMSEC, que resulta de la aplicación de criptosistemas (métodos mediante los cuales la información se vuelve indescifrable sin una llave), técnicamente hablando y su uso.

2.2.6 Seguridad en la Transmisión (TRANSEC)

El componente de COMEC que resulta que de todas las medidas destinadas a proteger los trasmisores de interceptaciones y exploraciones no autorizadas.

2.2.7 Emisión de Seguridad (EMSEC)

El componente de COMSEC que resulta que todas las medidas tomadas para negar el acceso a personas no autorizadas, el acceso a información valiosa, que podría ser obtenida de interceptar las emanaciones de equipo de encriptamiento y sistemas de telecomunicaciones.

2.2.8 Seguridad Física

El componente de COMSEC que resulta que todas las medidas físicas necesarias para salvaguardar equipo clasificado, material y documentos de acceso u observación por personas no autorizadas.

[3] Madron, Thomas W. Network Security in the 90's. Issues and Soluctions form Managers. Ed. Wiley Professional Computing. USA 1992 p.3-24.

2.2.9 Sistemas de Seguridad

Consiste de la combinación de subsistemas de hardware y software. Seguridad en equipo de comunicaciones. Por ejemplo, equipo diseñado para proveer seguridad a telecomunicaciones, para convertir la información a una forma ininteligible a un interceptor no autorizado, y posteriormente reconvertir ésta información a sí forma original para los receptores autorizados; tanto como equipo diseñado específicamente para obtener ayuda o como sólo un elemento en el equipo de comunicación.

2.3 Servicios de Seguridad[4]

Existen diferentes tipos de servicios sobre seguridad en cómputo. Es importante que ambos administradores y usuarios, conozcan los servicios de seguridad que los profesionales en la materia manejan (y que los usuarios esperan).

2.3.1 Privacidad o Confidencialidad

Es proteger la información para que ésta no sea leída por alguien que no ha sido autorizado explícitamente. Esta protección no sólo abarca información conjunta (total), si no fragmentos de la misma que pueden parecer inofensivas por sí mismas, pero pueden ayudar a inducir a información confidencial.

2.3.2 Autenticación

En este servicio debe considerarse una doble autenticación: el origen de los datos y la entidad en comunicación. La autenticación del origen puede definirse como: “La corroboración de que el originador de los datos recibidos es quien pretende ser” y la autenticación de la entidad en comunicación es verificar que el otro extremo en la comunicación es el que se esperaba.

2.3.3 Integridad de los datos

Protección a la información (incluyendo programas) de ser borrada o alterada, sin autorización del dueño de la misma. La información a proteger también incluye registros de contabilidad, respaldo en cintas, tiempo de creación de los archivos y documentación.

2.3.4 Consistencia

Asegurarse de que el sistema funciona tal como los usuarios esperan que se comporte. No existe si el hardware o el software repentinamente empieza a comportarse de forma diferente a como solía comportarse, especialmente después de una actualización al sistema o de revisión de una falla.

2.3.5 Aislamiento o Control de Acceso

Regularización del acceso al sistema. Controlar el acceso al sistema de individuos no autorizados o no conocidos; se deben determinar los siguientes puntos: cómo logro entrar, qué ha hecho y quién, o quién más tiene acceso al sistema. No debe confundirse el controlar el acceso con autenticar ya que se puede autenticar a un usuario para acceder el sistema y mediante el aislamiento se definen los permisos que tiene.

[4] Lynch, Daniel C. And Marshall T. Internet System Handbook. Addison Wesley Publishing Company I.nc. 1993.

2.3.6 Revisión o No Repudio

Así como los usuarios no autorizados deben ser controlados, los usuarios autorizados también comenten errores y aún más actos maliciosos. En este caso se debe determinar qué fue hecho, por quién y qué fue afectado. La única forma de obtener esta información es por medio de un registro incorruptible que registre todas las actividades del sistema y que sea capaz de identificar el actor y las acciones involucradas, de esta manera se evita que quien(es) esté(n) involucrado(s) en la comunicación niegue(n) haber participado.

2.4 Criterios de Seguridad[5]

Para poder definir que tan confiable es un sistema, el Departamento de la Defensa delos Estados Unidos en su *ORANGE BOOK* indica los diferentes niveles de seguridad que se han establecidos. Se enuncias las características de implementación que deben cumplir los sistemas para pertenecer a una o a otra división.

2.4.1 Introducción

Los criterios están clasificados en cuatro divisiones D, C, B, y A ordenados de manera jerárquica, estando la división más alta (A) reservada para sistemas que proveen mayor seguridad. Cada división representa una mejor implementación que se traduce en mayor confiabilidad en un sistema en cuanto a protección de información sensible (llamaremos información sensible a aquella que es factible a ser dañada, y que además tiene nuestra atención por su importancia). Dentro de las divisiones C y B existen subdivisiones llamadas clases, que a su vez son ordenadas de manera jerárquica (C2 a mejor implementación C1 a menor).

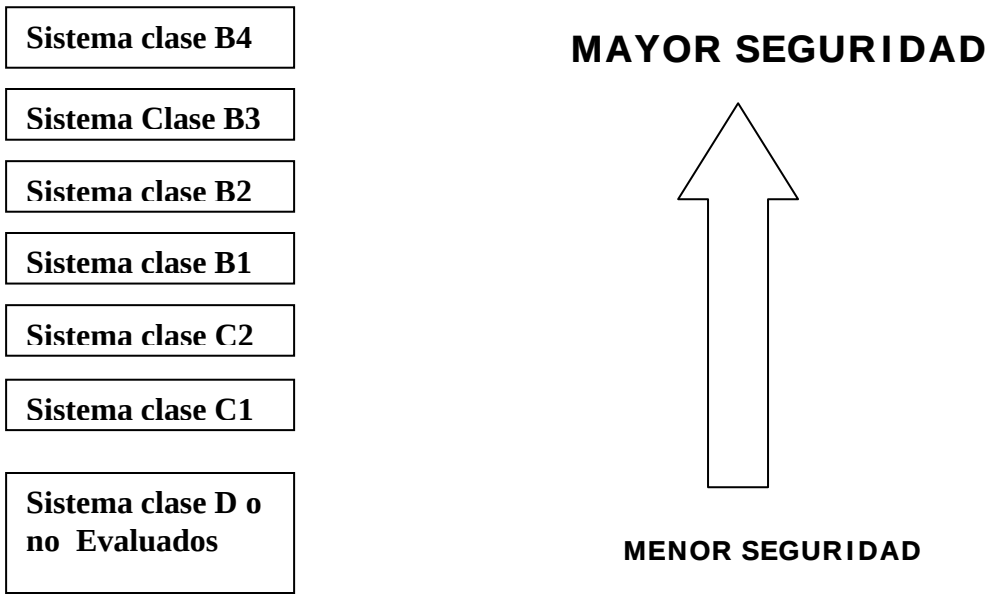


Figura. 2.1 Niveles de Seguridad según Orange Book.

Para garantizar el diseño e implementación de los sistemas se realizan pruebas sobre porciones relevantes para la seguridad del mismo sistema. Dichas porciones son referidas como Trusted Computing Base (TCB). O como lo define James Arlin Cooper:[6]

[5] Departament of defense Trusted Computer System Evaluation Criteria, DOD 5200.28.STD 1985.

"La totalidad de mecanismos de seguridad de hardware y software en un sistema computacional."

Esto es, un TCB es el conjunto de mecanismos de protección dentro de un sistema computacional, incluyendo el Hardware, firmware y software, combinación responsable de reforzar las políticas de seguridad sobre un producto o sistema. La habilidad de un TCB para reforzar correctamente una política de seguridad depende únicamente de los mecanismos dentro del TCB y de las entradas correctas de parámetros introducidas por el personal administrador del sistema en relación con las políticas de seguridad.

A partir de pruebas al TCB se declara un sistema dentro de una clase u otra, estas pruebas principalmente verifican atributos de seguridad, específicamente su estructura de diseño e implementación.

Para cada criterio existe un grupo de requerimientos. Estas agrupaciones fueron desarrolladas para asegurar que los tres objetivos de control básicos sobre seguridad computacional sean satisfechos y no pasados por alto, entendiendo como objetivos de control a métodos que expresan metas de seguridad. Estos objetivos son:

- Políticas de seguridad.
- Contabilización.
- Confianza.

Los métodos deben proveer un esquema que permita desarrollar una estrategia que llene completamente un conjunto de requerimientos de seguridad en cualquier sistema dado.

2.4.2 Clases y Divisiones

Como se mencionó algunas de las divisiones (C y B) contienen subdivisiones llamadas clases. A continuación se resumen las características a cumplir por un sistema para encontrarse dentro de una división y según corresponda a una clase.

2.4.2.1 División D: Protección Mínima

Esta división contiene sólo una clase. Esta reservada para aquellos sistemas que han sido evaluados pero que fallan en alcanzar requerimientos de una clase mayor. La mayoría de los sistemas de PC pueden pertenecer a esta clase, pero no tiene sentido evaluar para caer en esta división, que es por omisión.

2.4.2.2 División C: Protección Discreta

Las clases en esta división proveen protección discreta e informes de sujetos y las acciones que ellos realizan a través de la inclusión de capacidades auditoras y contabilizaciones de sujetos y las acciones que estos inician.

A) Clase C1: Protección de seguridad discreta

El TCB de un sistema de clase C1 proporciona los elementos básicos para satisfacer los requerimientos mínimos de seguridad discreta proveyendo separación de los usuarios y los

[6] Cooper, James Arlin, Computer & Communications Security Strategies for the 1990's. McGraw Hill Communications, Series, New York, 1989 pág. 386

datos. Incorpora algunos controles capaces de reforzar las limitaciones de acceso en una base individual, por ejemplo, permitir a los usuarios el proteger o privatizar información no dejando a otros usuarios leer "accidentalmente" o destruir sus datos. Se supone que el ambiente de una clase C1 sea de usuarios procesando datos al mismo nivel de sensibilidad de manera cooperativa.

B) Clase C2: Protección de acceso controlada

Los sistemas en esta clase refuerzan de una manera más granular el control de acceso discreto que los sistemas de clase C1, haciendo a los usuarios responsables de manera individual de sus acciones a través de sus procedimientos de *login,* auditando los eventos de seguridad relevante, y del aislamiento de recursos.

El sistema operativo Windows NT cae dentro de esta clase C2.

2.4.2.3 División B: Protección Obligatoria

Un requerimiento básico en esta división es la noción de un TCB que se encargue de preservar la integridad de las etiquetas y que utilice éstas para reforzar un conjunto de reglas de control de acceso obligatorios. Los sistemas en esta división deben manejar las etiquetas con estructuras de datos en el sistema. El desarrollador del sistema también proveerá el modelo de políticas de seguridad en el que se basa el TCB. Se debe de proveer también la evidencia necesaria que demuestre que el concepto de monitor de referencia se ha implementado.

A) Clase B1: Protección de seguridad mediante etiquetas

Los sistemas de la clase B1 requieren todas las características de la clase C2, además de un modelo de seguridad informal, etiquetamiento de datos, y control de acceso obligatorio sobre objetos y sujetos. Cualquier "flujo"[7] identificado por pruebas debe ser removido.

Sybase Secure SQL Server ha sido evaluado para esta clase.

B) Clase B2: Protección Estructurada

En los sistemas de la clase B2, el TCB se basa en un modelo formal de políticas de seguridades claramente definidas y documentadas que requiere del reforzamiento del control obligatorio y discreto encontrados en la clase B1 extendiéndose a todos los sujetos y objetos en el sistema. Además se direccionan canales ocultos. La interface TCB está mejor definida y su diseño e implementación se someten a mayores pruebas y más complejas revisiones. Se refuerzan mecanismos de autentificación. Se agregan elementos de confiabilidad para el operador y administrador del sistema. El sistema es relativamente resistente a la penetración.

C) Clase B3: Seguridad en dominios

El TCB de la clase B3 debe satisfacerlos requerimientos del monitor de referencia, intervenir todos los accesos de sujetos y objetos, ser a prueba de intromisiones, y lo suficientemente pequeños para ser sujeto de análisis y pruebas. Por esto, el TCB está estructurado para excluir código no esencial para reforzar las políticas de seguridad. Soporta un administrador de seguridad, los mecanismos de auditoria se expanden para señalar eventos de relevancia

[7] Flujo: Error por descomposturas, omisión o descuido en un sistema que permite eludir los mecanismos de protección.

en seguridad, además se requieren procedimientos de recuperación del sistema. El sistema es altamente resistente a la penetración.

2.4.2.4 División A: Protección Verificada

Esta división se caracteriza por el uso de métodos de verificación formal de la seguridad para asegurarse de que los controles de seguridad obligatorios y discretos empleados en el sistema pueden efectivamente proteger la información clasificada o sensible almacenada o procesada por le sistema. Se requiere una extensiva documentación para demostrar que el TCB cumple con los requerimientos de seguridad en todos los aspectos de diseño, desarrollo e implementación.

A) Clase A1: Diseño verificado

Los sistemas en la clase A1 son equivalentes funcionalmente a los de la Clase B3, no se agregan características en la arquitectura o requerimientos de políticas. Los rasgos distintivos de los sistemas en esta clase son el análisis derivado de la especificación formal del diseño, las técnicas de verificación y el resultante alto grado de confianza de que el TCB está correctamente implementado. Esta seguridad proviene del desarrollo, desde el modelo formal de las políticas de seguridad hasta las especificaciones de diseño formales del más alto nivel. Independientemente del sistema o lenguaje de verificación empleado, existen criterios importantes para la verificación del diseño, entre ellos destaca que el modelo formal de políticas de seguridad debe de estar claramente identificado y documentado, incluyendo pruebas matemáticas de la consistencia del modelo con sus axiomas respectivos. En concordancia con el exhaustivo diseño y análisis de desarrollo del TCB requerido de sistemas de clase A1, se requiere un más riguroso manejo d la configuración y se establecen procedimientos para una segura distribución del sistema a los diferentes sitios. Es soportado un administrador de seguridad.

Consideramos importante mencionar las áreas que destacan en una clase A1:

Arquitectura del sistema

Debe proporcionarme una demostración formal que muestre los requerimientos de auto-protección y completitud para los monitores de referencia que hallan sido implementados en le TCB.

Pruebas de seguridad

Se debe aspirar que a un futuro se implemente algún tipo de auto-prueba automática para las especificaciones formales.

Especificaciones y verificaciones formales

El TCB debe ser verificado a nivel de código fuente, utilizando métodos de verificación formal donde sea posible (se ha probado que este tipo de verificaciones sobre un sistema operativo son realmente difíciles).

Ambiente de diseño confiable

El TCB debe ser diseñado bajo condiciones confiables, con características de confiabilidad y sólo con personal confiable.

Hasta la fecha el único que ha alcanzado la clasificación A1 ha sido el sistema Honeywll SCOMP.

2.5 Agujeros de Seguridad

Los “agujeros” en la seguridad (puntos vulnerables) se manifiestan de cuatro formas:

1. Agujeros de Seguridad en la parte física.

En estos el problema básicamente consiste en dar acceso a la parte física de la máquina a personas no autorizadas. Ejemplo de esto son aquellos centros donde tienen estaciones de trabajo y para un usuario puede resultar trivial reinicializar una máquina en modo monousuario (single user) y alterar el almacenamiento de archivos, o cualquier usuario con acceso al manejador de cintas.

2. Agujeros de Seguridad en Software.

Éstos son básicamente software mal desarrollado, que debido a esto tiene altos privilegios que permiten acceder a información confidencial.

3. Agujeros de Seguridad por incompatibilidad de uso.

En ocasiones debido a la falta de experiencia del administrador del sistema, ensambla una combinación de hardware con software que son útiles, pero desde el punto de vista de seguridad presentan un agujero, esto es conectar dos cosas incompatibles que aunque funcionen, son vulnerables en seguridad.

4. En no elegir una idónea filosofía de seguridad y mantenerla.

El cuarto tipo es percepción y entendimiento. Un software perfecto, hardware protegido, y compatibilidad de los componentes no trabajan a menos que se seleccione y aplique una política de seguridad adecuada. Tener el mejor mecanismo del mundo para asignar una contraseña (passwords), está por demás si los usuarios asignan el nombre de su clave como contraseña.

La seguridad es relativa a la política, o conjunto de políticas y a la función del sistema conforme a ese conjunto de políticas.

2.5.1 Atacantes

Este es uno de los puntos más importantes, identificar quiénes pueden ser nuestros “enemigos” y sus causas.

A diferencia de lo que muchos pueden creer el mayor número de atacantes en las diferentes redes han sido personas de la misma empresa: administradores resentidos, vengativos, empleados que buscan algún beneficio propio ($) y los menos pero no por eso menos peligrosos son aquellos que por curiosidad o para probar sus capacidades y la de su objetivo se entrometen en nuestro sistema, éstos últimos son los más famosos y existen diferentes acepciones para ellos, a veces llamados hackers y en otras crackers, aunque difieren las definiciones a continuación se proporciona una definición de hacker según Arlin Cooper y en el capítulo 5 estudiaremos más a fondo este concepto.

Hacker (Según James Arlin Cooper)[8]

"Individuo que persistentemente explora computadoras u redes para aprender como pueden ser utilizadas. Actualmente el término se aplica a aquellos que tratan de burlar las barreras de seguridad de la computadora y de la red, la mayoría de las veces como desafío."

La diferencia básicamente que hay entre un hacker y un cracker es la intención para el primero de aprender y para el segundo de dañar, no por esto va a justificar al hacker que de cualquier forma está violando nuestra seguridad. Aunque éstos atacantes son muy peligrosos, no debemos olvidar a los cracker que son más dañinos por su propia naturaleza. La mayoría de las perdidas ocurridas en empresas u organizaciones cada año, es el resultado de errores humanos, accidentes y omisiones, y de esto se deriva que las más de las veces éstos son ocasionados por el personal de la empresa o gente que colabora en la organización, y una minoría de estas pérdidas es ocasionada por personas ajenas al lugar donde suceden las mismas. Una persona que tiene por su labor acceso a nuestro sistema, un usuario, no tiene que evadir las barreras que un hacker ni las lógicas ni las físicas, así que les, es más fácil destruir u obtener provecho de la información o del equipo, existente cientos de casos de gente que ha violado la seguridad, realizando fraudes, haciéndose ricos, obteniendo información clasificada o vengándose de alguna actitud tomada hacia él, y estas personas estaban o habían laborado en la empresa.

2.6 Modelos de Seguridad

Antes de que una política de seguridad pueda implementarse en un lugar, el primer paso es escoger un modelo de seguridad. El modelo de seguridad es el armazón dentro del que se desarrolla una política de seguridad que es único. En su nivel más básico un modelo de seguridad actúa como una lista de verificación (checklist), asegurando que allí no se están abriendo boquetes o agujeros en la política de seguridad.

Pero un modelo de seguridad es mucho más que eso. Es una filosofía que guía la manera en la que se enfoca en la seguridad. Mientras la mayoría de los modelos cubren los mismos temas, los enfoques pueden variar, para que sea importante escoger un modelo que cubre bien con su filosofía corporativa.

Antes de proceder, es una idea buena definir términos que se usarán en este capítulo. Éstas son palabras que pueden haber sido escuchadas sin estar claras en su definición. Es importante entender estos términos, porque tendrán que ser comunicados a los administrativos y a todos los empleados, el responsable va desarrollar la política de seguridad en red.

Para nuestras definiciones, nosotros enfocaremos lo siguiente:

- Modelo de seguridad.
- La política de seguridad.
- Las normas.
- Las pautas.

El modelo de seguridad simplemente es, como ya se mencionó, un armazón. Dentro de este armazón, hay políticas que se desarrollan. Por otra parte los diferentes modelos de seguridad llegarán a tener políticas de seguridad ligeramente diferentes.

[8] Cooper, James Arlin. Computer & Communications Security. McGraw Hill Publishing N.Y. 1989 Pág. 375.

Qué plantea una política de seguridad. La política de seguridad es una publicación, y comunicado, donde se ponen "reglas" que se exigen a todos los empleados, clientes, o vendedores y son requeridas para ser adheridas y observadas. La política de seguridad, o políticas, no es optativo.

Para que una política de red sea eficaz tiene que ser comunicada y reforzada. Si nadie sabe sobre una política, no va a ser seguida. Recíprocamente, si la política se ha publicado, pero nadie la sigue, es igualmente ineficaz.

El modelo de seguridad que se escoja debe permitirle flexibilidad desarrollando y evaluando políticas. Sobre las contraseñas que manejan en la red, se puede crear una política en la cual requiere que todas las contraseñas sea por lo menos de 10 caracteres, que tenga las últimas dos letras importantes para usted, dos números, y dos caracteres del standard por lo menos ($, @, #, etc.), y sea cambiado una vez a la semana. Al principio esto parece muy seguro hasta que usted da una vuelta y ve pequeños notas en las que se escriben contraseñas, pegadas a todos los monitores.

Otras dos definiciones que están integradas en este capítulo son normas y pautas. Las normas son sistemas o requisitos de propósito-específicas. Las normas proporcionan una guía al escoger nuevos equipos, o al instalar un nuevo componente de hardware o software.

Las pautas son similares a las normas, pero no se requieren. En cambio, se les sigue fuertemente. Una pauta podría ser que todos los switches permitan el acceso remoto a través de SSH, y Telnet y ser desactivados. Mientras ésta es una precaución de seguridad excelente que simplemente no puede ser practica, ya que tantos switches no soportan esta capacidad. Por supuesto, cuando más switches empiezan a permitir que SSH acceda, usted puede decidir que SSH-sólo acceda a una norma.

La política de seguridad usará políticas, normas, y pautas. Estando tan completa como sea posible la cual prevendrá confusión en la aplicación de la política, y la hará más fácil de seguir.

El enfoque de este capítulo es la seguridad. Por consiguiente cuando se discute de modelos de seguridad, el enfoque que se estará llevando a cabo para implementar un modelo de seguridad será para la red, una red tiene que estar integrada en una política de seguridad más grande.

Aún cuando no se tiene un modelo de seguridad bien definido, se necesitará trabajar con colegas en otras secciones al desarrollar un modelo de seguridad, así como personal tendrá que trabajar con otros miembros administrativos antes de determinar qué modelo se usará.

El primer paso es entender qué tipos de modelos están disponibles. Escoger el modelo más fácil será determinando las necesidades. Se verán a continuación algunas opciones de modelos de seguridad entre las cuales escogeremos un modelo en el cual basaremos nuestra seguridad.

2.6.1 RFC 2196: El Manual de Seguridad de Sitio

La Fuerza de Tarea de Ingenieros de Internet (IETF) ha desarrollado un manual para crear políticas de seguridad de sitio. Este manual es comúnmente llamado como, el Manual de

Seguridad de Sitio, también conocido como RFC 2196, detallando los procesos por los que los administradores[9] pueden desarrollar políticas de seguridad y procedimientos.

Uno de las mayores apelaciones del Manual de Seguridad de Sitio es que se diseña con flexibilidad en mente. Este modelo puede aplicarse a las compañías grandes y pequeñas, con muchos tipos diferentes de infraestructuras de red.

El Manual de Seguridad de Sitio se acerca al proceso de desarrollo de una política de seguridad a través de un proceso de cinco pasos:

1. Identificar lo que se está intentando proteger.

2. Determinar lo que se está intentando proteger.

3. Determinar cuales son las probables amenazas.

4. Implementar medidas de instrumento que protegerán los recursos de una manera rentable.

5. Revisar el proceso continuamente y hacer mejoras cada determinado tiempo para encontrar una debilidad.

Este modelo de cinco pasos es bastante trivial, y se documentó originalmente en el Control y Seguridad de Sistemas de Información de Computadoras (Fites, Kratz, y Brebner, 1989).

El Manual de Seguridad del Sitio es bueno ya que proporciona ejemplos concretos de políticas de seguridad que normalmente se llevan a cabo. Estos ejemplos proporcionan una guía al desarrollar primero un plan, dándole una base de información para trabajar. El downside es el Manual de Seguridad de Sitio que se escribió en 1997. Hay varios agujeros provistos en él, se comentan como ninguna discusión de VLANs o otros métodos de seguridad de interrupción, y como ninguna discusión de Protocolo de la seguridad Entrada Fronterizo (BGP).

Como cualquier modelo de seguridad bueno, el Manual de Seguridad de Sitio permite omisiones animando a que se implementen políticas flexibles. Mientras el paso 4 es discutiblemente el de la mayoría de tiempo consumido, el paso 5 es indudablemente el más importante. Si los administradores no se quedan parados de frente a los problemas de seguridad actuales, entonces la política de seguridad se volverá inútil en el futuro.

El Manual de Seguridad del Sitio no recomienda políticas en vías de desarrollo para hardware específico; en cambio, deben desarrollarse políticas para las clases de dispositivos como: servidores de red, routers, estaciones de trabajo, y protocolos: RIP (Protocolo de Información de Routers) Versión 2.0, (OSPF), DNS, y así sucesivamente.

Finalmente, el Manual de Seguridad de Sitio ayuda a los usuarios a documentar el proceso para identificar, manejar, e informar un incidente de seguridad. También le ayuda a desarrollar una política para la consecuencia de un incidente de seguridad.

2.6.2 Seguridad Cisco

Cisco ha desarrollado un modelo de seguridad específicamente diseñado para redes. La seguridad no es una norma autosuficiente. De hecho, los diseñadores asumen que los

[9] Los autores de este RFC usan el término administradores para referirse a una red de computadoras y administradores del sistema, así como la sub-dirección, a quienes pueden tomar decisión.

usuarios tienen su propio modelo, La seguridad son actos como un aditamento específicamente para la red.

El modelo de seguridad tiene seis metas, listadas en orden de importancia:

1. La seguridad y mitigación del ataque basados en una política
2. La implementación de la seguridad a lo largo de la infraestructura
3. La administración segura y de reportes
4. La autentificación y autorización de usuarios y administradores a los recursos críticos de la red.
5. La detección de la intrusión para los recursos críticos y subredes.
6. El soporte para aplicaciones conectadas a la red de computadoras.

Esto es verdad con la mayoría de modelos de seguridad que se planean para la red, pero ese acercamiento de módulos no se declara a menudo explícitamente. En este caso, la seguridad de los módulos está que el segundo listado alcancé la meta de seguridad. Otra ventaja del modelo de seguridad es que usa un plan modular diseñado.

La seguridad actualmente acostumbra un acercamiento modular predispuesto en grados de seguridad. El primer grupo de módulos contiene divisiones de red, mientras el segundo grupo contiene divisiones dentro de los módulos más grandes.

Hay dos modelos de seguridad diferentes, el primero cubre las necesidades de organizaciones de la empresa, el segundo cubre las necesidades de negocios pequeños. El plan del módulo para ambos modelos es el mismo (vea la figura 2.2)

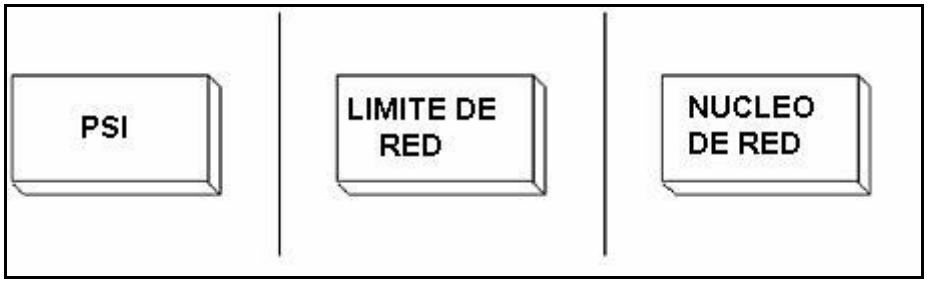


Figura 2.2 Módulos de Seguridad

Dentro de cada módulo hay más módulos pequeños que cubren áreas de plan de red importantes. Por ejemplo, el módulo de Borde de Red tiene módulos más pequeños para las puertas de enlace de entrada, Los accesos VPN, y los servicios públicos (Web, FTP, o servidores de DNS).

Este tipo de modularidad le permite al modelo de Seguridad ser integrado lentamente. Llevando a cabo uno o dos de los módulos del segundo-grado en un momento, en lugar de intentar convertir una red entera, Los administradores de la red pueden guardar registros de lo que se ha hecho fácilmente, y lo que tiene que ser completado todavía.

El inconveniente de estos módulos es que no pueden reflejar su plan de la red. La Seguridad le permite esto obligándole a que usara todos los módulos disponibles para desarrollar su política de seguridad. Sin embargo, usted puede encontrarse con los problemas cuando ni siquiera el equipo dentro de un módulo no empareja en la infraestructura de red.

La Seguridad aventaja a describir maneras detalladas de asegurar routers y switches. El aspecto de seguridad de red de este modelo es excepcional; proporciona muchos consejos prácticos que no es ninguna plataforma específica.

Los consejos de Seguridad ofrecidas para la seguridad del servidor no son detalladas. Esto es indudablemente porque los servidores no se ven desgraciadamente como dispositivo en una red, la realidad es que se intenta separar servidores públicos de la red por consiguiente imposible, y a menudo un equipo de seguridad de red es muy activo en políticas de seguridad en vías de desarrollo para los servidores públicos.

2.6.3 Criterios Comunes / ISO 15048

El Criterio Común para las Tecnología de Información en Seguridad fueron revisadas en mayo de 1998. La Organización Internacional para la Standardización (ISO), Criterio Común usado como la base para su modelo de seguridad, ISO 15048, salió en junio de 1999. La versión del Criterio Común que estudiaremos es la 2.1 que son ISO 15048.

El Criterio común es en él que se evalúan sistemas y productos específicos. Si una organización adopta un Criterio Común como un modelo de seguridad, ya hay productos que son certificados por ISO 15048 qué deben integrarse transparentemente en la organización.

El Criterio Común se refiere al sistema que está evaluándose como un blanco de evaluación (TOE).El TOE se evalúa para tres tipos de fallas: descubrimiento desautorizado, modificación desautorizada, y disponibilidad.

El Criterio común en tecnologías de la información enfoca amenazas de seguridad que involucran interacción humana, sin tener en cuenta si o no estas amenazas son intencionales o accidentales. Mientras esto es adecuado, expone dos limitaciones con este modelo: No se dirige a otros tipos de problemas de seguridad, y no tiene en cuenta los problemas de seguridad en tecnologías de la información.

Mientras el criterio común puede integrarse ciertamente con otros modelos de seguridad, es más fácil de seguir un solo modelo a lo largo del proceso de seguridad entero. Teniendo un modelo de seguridad separado para las tecnologías de la información porque pueden causar sólo confusión.

El Criterio Común se divide en tres grupos diferentes:

1. Consumidores - El grupo o persona que pone los requisitos para el nivel de seguridad de un recurso o sistema. Los consumidores dictan que nivel de seguridad es importante y usan el perfil de una protección desarrollando y usando un criterio común.

2. Diseñadores – Los diseñadores pueden usar el método del Criterio Común para certificar su recurso antes de soltarlo al público. Siguiendo una estandardización aceptada, o bien, una metodología de diseño de seguridad para un recurso o sistema.

3. Evaluadores - El criterio común proporciona normas que pueden usar los evaluadores cuando un nuevo recurso o el sistema está probándose. Usando estas normas se puede simplificar el proceso de la evaluación.

El método del criterio común es dividido en tres partes diferentes. Cada uno de los grupos mencionados tiene responsabilidades diferentes dentro de las partes. Las tres partes del modelo del criterio común son:

1. La introducción en esta parte del modelo de criterio común define el proceso involucrado evaluando la seguridad de los productos. También repasa el proceso y el idioma involucrado, Poniendo por escrito los requisitos de seguridad para los productos de tecnologías de la información.

2. La seguridad los requisitos funcionales. Esta parte se usa para construir el catálogo de requisitos de seguridad para un TOE especifico. Los Evaluadores usan este catálogo para probar un TOE.

3. Los requisitos de garantía de seguridad - Esta parte del proceso de la evaluación se usa para predefinir la convicción del criterio común y garantizar los niveles para clasificar un TOE.

La certificación del criterio común requiere que cada grupo cumpla los tres pasos en este proceso.

2.6.4 ISO 17799

Desde su publicación por parte de la Organización Internacional de Normas en diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

En diciembre de 2000, la Organización Internacional de Normas Técnicas (ISO) adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799. Alrededor de la misma época, se adoptó un medio formal de acreditación y certificación para cumplir con la norma técnica. La calidad total de la norma técnica ha mejorado considerablemente. La adopción por parte de ISO de la Parte 1 - los criterios de la norma técnica - de BS 7799 recibió gran aceptación por parte del sector internacional y fue en este momento que un grupo de normas técnicas de seguridad tuvo amplio reconocimiento. La norma ISO 17799 no incluye la segunda parte de BS 7799, que se refiere a la implementación. ISO 17799 hoy en día es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes.

La flexibilidad e imprecisión de ISO 17799 es intencional por cuanto es difícil contar con una norma que funcione en una variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 17799 simplemente ofrece un conjunto de reglas a un sector donde no existían.

Las diez áreas de control de ISO 17799:

- Política de seguridad: Se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.

- Organización de la seguridad: Sugiere diseñar una estructura de administración dentro la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

- Control y clasificación de los recursos de información: Necesita un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

- Seguridad del personal: Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe tener implementar un plan para reportar los incidentes.

- Seguridad física y ambiental: Responde a la necesidad de proteger las áreas, el equipo y los controles generales. Manejo de las comunicaciones y las operaciones: Los objetivos de esta sección son:

  a) Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

  b) Minimizar el riesgo de falla de los sistemas.

  c) Proteger la integridad del software y la información.

  d) Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.

  e) Garantizar la protección de la información en las redes y de la infraestructura de soporte.

  f) Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.

  g) Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

Control de acceso: Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

- Desarrollo y mantenimiento de los sistemas: Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

- Manejo de la continuidad de la empresa: Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

- Cumplimiento: Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne la Privacidad, la Ley de Responsabilidad y Transferibilidad del Seguro Médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Billey (GLBA por su sigla en inglés). Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoria del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

Beneficios de la norma técnica ISO 17799

Una empresa o centro de cómputo certificado con la norma técnica ISO 17799 puede ganar frente a los competidores no certificados. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa certificada. Además un centro de cómputo para cualquier empresa o institución certificado tendrá en cuenta lo siguiente:

- Mayor seguridad.
- Planeación y manejo de la seguridad más efectivos.
- Alianzas comerciales y e-commerce más seguras.
- Mayor confianza en los usuarios o clientes.
- Auditorías de seguridad más precisas y confiables.
- Menor Responsabilidad civil

La norma técnica ISO 17799

Actualmente ISO está revisando la norma técnica 17799 para que se adapte mejor a su amplio público. ISO 17799 es la primera norma técnica y se harán y ampliarán sus recomendaciones y sugerencias básicas en la medida en que sea necesario. Por ahora, ISO 17799 es la norma técnica a seguir.

Aunque no se haya adoptado un programa de protección definido de la información, es recomendable ISO 17799 ya que puede servir de parámetro para que lo defina en cualquier centro de cómputo que se necesite. También ISO 17799 ayuda a configurar la política de seguridad de centro de cómputo.

2.6.5 OCTAVE

El CERT/CC ha desarrollado un modelo de seguridad, OCTAVE, basado en las mejores prácticas de ISO 15048 y RFC 2196.

OCTAVE utiliza un acercamiento de tres partes para ayudar a guiar una organización a través del proceso de identificar y dirigir problemas de seguridad:

1. Construir Perfiles basados en la amenazas.
2. Identificar vulnerabilidades en la infraestructura.
3. Desarrollar estrategias de seguridad y planes.

OCTAVE se ha diseñado completamente para ser administrado internamente. CERT encontró que muchas organizaciones recurren a evaluaciones de seguridad de terceros. El problema con este método es que no se pueden evaluar los riesgos de seguridad adecuadamente. Cada organización requiere de una seguridad diferente, y depende de los recursos del site. La persona contratada para realizar un análisis de riesgo no puede identificar apropiadamente el núcleo de los recursos que podrían llevar al fracaso para protegerlos.

Antes de que usted despida a su consultor de seguridad, entienda que usando OCTAVE no niega la necesidad de consultores de seguridad, pero el acercamiento tiene que ser

diferente. De hecho, el método OCTAVE puede trabajar bien con consultores de seguridad, porque, estos pueden proporcionar áreas de especialización a su personal, que le puede estar faltando.

Los consultores de seguridad también pueden ayudar a guiar conversaciones, que es una parte íntegra del método OCTAVE. Esto es especialmente cierto al principio del proceso del método OCTAVE. Si su organización nunca ha intentado desarrollar un plan de seguridad, usted puede estar perdido en estas reuniones, y no poder identificar los recursos del site.

Es imprescindible un consultor de seguridad especialmente en la segunda fase de OCTAVE. Su personal no puede tener conocimiento adecuado de las vulnerabilidades potenciales en su infraestructura, y un consultor de seguridad puede ayudar en aquellos puntos, y recomienda arreglar esas vulnerabilidades.

2.6.5.1 El equipo del Site

Basándose en el método OCTAVE un equipo del site consiste de tres a cinco personas dependiendo del tamaño de la Unidad. Este equipo hará valoraciones de seguridad y guiará a través de los tres pasos del proceso OCTAVE.

Este equipo debe consistir en personas del site, así como de personas de varias secciones. No se esperará que el equipo del site tenga todas las respuestas, pero deben tener acceso a los recursos al necesitar encontrar esa información.

Ésta es la parte más importante de OCTAVE, o cualquier otro método de seguridad: apoyo por parte del jefe. Sin el apoyo del jefe cualquier modelo de seguridad fallará. La seguridad penetra todos los aspectos de una organización a través de medios que ayudan a cada sección lo requiere. Si las demandas de información no se originan por parte de la dirección general, ellos pueden darse una prioridad baja o pueden ignorarse. El equipo del site no necesita ser comprendido del todo por el jefe, pero el primer grupo que se informa debe contener miembros de la dirección para asegurarse de que el equipo tiene el apoyo completo y se discutirá brevemente todo con más detalle.

El equipo del site debe pasar por varios pasos durante el proceso de la evaluación de OCTAVE. Estos pasos generalmente corresponden con el acercamiento de tres partes del método OCTAVE y se usan para crear catálogos de prácticas y vulnerabilidades. De nuevo, estos pasos involucrarán a menudo a las personas fuera del equipo del site que puede proporcionar información o especialización en ciertas áreas.

2.6.5.2 Inicializando el Proceso

El primer paso, como se mencionó antes, es recibir patrocinio de la dirección. Pero si no se hace, es importante acercarse a la dirección para explicar el proceso y el porque de los pasos son necesarios, para asegurar una seguridad. El despliegue inicial de un modelo de seguridad puede tomar una cantidad considerable de tiempo. La dirección necesita entender esto, y tener preparados algunos de sus empleados para organizar a tiempo sus deberes regulares y apoyar esta parte.

2.6.5.3 Figuras de los perfiles las amenazas.

La primera fase de OCTAVE construirá perfiles de amenazas de los recursos. El grupo del site realiza reuniones de niveles diferentes para proveer de personal para identificar que recursos son críticos, y los impactos negativos deben ser corregido estos recursos.

Para el diseño hay reuniones por separado para cada nivel de la organización. De este modo separando los niveles, cada grupo estará más inclinado a hablar libremente, y no se detendrá por miedo a las represalias. La naturaleza del asunto dicta que las reuniones tienen que ser algo formales, pero las reuniones deben ser tan relajadas como sea posible para que los asistentes estén dispuestos a compartir la información.

Es importante que cada uno de los asistentes pueda contribuir a la discusión. Y asegúrese de que los asistentes que estén allí sean debido a su conocimiento o habilidades, y no solo porque están disponibles en cierto momento.

En cada reunión, los asistentes deben determinar lo que perciben para ser los recursos más valiosos de la organización. Los recursos pueden ser datos, gente, equipo, software, o cualquier cosa que tiene un valor tangible. El paso siguiente es alinear los recursos en orden de importancia. La importancia del recurso, en este caso, es relativa al impacto en la organización si se compromete.

Una vez que se hayan identificado y se hayan enlistado los recursos, el paso siguiente es identificar las amenazas a estos recursos. Una amenaza, en este caso, se define como cualquier acontecimiento indeseable que podría dar lugar a un compromiso de un recurso. Las amenazas se pueden basar en error humano (un ingeniero configura la mascara en un switch incorrectamente), o en la naturaleza (un tornado destruye su site de datos).

Cada recurso debe tener una lista de amenazas potenciales, así como los resultados posibles si se ejecuta esa amenaza. Hay que cerciórese de que las amenazas estén dentro de algo realistas. Mientras que un asteroide que choca en el site de datos sería indudablemente devastador, la probabilidad de que suceda, combinado con los costos exorbitantes implicados en la prevención, lo hace irrazonable enumerarlo como amenaza.

Si ha reunido los recursos y las amenazas asociadas, así como el impacto de esas amenazas. El paso siguiente es definir los requisitos de la seguridad para cada recurso. Hay tres pautas que necesitan ser utilizadas al crear los requisitos de seguridad: confidenciabilidad, integridad, y disponibilidad. Éstos son similares a las pautas usadas para desarrollar los requisitos de la seguridad para los datos en el modelo de criterios comunes.

La confidencialidad es el proceso de guardar la información que es privada y sensible lejos de cualquier persona que no deba tener acceso a ella. La integridad implica el asegurar que un recurso no sea deteriorado, o modificado de cualquier manera por alguien o un cierto proceso que no se autoriza. La disponibilidad es cuándo el personal a menudo autorizado alcanza un recurso.

Recurso	Amenazas	Resultado de Amenazas	Requerimientos de Seguridad
Lista de importancia de recursos	Amenaza para cada recurso	Panorama de cada escenario	Estándares mínimos de la seguridad

La tabla 2.1 enumera la matriz que se está desarrollando para cada recurso.

A este punto los recursos importantes se han identificado y se han enumerado las amenazas asociadas a esos recursos, y se han creado los requisitos de seguridad. Los requisitos de seguridad que se han enumerado para cada recurso se agregan a un catálogo de prácticas de seguridad que la organización debe esforzarse en seguir. Este catálogo de prácticas de seguridad debe ser la meta en la que tres partes del proceso de OCTAVE se estén esforzando por ayudar en la reunión de la organización.

El paso siguiente es identificar las prácticas actuales de seguridad para cada recurso. Estas prácticas se deben obtener usando exámenes anónimos en cada una de las reuniones de grupo. Es esencial obtener un cuadro exacto de seguridad actual practicado para cada recurso, incluso si se refleja gravemente en un departamento o un individuo. Cuando se hayan reunido las practicas de seguridad actual, es importante tranquilizar a las personas de que no habrá repercusiones negativas de los fracasos en el modelo actual de seguridad. Los empleados deben de poder proporcionar una comunicación honesta.

Enumerar las prácticas actuales hará a menudo que algunas de las vulnerabilidades de la seguridad lleguen a ser más evidentes. Aquellos que no son evidentes se deben todavía identificar dentro de otro examen. Las vulnerabilidades pueden incluir cosas como ejecutar código de funcionamiento del software más viejo en los ruteadores y los switchs, y no poner al día sistemas operativos con el servicio más último, malas políticas de contraseña, etc.. Las vulnerabilidades son diferentes tipos de amenazas de la manera en que se acercan a un problema de seguridad. Una amenaza sería un atacante que lanza un ataque de DOS contra su servidor de red; la vulnerabilidad estaría ejecutando una versión más vieja de su software de servidor de red que es susceptible a los ataques de DOS. El mapa de la evaluación de seguridad se muestra en la tabla 2.2.

Tenga presente que cada grupo tendrá su propio mapa, y los mapas representan las opiniones de cada grupo individual. Espere que los mapas de cada grupo sean muy diferentes, especialmente al comparar los resultados con la dirección y de las reuniones del personal. Las diferencias son porqué el grupo de la base es tan importante para este proceso. El grupo de la base tiene que evaluar las listas de cada uno de las reuniones y combinar la información para producir un mapa principal que identifica los recursos de la base de la organización y las amenazas percibidas así como los requisitos necesarios para asegurarse contra estas amenazas. Ahora, el grupo puede partir de la parte 2: Identificar vulnerabilidades de la infraestructura.

Evaluación de Seguridad					
Recursos	**Amenaza**	**Resultado de Amenaza**	**Requisitos de Seguridad**	**Prácticas Actuales de la Seguridad**	**Vulnerabilidades Conocidas de la Seguridad**
Lista de importancia de los recursos	Amenaza para cada recurso	Panorama de cada escenario	Estándares mínimos de la seguridad	Procedimientos actuales de la seguridad	Áreas donde la seguridad podría ser mejorada

Tabla 2.2. Evaluaciones de Seguridad

2.6.5.4 Identifique las vulnerabilidades de la infraestructura

La parte 2 del método de OCTAVE implica una evaluación comprensiva de la infraestructura de la tecnología para determinar qué medidas de seguridad adicionales necesitan ser tomadas en orden en el que satisfagan los requisitos de seguridad presentados en la parte 1 del proceso de la evaluación.

Algunos de los cambios en la infraestructura serán fáciles. Podran llevarse a cabo los cambios recomendados por los empleados en la parte 1 de la evaluación rápidamente. Lo que probablemente será más difícil es corregir las vulnerabilidades de seguridad de las cuales los miembros son inconscientes.

Las vulnerabilidades adicionales de determinación y que no fueron recolectadas durante la primera fase pueden involucrar a un consultor externo que se especialice en este tipo de trabajo.

OCTAVE agrupa vulnerabilidades de la seguridad en tres categorías:

1. Diseño -- una vulnerabilidad es un defecto basado en hardware, software, o un protocolo. Esto podría ser un agujero de la seguridad en un sistema operativo o un problema con la versión de una especificación, por ejemplo los defectos de seguridad encontrada en SSL 1.0.

2. Aplicación – Una vulnerabilidad es la manera en la que se está utilizando un sistema, no en cómo se despliega o se diseña.

1. Configuración -- las vulnerabilidades más comunes. Las vulnerabilidades de configuración provienen de errores administrativos: una mala contraseña, acceso inseguro del sistema, u otros errores.

Cada sistema dentro de su infraestructura tendrá muy probablemente vulnerabilidades múltiples que atraviesen las tres categorías. Para mantener las mejores prácticas mientras que prueba el sistema, OCTAVE requiere el uso de un catalogo establecido de vulnerabilidades.

2.6.5.5 CVE

El catálogo más popular de Vulnerabilidades Comunes y Exposiciones es el diccionario (CVE), patrocinado por el Mitre Corporation (cve.inglete.org). CVE es utilizado por muchas organizaciones a manera de estandaridizar vulnerabilidades a través de plataformas múltiples. Más bien actúa como una base de datos o depósito (similar a BugTraq) de la información, CVE proporciona a convención de nombramiento estándar a las vulnerabilidades.

Otras organizaciones que apoyan el uso de CVE usan los nombres definidos dentro de CVE en sus productos. De una perspectiva del usuario final, esto significa que todos los dispositivos que son CVE vulnerables se enumerarán en CVE-2001-0494 como problema de desbordamiento del resguardo intermedio con el servidor de smtp de IPSwitch.

Los sistemas de diccionario, por ejemplo CVE, proporcionan una herramienta valiosa a los administradores de red porque hacen más fácil determinar qué vulnerabilidades detectará una herramienta del sistema de detección de intrusión(identificaciones). La desventaja a las herramientas como CVE es, porque intenta ser hilo neutro del vendedor, los incidentes que se agregan a la base de datos de CVE son determinados por un grupo de expertos de la industria. Esto puede significar que la base de datos oficial de CVE puede retrasarse varios meses detrás del informe de un incidente de seguridad.

Afortunadamente, CVE también provee una lista de incidente a incluir en la base de datos. Estos incidentes no se han agregado oficialmente, pero muchos vendedores de CVE los incluirán en sus herramientas en un esfuerzo de ser tan completos como sea posible. Los son distinguidos por palabras reales por sus títulos. Una palabra incluye las letras CVE, seguidas por el año, y el número del incidente. Los incidentes tienen el formato de letras, seguido por el año y el número del incidente. El incidente CAN-2002-0085 describe una hazaña potencial de Apache que implica PHP, que fue divulgado en febrero de 2002.

Antes de que pueda ser listado en el diccionario tiene que recibir bastantes votos de aceptación de los miembros del tablero de CVE, e informar a detalle sobre el incidente, y que esté disponible con cada listado.

Una amplia gama de herramientas para las identificaciones IDS utiliza el sistema CVE. Las herramientas que utilizan CVE incluyen VLAN el explorador, un explorador abierto de la fuente disponible de BindView, e identificaciones de Cisco IDS (conocidas antes como NetRanger). El Web site de CVE enumera más de 1.600 sistemas que utilizan el diccionario de CVE.

2.6.5.6 Evaluando los resultados

Usando cualquier diccionario o sistema IDS se puede sentir confiado en analizar su sistema crítico de tecnologías de la información.

Cuando el análisis es completo, otra reunión necesita ser celebrada con el grupo de base y personal de tecnologías de la información. Los resultados de la prueba se deben analizar y poner en tres grupos separados:

1. Vulnerabilidades fuera de la organización.
2. Vulnerabilidades dentro de la organización.
3. Vulnerabilidades en cada sistema.

Cada vulnerabilidad se debe revisar, dentro del contexto de su grupo, por el personal IT antes de pasar a la parte 3 de la evaluación de OCTAVE.

2.6.5.7 Evalúe la estrategia y los planes de seguridad

En la parte 1 y 2 de la evaluación de OCTAVE el equipo de base, ha construido una base de datos de recursos críticos, amenazas para esos recursos, y vulnerabilidades.

La meta de la parte 3 de la evaluación de OCTAVE es determinar cómo reducir riesgo a los recursos críticos.

Un riesgo, en esta situación, se define como amenaza combinada con el impacto, si esa amenaza se realiza contra un recurso crítico. El riesgo se puede definir como valor cualitativo o cuantitativo; OCTAVE se centra en el aspecto cualitativo de la evaluación del riesgo.

Antes de decidir cómo responder a los riesgos que emergieron de la parte 1 y 2 de la evaluación de OCTAVE, se debe dirigir un análisis de riesgo. Hay tres pasos involucrados en el proceso de análisis de riesgo de OCTAVE.

1. Examine las amenazas a los recursos juzgados como críticos. Cada amenaza se debe evaluar en los términos del impacto de las vulnerabilidades que afectan confidencialidad del recurso, integridad, y disponibilidad. Esto crea un perfil de riesgo para cada amenaza.

2. Cree una prueba patrón contra la cual cada perfil del riesgo pueda ser examinado. La prueba patrón debe consistir en valores cualitativos simples, como por ejemplo: alto, medio, y bajo, eso se puede asignar a cada perfil.

3. Asigne los valores creados en la fase de la prueba patrón a cada perfil.

Esto es hecho por el equipo base.

Después de que a cada perfil de riesgo se le ha asignado un valor, hay tres posibles resoluciones a las vulnerabilidades:

1. Desarrolle las nuevas prácticas de seguridad.

2. Continúe manteniendo prácticas actuales de seguridad.

3. Arregle vulnerabilidades identificadas, sin que cambien las prácticas existentes de seguridad.

El grupo base, trabaja conjuntamente con los departamentos afectados y la tecnología de la información, y desarrolla una lista de los pasos que se tomarán para tratar las amenazas, o políticas existentes que requieren de cambio. Como con los otros pasos en la evaluación de OCTAVE, esto requiere la implicación de la dirección asegurándose de que todos los departamentos sean cooperativos en este proceso.

Una evaluación de OCTAVE no es un fenómeno de una sola vez. Debe ser realizado continuamente a través del año. La evaluación inicial de OCTAVE puede causar una cierta confusión pues los empleados pueden no ser acostumbrados a este tipo de metodología de seguridad. Sin embargo, cuando los empleados se acostumbran a él, comenzará a tener sentido, y las evaluaciones subsecuentes llegarán a ser más rápidas y más fáciles.

También proporcionara una manera de llegar a ser más pro-activa respecto a problemas de seguridad.

El involucramiento del empleado es un aspecto crítico en las evaluaciones de OCTAVE. Por otra parte actualizaciones del código y protocolos de seguridad no son suficientes para crear una política de seguridad eficaz. Los empleados deben estar dispuestos a participar completamente. Esta es la razón por la cual las reuniones son una parte tan importante del método de OCTAVE. Las reuniones permiten que los empleados den su opinión en las políticas de seguridad, así como dar al grupo base una oportunidad de explicar porqué se están tomando las medidas de seguridad y cuál será el resultado final del proceso.
Proporcionando a sus empleados tanta información sobre el proceso como sea posible, usted construirá una política más fuerte y más eficaz de seguridad.

En esta parte del capitulo nos enfocaremos mas al modelo Octave ya que es en el que nos basaremos para implementar este tema de tesis.

2.7 Modelo Octave

Este documento describe (The Operationslly Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)), un acercamiento para el manejo de los riesgos de seguridad de la información. Presenta la descripción del acercamiento de OCTAVE y describe brevemente y conciso dos métodos de OCTAVE, convertido en el instituto de la tecnología de dotación lógica (SEI).

El acercamiento total incorpora primero la descripción de OCTAVE, seguida por una descripción general de los dos métodos: el método de OCTAVE para las organizaciones grandes y OCTAVE-S para organizaciones pequeñas. La información se proporciona para asistir al lector en distinguir entre los dos métodos, incluyendo las características que

definen las tarjetas para cada método, así como cualquier obligación y limitación de cada método. Una serie de preguntas también se proporciona para ayudar a lectores a determinar qué método es el mejor. Entonces dirigen a los lectores al Sitio Web para descargar el método de su elección. Se debe percatar de que algunas organizaciones pueden necesitar un solo método o una combinación de ambos, o una versión totalmente diversa de OCTAVE.

2.7.1 Descripción

Una evaluación eficaz de riesgo de seguridad de la información que considera a ambos, la edición organizacional y tecnológica, examina cómo la gente utiliza la infraestructura de cómputo diariamente. La evaluación es de vital importancia para cualquier iniciativa de mejorar la seguridad, porque, genera una visión más amplia en cuanto a los riesgos de seguridad de la información, abasteciendo una línea de fondo para mejorar.

2.7.2 OCTAVE

Para entender las necesidades de seguridad de información, OCTAVE esta basada en riesgos, la técnica estratégica de la evaluación y la planificación para la seguridad. OCTAVE es autodirigida, significa que la gente asume la responsabilidad de poner estrategias de seguridad. La técnica provee al personal del conocimiento de su organización, las prácticas de seguridad relacionan los procesos para capturar el estado actual de seguridad. Los riesgos a los recursos más críticos se utilizan para dar prioridad a esas áreas de mejora y fijar la estrategia de la seguridad.

A diferencia de la evaluación típica enfocada a la tecnología, la cual se concentra en el riesgo tecnológico y enfocada en cuestiones tácticas, OCTAVE se concentra en el riesgo organizativo y se enfoca en cuestiones estratégicas, relacionadas con la práctica. Esto es una evaluación flexible que puede ser adaptada para la mayor parte de las organizaciones. Aplicando OCTAVE, un pequeño equipo de gente de la unidad operacional (o negocios) y del departamento de tecnología de información (IT) tienen que trabajar juntos para dirigirse a las necesidades de seguridad, equilibrando los tres aspectos claves ilustrados en la figura 2.2 riesgo operacional, prácticas de seguridad, y tecnología.

El enfoque de OCTAVE es manejado por dos de los aspectos: las prácticas operacionales del riesgo y la seguridad. La tecnología es examinada sólo con relación a prácticas de seguridad, permitiendo refinar la vista de sus prácticas actuales de seguridad. Usando el enfoque de OCTAVE, se toman decisiones de protección de información basadas en riesgos a la confidencialidad, a la integridad, y disponibilidad de los recursos críticos relacionados con la información. Todos los aspectos del riesgo (recursos, amenazas, vulnerabilidades, e impacto organizativo) son factores en la toma de decisiones, permitiendo emparejar una estrategia de protección basada en la práctica de riesgos a la seguridad. La tabla 2.3 resume diferencias claves entre OCTAVE y otras evaluaciones.

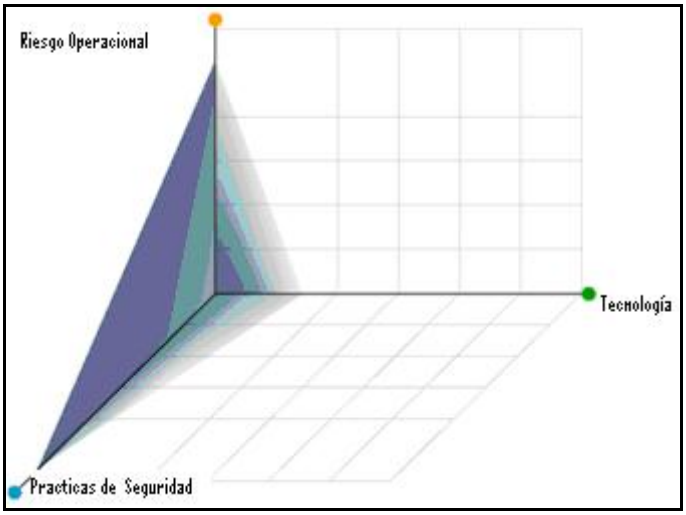


Figura 2.3 OCTAVE equilibra tres aspectos

OCTAVES	OTRAS EVALUACIONES
Evaluacion Organizacional	Evaluación del Sistema
Enfoque en Practicas de Seguridad	Enfoque en la Tecnología
Emisiones Estrategicas	Emisiones del Sistema
Autodireccionamiento	Experto Conducido

Tabla 2.3 Diferencias entre claves de OCTAVE y otros enfoques

2.7.3 Características claves del enfoque de OCTAVE.

OCTAVE es auto dirigido, requiere que se trate de manejar el proceso de evaluación y tome decisiones de información. Un equipo interdisciplinario, llamado equipo de análisis, conduce la evaluación. El equipo incluye a la gente tanto de las unidades comerciales como del departamento IT porque ambas perspectivas son importantes al caracterizar la vista global del riesgo para la seguridad de la información. OCTAVE es un enfoque que maneja las ventajas de la evaluación.

- Identifica los recursos relacionados con la información (p.ej, información y sistemas) que son importantes.

- Enfoca actividades de análisis de riesgo en aquellos recursos juzgados más críticos.

- Considera las relaciones entre los recursos críticos, las amenazas para aquellos recursos, y vulnerabilidades (tanto organizativas como tecnológicas) que pueden exponer los recursos.

Introducción OCTAVE

• Evalúa riesgos en un contexto operacional como aquellos que son utilizados para guiar el negocio y como estos recursos están en peligro debido a amenazas de seguridad.

• Crea una estrategia de protección basada en la práctica para la mejora de la organización, así como los planes de mitigación de riesgo para reducir el riesgo de los recursos críticos.

Lo organizativo, tecnológico, y los aspectos de análisis de una evaluación de riesgo a la seguridad de información son complementados por un enfoque de tres fases. OCTAVE se organiza alrededor de estos tres aspectos básicos (ilustrados en la Figura 2.4), permitiendo al personal organizativo reunir un cuadro completo de las necesidades de seguridad de información. Las fases son

• Fase 1: Construye perfiles de amenaza a basados en los recursos – Esta es una evaluación organizativa. El equipo de análisis determina lo que es importante (recursos relacionados con la información) y lo que está siendo actualmente utilizado para proteger aquellos recursos. El equipo entonces selecciona aquellos recursos que son los más importantes (recursos críticos) y describe exigencias de seguridad para cada recurso crítico. Finalmente, esto identifica amenazas para cada recurso crítico, creando un perfil de amenaza para aquel recurso.

• Fase 2: Identifica vulnerabilidades de la Infraestructura – Esta es una evaluación de la infraestructura de información. El equipo de análisis examina caminos de acceso de red, identificando clases de componentes de tecnología de información relacionados con cada recurso crítico. El equipo entonces determina el grado al cual cada clase del componente es resistente para conectar una red de ataques.

• Fase 3: Desarrolla estrategias de seguridad y proyectos – Durante esta parte de la evaluación, el equipo de análisis identifica riesgos a los recursos críticos y decide que hacer sobre ellos. El equipo crea una estrategia de protección y la mitigación planea dirigirse a los riesgos de los recursos críticos, basados sobre un análisis de información recabada.

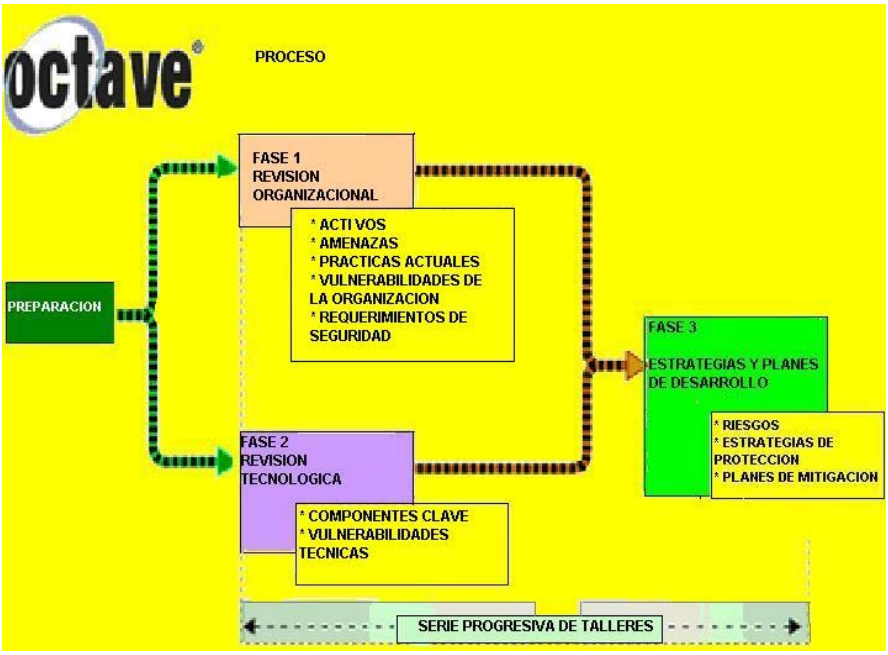


Figura 2.4 Fases de OCTAVE

2.7.4 Criterios de OCTAVE

Los elementos esenciales, o las exigencias, del enfoque de OCTAVE se han personificado en un conjunto de criterios [Alberts 01b]. Pueden haber muchos métodos consecuentes con estos criterios, pero hay sólo un conjunto de criterios de OCTAVE. En este momento, hay dos métodos consecuentes con los criterios que han sido desarrollados.

El Método de OCTAVE, documentado en la Guía de la Implementación del Método de OCTAVE, v2.0 [Alberts 01a], fue diseñado para organizaciones grandes en mente, mientras OCTAVE-S fue desarrollado para pequeñas organizaciones. Además, los otros podrían definir métodos para contextos específicos que son consecuentes con los criterios. La figura 2.5 ilustra estos puntos.

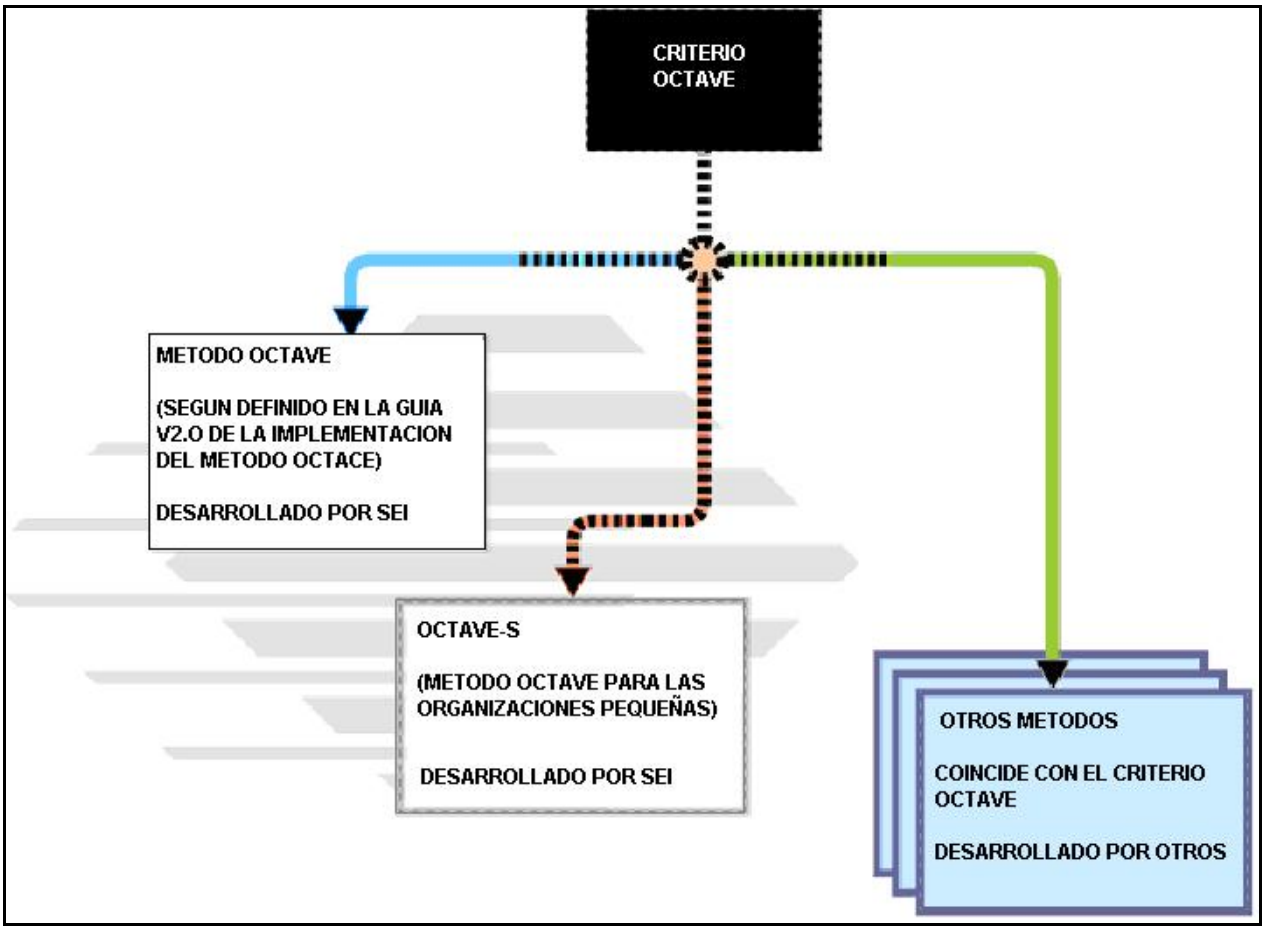


Figura 2.5 Los Criterios de OCTAVE sostienen múltiples implementaciones.

Los criterios de OCTAVE son un conjunto de principios, atributos, y producciones.

Los principios son los conceptos fundamentales que conducen la naturaleza de la evaluación, y definición de la filosofía detrás del proceso de evaluación. Ellos forman el enfoque de la evaluación y proporcionan la base para el proceso de evaluación. Por ejemplo, el auto - direccionamiento, es uno de los principios de OCTAVE.

El concepto de auto direccionamiento significa que la gente está en la mejor posición para dirigir la evaluación y tomar decisiones.

Las exigencias de la evaluación son incorporadas en los atributos y las producciones. Los atributos son las calidades distintivas, o características, de la evaluación. Ellas son las exigencias que definen los elementos básicos de OCTAVE se acercan y definen lo que es necesario para hacer la evaluación con éxito tanto del proceso como de perspectivas organizativas. Los atributos se derivan de los principios de OCTAVE. Por ejemplo, uno de los atributos de OCTAVE es que un equipo interdisciplinario (el equipo de análisis) proveído por el personal dirige la evaluación. El principio detrás de la creación de un equipo de análisis es la auto dirección.

Finalmente, las producciones son los resultados requeridos de cada fase de la evaluación. Ellos definen los resultados que un equipo de análisis debe conseguir durante cada fase. Hay más de un conjunto de actividades que pueden producir las salidas de OCTAVE; por esta razón, un conjunto único de actividades no es especificado.

Las producciones definen los resultados que un equipo de análisis debe conseguir durante la evaluación y es organizado según las tres fases. Las tablas 2.4 y 2.5 ponen los principios en una lista de las actividades, y salidas del acercamiento de OCTAVE.

PRINCIPIOS	ATRIBUTOS
AUTO DIRECCIONAMIENTO	RA.1 EQUIPO DE ANÁLISIS RA.2 AUMENTAR HABILIDADES DEL EQUIPO DE ANÁLISIS
MEDIDAS ADAPTABLES	RA.3 CATALOGO DE PRACTICAS RA.4 PERFIL GENÉRICO DE LA AMENAZA RA. 5 CATALOGO DE VULNERABILIDADES
PROCESO DEFINIDO	RA. 6 ACTIVIDADES DEFINIDAS DE LA EVALUACIÓN RA. 7 RESULTADOS DOCUMENTADOS DE LA EVALUACIÓN RA. 8 ALCANCE DE LA EVALUACIÓN
FUNDACIÓN PARA UN PROCESO CONTINUO	RA. 9 PASOS SIGUIENTES RA. 3 CATALOGO DE PRACTICAS
REVISIÓN	RA. 10 ENFOQUE DE RIESGOS
ENFOQUE MÍNIMO	RA. 8 ALCANCE DE LA EVALUACIÓN RA. 11 ACTIVIDADES ENFOCADAS
GERENCIA INTEGRADA	RA. 12 EDICIONES DE ORGANIZACIÓN Y DE TECNOLOGÍA RA. 13 PARTICIPACIÓN DE LA TECNOLOGÍA DEL NEGOCIO Y DE LA INFORMACIÓN RA.14 PARTICIPACIÓN DE LA GERENCIA GENERAL
COMUNICACIÓN ABIERTA	RA. 15 ACERCAMIENTO DE COLABORACIÓN
PERSPECTIVA GLOBAL	RA. 12 EDICIÓN DE ORGANIZACIÓN Y DE TECNOLOGÍA RA. 13 PARTICIPACIÓN DE LA TECNOLOGÍA DEL NEGOCIO Y DE LA INFORMACIÓN

Tabla 2.4 Principios de OCTAVE y Atributos

FASES	RESULTADOS
FASE 1	RO1.1 ACTIVOS CRÍTICOS RO1.2 REQUISITOS DE SEGURIDAD PARA LOS ACTIVOS CRÍTICOS RO1.3 AMENAZAS PARA LOS ACTIVOS CRÍTICOS RO1.4 PRACTICAS ACTUALES DE SEGURIDAD RO1.5 VULNERABILIDADES ACTUALES DE LA ORGANIZACIÓN
FASE 2	RO2.1 COMPONENTES DOMINANTES RO2.2 VULNERABILIDADES DE LA TECNOLOGÍA ACTUAL
FASE 3	RO3.1 RIESGOS PARA LOS ACTIVOS CRÍTICOS RO3.2 MEDIDAS DEL RIESGO RO3.3 ESTRATEGIAS DE PROTECCIÓN RO3.4 PLANES DE LA MITIGACIÓN DEL RIESGO

Tabla 2.5 Resultados OCTAVE

2.7.5 OCTAVE es parte de una serie continua

OCTAVE crea una panorámica de los riesgos de seguridad actual de información, proporcionando una fotografía en el tiempo, o una línea de fondo, que puede ser utilizada para enfocar actividades de mejora y mitigación. Con OCTAVE, un equipo de análisis realiza las siguientes actividades

• Identifica los riesgos de seguridad de información.

• Analiza los riesgos para determinar las prioridades

• Plan para mejorar y desarrollar una estrategia de protección y planes de mitigación de riesgo para reducir el riesgo de los recursos críticos.

Uno no mejorará a menos que esto ponga en práctica sus proyectos. Las actividades de mejora siguientes son realizadas después de que OCTAVE ha sido completada. Después de OCTAVE, el equipo de análisis, u otro personal designado.

Introducción al acercamiento de OCTAVE Agosto 2003

• Plan como poner en práctica la estrategia de protección y proyectos de mitigación de riesgo desarrollando proyectos de acción detallados (Esta actividad puede incluir un análisis detallado de costo-beneficio entre estrategias y acciones, y tiene como resultado los planes detallados de la implementación.)

• Pone en práctica los planes detallados de la acción.

• Controla los planes de la acción para el horario y para la eficacia (Esta actividad incluye los riesgos que controlan cualquier cambio)

• Variaciones de control en ejecución del plan tomando acciones apropiadas correctivas. Una evaluación de riesgo para la seguridad de la información forma parte de las actividades para manejar riesgos de seguridad de información. OCTAVE es una actividad de evaluación, no es un proceso continuo. Así, esto tiene un principio definido y un final. La figura 2.6 muestra la relación entre estas actividades y donde queda OCTAVE. Note que las actividades de dirección de riesgo definen un ciclo "un plan que comprueba realmente el acto".

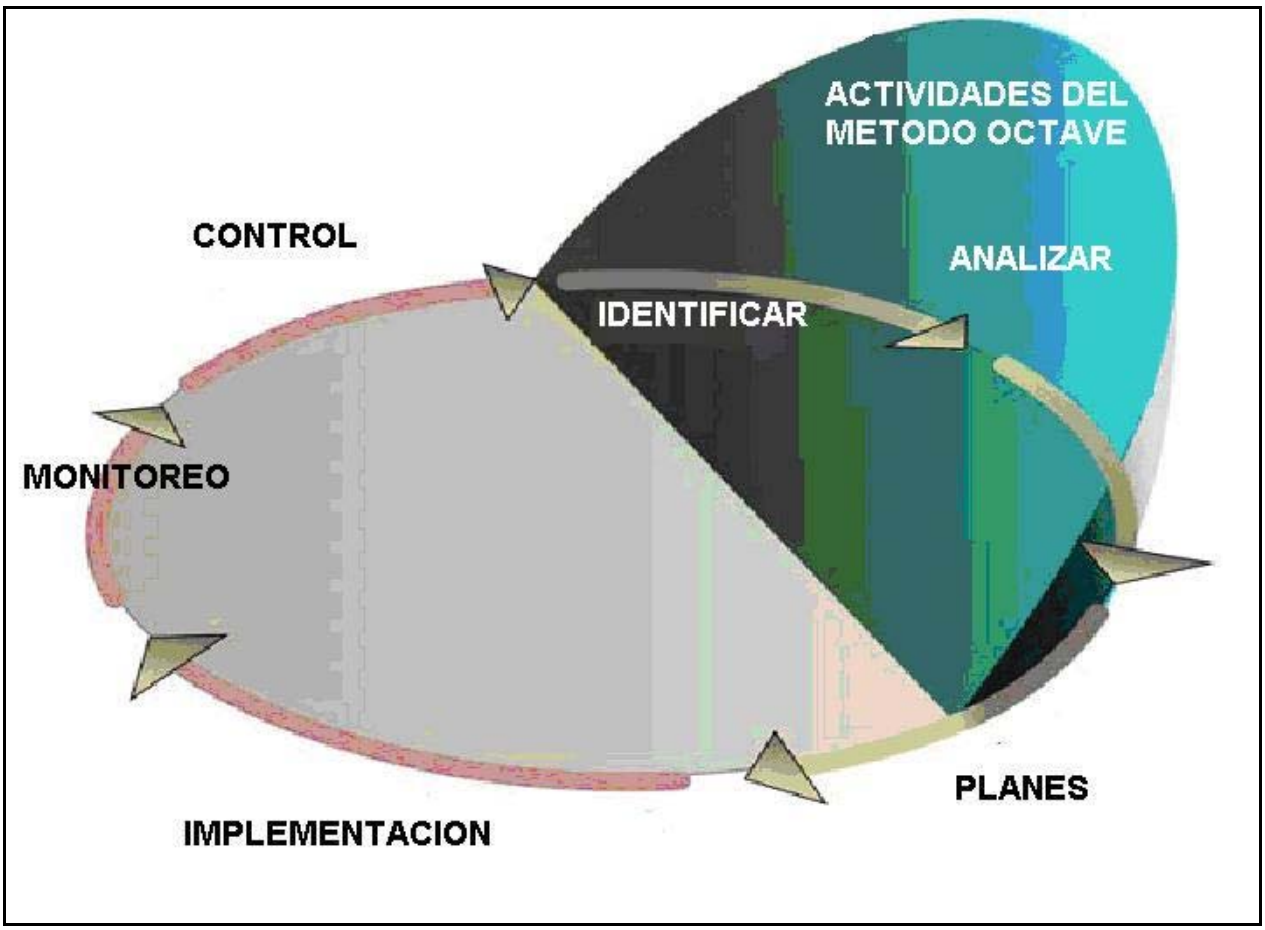


Figura 2.6 OCTAVE y las actividades de dirección de riesgo periódicas.

Se tendrá que "reinicializar" su línea de fondo conduciendo a otro OCTAVE. El tiempo entre evaluaciones puede ser predeterminado (por ejemplo, cada año) o provocado por los acontecimientos principales.

Entre evaluaciones, se puede identificar periódicamente nuevos riesgos, analizar estos riesgos con relación a riesgos existentes, y desarrollar proyectos de mitigación para ellos.

El Método OCTAVE fue desarrollado para organizaciones grandes en mente (p.ej, 300 empleados o más). El tamaño no es la única consideración decidiendo utilizar el Método OCTAVE. Las organizaciones grandes generalmente tienen una jerarquía multicapas y son a menudo desordenadas (desarticuladas) o geográficamente distribuidas. Las actividades de recopilación de datos formales para determinar que recursos relacionados con la información son importantes, como son usados, y como son amenazados se hacen una parte esencial de conducir OCTAVE en organizaciones grandes.

Escoger Entre los Métodos OCTAVE Y OCTAVE-S

El Método de OCTAVE se estructura para un equipo de análisis con alguna protección de IT y de asuntos de seguridad, empleándose abiertamente, poniendo en común el enfoque para reunir y analizar la información.

Por otra parte, OCTAVE-S es más estructurado. Los conceptos de seguridad son enfocados en hojas de trabajo de OCTAVE-S, teniendo en cuenta su uso por practicantes menos experimentados.

El enfoque de este tema estará basado en el modelo OCTAVE (Operación de Amenaza Crítica, Recurso, y Evaluación de Vulnerabilidad). El CERT/CC se creó en 1988 por la Defensa Agencia de Proyectos Avanzados de Investigación (DARPA) para tratar con emergencia la seguridad relacionadas con computadoras. El CERT/CC creció rápidamente, y hoy disemina información sobre los problemas de seguridad potenciales a lo largo del Internet.

OCTAVE es escogido como un modelo de ejemplo a seguir, porque fue diseñado para integrarse con cualquier modelo de seguridad existente. Porque la seguridad de la red tiene que ser un subconjunto de un modelo de seguridad más grande, necesitará un modelo que haga este tipo de integraciones sin costura de la integración, y sin dolor.

OCTAVE no es el único modelo de seguridad que se integra bien con otros modelos; hay muchos de hecho. Sin embargo, el hecho que es mantenido por CERT/CC presta mucho peso a su integridad y a la calidad de su plan.

CAPÍTULO 3

SEGURIDAD FÍSICA

3.1 Seguridad Física

Para lograr una protección total de la información, deben tomarse en cuenta dos aspectos básicos de los sistemas: el aspecto físico y el aspecto lógico. El primero abarca las condiciones de seguridad de los centros de cómputo, de los laboratorios de desarrollo y de las oficinas en donde se encuentran instalados en los equipos.

Las instalaciones del centro de cómputo son áreas restringidas internas, ya que se mantienen controles de acceso físico adicionales por la importancia del trabajo que se desarrolla y la información que alberga, Se mencionarán aquellas características y medidas que se deben de tomar en cuenta para garantizar la seguridad física de cualquier centro de cómputo, siendo su objetivo principal mantener la operación normal de los servicios en todo momento; que se podrían ver afectados como consecuencia de ataques deliberados o agresiones naturales.

Es necesario planear, desde la ubicación del equipo de cómputo, la instalación de la red de energía eléctrica y el aire acondicionado, hasta el control de acceso a bancos de datos y la prevención de los posibles daños causados por los fenómenos naturales. A continuación se explican algunos puntos importantes que deben ser tomados en cuenta para procurar el buen uso y funcionamiento de los sistemas de cómputo.

3.2 Ubicación del centro de cómputo

Para determinar correctamente la ubicación del centro de cómputo deben contemplarse varios aspectos: como son la facilidad de acceso al centro de computo, la correcta comunicación entre sus áreas (área de impresora, área de cintas, de consolas, etc.), los probables intentos de daño o robo, la ventilación del centro y la iluminación.

Para la ubicación de los centros de cómputo se prefieren zonas poco transitadas o poco concurridas, de manera que el tráfico es limitado y fácilmente controlado. La entrada debe estar alejada del acceso común al edificio, esto nos dará la posibilidad de proteger de mejor manera a todo el equipo. Este acceso puede funcionar también como entrada y salida para equipos de cómputo, con lo cual se pueda centralizar en un solo punto la entrada y la salida del centro. En caso de que el flujo de personas sea excesivo, el control de la entrada equipos deberá llevarse en una puerta diferente a la usada por los usuarios.

Debido a la existencia de atentados terroristas en algunos países, un laboratorio de cómputo no debe estar junto a áreas públicas como centro comercial, restaurantes o estacionamientos, ya que esto facilitaría cualquier tipo de ataque. En estos caso, si el centro de computo es muy grande y procesa mucha información importante, se recomienda ubicarlo en una localidad lo mas alejada posible de los centros urbanos, aun separada de las oficinas centrales de la compañía.

Las zonas industriales son particularmente inadecuadas para el uso de sistemas electrónicos a las variaciones en el suministro de energía eléctrica que produce la maquinaria y equipos instalados en las fábricas y talleres de estos lugares. Las altas y bajas del voltaje pueden dañar muy seriamente los equipos de cómputo y sus dispositivos periféricos, ya que estos contienen microcircuitos que son afectados por campos magnéticos muy intensos o descargas de energía.

Deben evitarse también los sótanos ya que ahí se pueden generar inundaciones que provoquen severos daños a todo nuestro equipo. En caso de tener que ubicar el centro de cómputo en una planta baja o sótano, conviene verificar que el piso falso cuente con las condiciones suficientes para evitar cualquier problema generado por lluvias o fugas de

agua. Cabe señalar que el uso del cableado adecuado para este tipo de centros es un punto fundamental para evitar accidentes.

La protección externa para nuestro centro de cómputo debe incluir bardas, muros, vigilantes, rejas, puertas y canceles. El diseño de estas protecciones deberá estar a cargo de personal especializado que determine la mejor ubicación y disposición de estos medios de seguridad con los cuales resguardaremos nuestra información y equipos.

Por supuesto, la inversión destinada a estos medios de seguridad dependerá del tamaño e importancia de nuestro servicio de cómputo: a mayor valor de nuestra información, sistemas y equipos corresponde una mayor protección. No será lo mismo invertir en la seguridad de tres o cuatro computadoras personales utilizadas por tres personas, que invertir en la protección de un laboratorio para 30 usuarios con cinco servidores de red, 10 servidores de impresión y cuatro antenas de telecomunicaciones.

En la mayoría de los casos, las instalaciones de cómputo y los departamentos de sistemas se encuentran ubicados dentro de las mismas oficinas generales de las empresas, y por lo tanto, se tiene una continua interacción con el personal de otras áreas. El tipo de protección en estos casos, puede implementarse a través del control de acceso mediante puertas de tarjeta, bitácoras de entrada y salida y una ubicación estratégica del centro de cómputo de manera que se eviten cruces de información o cruces de personal innecesarios. De igual manera, dentro del mismo centro de cómputo es conveniente crear divisiones por área de forma que se tenga un perfecto control de entrada/salida y actividad en cada zona.

Además debemos de realizar las siguientes consideraciones para elegir el lugar donde se establecerá un centro de cómputo:

- Suelo sólido. No deben de existir túneles o drenajes principales de la localidad en el subsuelo.

- Facilidad de acceso. Se refiere al tiempo, distancia, tipo de transporte y las vías de acceso para llegar al lugar de las instalaciones.

- Necesidad de espacio. En este punto se debe garantizar la cantidad de espacio suficiente para la construcción del centro de cómputo, además de considerar futuras ampliaciones.

- Alimentación de energía eléctrica. Es decir la disponibilidad de energía frecuencia de sobrecargas y descargas de voltaje, así como ausencia total de energía.

- Líneas Telefónicas. Considerar la disponibilidad de líneas, así como la prestación de servicios por parte de la compañía telefónica.

- Empresas Vecinas. Conocer el giro o actividad de las empresas circunvecinas, ya que éstas pueden emitir sustancias muy contaminantes y pequeñas, o ser muy riesgosas.

- Índice de fenómenos naturales. Como terremotos, incendios inundaciones o huracanes.

3.3 Construcción

El diseño y edificación del centro de cómputo debe ser cuidadosamente planeado. Básicamente se refiere a los tipos de materiales que se utilizarán para la edificación del centro de cómputo así como algunas características de ingeniería, donde se deberán considerar los siguientes puntos:

- Capacidad de carga del suelo.
- Sistema de drenaje en el suelo real.
- Edificación de una construcción sólida y resistente.
- Altura libre entre el suelo y el techo.
- Extensión de la pared entre el piso y el techo falso para evitar comunicación entre cuartos.
- Resistencia de los materiales.
- Instalaciones eléctricas.
- Instalaciones telefónicas.
- Utilización de material incombustible en piso, techo paredes.
- Número de entradas y salidas.
- Puertas de emergencia controladas por “crash bars” las cuales solo pueden ser usadas por dentro.
- División de centro de cómputo en cuarto de impresión, cintoteca, almacén de papelería, área de consolas, área de cpu’s y otros dispositivos.
- Utilización de alarmas contra fuego e incursión no autorizada.
- Cuarto de vigilancia
- Vigilancia del exterior e interior a través de circuito cerrado de tv.
- Área de backup alejada al menos 100 metros de distancia del computador central.

3.4 Interrupción del suministro eléctrico y variaciones del voltaje

Las variaciones de voltaje se refieren a los incrementos o decrementos de energía o la pérdida total de ésta. Se debe considerar el uso de reguladores que protegen el hardware de incrementos eventuales en el voltaje, a fin de que éste no se dañe.

Las consecuencias de las irregularidades en el suministro de energía eléctrica suelen ser muy costosas sino se cuentan con plantas eléctricas auxiliares o con equipos de fuente ininterrumpible de energía, también conocidos como UPS (Uninterruptable Power Sources).

Sino que comúnmente decimos, "se va la luz" y los equipos de procesamiento de datos no se encuentran conectados a sistemas no-break(sistemas auxiliares de energía) puede ser que el sistema operativo no provea un mecanismo de seguridad para estos casos (MSDOS y Windows 95, por ejemplo) y se pierda la información de los archivos que se encontraban abiertos en ese momento. Hay casos en los que las tormentas eléctricas o la puesta en marcha de generadores producen alteraciones en la señal eléctrica, misma que presentan picos (altas y bajas en la señal) que dañan las fuentes de las computadoras, los microprocesadores, memorias y, en general, todos los circuitos integrados que contienen. Estos imprevistos originan la paralización de los equipos de Cómputo y la pérdida de la información cargada en memoria de acceso aleatorio por todo lo anterior:

- Es recomendable el uso de equipos UPS. Estos equipos funcionan con baterías o pilas que entran en actividad cuando se detecta el corte del suministro primario de energía. Su tiempo de duración es variable y éste debe ser él suficiente para cerrar todos los archivos abiertos y dar de baja los servidores de manera regular y segura. Para saber cual es el

equipo auxiliar de energía adecuado para cada centro de cómputo, deberá tomarse en cuenta el consumo eléctrico de los equipos de cómputo, del aire acondicionado, así como de los sistemas de telecomunicaciones instalados.

- Si no se cuenta con presupuesto para equipos UPS, existe software con opciones de "auto-guardado" que ejecutan escrituras a disco de manera periódica, lo cual hace que la información en los dispositivos de almacenamiento se este actualizando constantemente y, en caso de que ocurriera una variación o corte de energía imprevisto, la perdida de información sería mínima.

- Para aminorar el riesgo de descargas eléctricas y picos en el suministro de energía, deberá existir un sistema pararrayos que garantice que toda carga eléctrica atmosférica sea conducida a tierra sin causar daño a los equipos. Estos pararrayos de tierra física se construyen comúnmente con el uso de varillas metálicas enterradas muy profundamente en el terreno. La punta del pararrayos llevará la descarga a estas varillas, las cuales se encargaran de dispersar su carga eléctrica a tierra. Conviene además que todas las líneas de tierra de las conexiones trifásicas estén conectadas a este punto de tierra física, de manera que se tenga una tierra común. Así no generará diferencias de potencial entre las propias tierras, y se evitaran problemas con la fuente de energía.

- Los supresores de picos y reguladores de voltaje son buenos métodos para mantener la señal eléctrica dentro de un determinado rango de variación que no exceda de los umbrales máximo y mínimo, dentro de los cuales nuestros equipos operan normalmente. Los reguladores son impredecibles para todo equipo de cómputo, desde computadoras personales hasta estaciones de trabajo. Si trabajamos en una zona en la que el flujo de energía eléctrica no es muy estable, estos equipos de regulación evitaran cualquier daño a los circuitos de las computadoras y sus periféricos.

3.5 Temperaturas para el equipo.

Los equipos de cómputo son equipos muy sofisticados que requieren condiciones de temperatura adecuadas para su buen funcionamiento. Las altas y bajas temperaturas causan daños a los dispositivos electrónicos y magnéticos de las computadoras y sus periféricos. Estos daños van desde la alteración de la información almacenada en discos hasta la descompostura de microprocesadores y memorias. La temperatura del centro de cómputo se debe de mantener alrededor de 19º C a 22º C. En general todos los centros de cómputo deben mantener un estricto control de temperatura que evite condiciones de operación inadecuadas para los equipos.

- Deben contarse con equipos de aire acondicionado con entradas y salidas bien distribuidas que permitan mantener una ventilación adecuada en todo el centro de cómputo.
- Conviene contar también con termómetros conectados a alarmas que adviertan temperaturas críticas que pudieran ocasionar daños a los equipos.
- Los ventiladores para microprocesadores suelen ser una excelente manera de procurar un buen rendimiento de estos dispositivos.
- Cada equipo incluye sus propias instrucciones de operación que deben ser analizados para conocer las condiciones de presión y temperaturas bajo las cuales cada equipo provee su mejor rendimiento.

3.6 Protección contra inundaciones

Las inundaciones son otro gran riesgo para las instalaciones de cómputo. Las fugas de agua en tuberías de drenaje tuberías emergentes contra incendios, sistemas de aire acondicionado y equipos con enfriamiento por agua, son las principales causas de estas

clases de desastres que ocasionan daños considerables a las instalaciones eléctricas y a los equipos computacionales. La humedad también genera serios desperfectos en equipos, cintas magnéticas y discos, por lo que se deben prevenir sus efectos.

Algunas de las consideraciones que se deben contemplar para proteger la instalación contra daños por inundación son:

- Uso de techos, paredes y pisos a prueba de agua.
- Existencia de un sistema de drenaje adecuado.
- Instalación de alarmas en puntos estratégicos.
- Instalación de detectores en los lugares más bajos.
- Existencia de bombas.

Dependiendo de la ubicación del centro de cómputo, puede ser que sea nula la posibilidad de una inundación, sin embargo puede generarse como resultado secundario de un incendio al activarse un sistema de regaderas, por lo que no se debe subestimar.

3.7 Protección contra fuego

Debido a la gran cantidad de material combustible que se almacena en el centro de cómputo y ala complejidad eléctrica, existe la posibilidad de incendio; debido a esto se deben adoptar medidas de seguridad. Así, para la prevención de incendios se deben de tomar en cuenta los siguientes puntos:

- Prohibido fumar en el área de cómputo.
- Establecer inspecciones regulares del lugar.
- Mantener la papelería fuera del cuarto principal.
- Reportar a mantenimiento cualquier desperfecto eléctrico que se observe.

Estas medidas se deben llevar a cabo junto con la implementación de un buen sistema contra incendio, el cual deberá combinar sistemas de alarma, prevención, detección y supresión de fuego.

Algunas características que deben tener un buen sistema de protección contra el fuego son:

- Colocación de alarmas manuales y automáticas en lugares estratégicos en toda la instalación.
- Colocación de extinguidores manuales en lugares estratégicos en toda la instalación.
- Existencia de un sistema automático que disperse el contenido adecuado: agua, CO_2 o gas halón.
- Marcar claramente extinguidores y salidas.
- Existencia de un panel de control que muestre en que parte de la instalación se ha activado una alarma manual o automática.
- Desactivación del aire acondicionado en caso de activarse la alarma contra fuego.
- Corte automático de energía al activarse la alarma.

Detectores de humo.

Los detectores de humo y calor deben estar colocados en toda la instalación a fin de detectar cualquier indicio de fuego, y activar la alarma, esperando un período de tiempo durante el cual se pueda confirmar la presencia de fuego y entonces se activará el sistema que disperse el supresante adecuado, ya sea CO_2, gas halón o agua.

Elementos de extinción.

Normalmente el control y extinción del fuego se realiza a través de distintos supresantes, dependiendo del lugar y naturaleza del fuego. A continuación mencionaré los supresantes, más comunes son:

Bióxido de Carbono (CO_2). Este supresante se recomienda para fuegos eléctricos, sin embargo se expulsa a tan bajas temperaturas que puede causar tanto daño al equipo como lo hacen las regaderas de agua.

Halón. Este gas es el supresante tradicional para los centros de cómputo. Su función es consumir el oxígeno lo que provoca que termine el proceso de combustión, no daña el equipo pero durante su expulsión se debe evacuar inmediatamente al personal. Algunas características son:

- La instalación de halón es cara.
- Almacenado en forma líquida bajo presión puede tener fugas y estar vacío al momento de su utilización.
- Una vez descargado necesita ser reemplazado.
- Para ser efectivo el área necesita estar sellada.
- A muy altas temperaturas puede producir gases tóxicos.

Agua. Funciona a través de regaderas, es un sistema barato, efectivo en cualquier tipo de fuego, disponible inmediatamente para su rehusó, además de permitir la entrada de personas al área afectada durante un desastre. Sin embargo causa daños irreparables al equipo y medios de almacenamiento.

Actualmente se ha desarrollado un nuevo sistema de supresión contra fuego llamado mist (vapor o llovizna) que consiste en una niebla fina de gotitas de agua y al parecer cuenta con ventajas del halón sin sus respectivas desventajas. Además su descarga no causa el daño que causaría la utilización de una regadera.

La elección e instalación de un sistema contra incendio se debe adecuar a las necesidades y características del centro de cómputo sin olvidar que aunque las pérdidas por hardware pueden ser muy altas, suelen ser rebasadas por la pérdida de programas, archivos y/o documentación.

3.8 Limpieza

Es por todos conocido que muchos usuarios de equipos de computo llevan alimentos a sus oficinas para ingerirlos mientras operan las maquinas. Las partículas de los alimentos y el derramamiento de líquidos sobre los teclados son causas frecuentes de descomposturas en los mismos. Además de evitar la introducción de alimentos a los centros de cómputo, otras recomendaciones de limpieza son las siguientes:

- Cuando se limpie el centro de computo debe tratarse de esparcir el polvo ya que este puede afectar las cabezas lectoras/escritoras de los discos, la cabeza dela impresora o las esferas de los ratones. Los paños ligeramente húmedos son el medio ideal para realizar este tipo de limpieza.

- Para evitar el daño de los gabinetes de computadora, su limpieza se debe hacer con líquido no corrosivo. En el mercado ya existen productos para este fin.

- La limpieza de las cabezas lectoras/escritoras de discos también resulta muy conveniente para garantizar su buen funcionamiento.

- Deben establecer reglas y señalamientos en el centro de cómputo que prohíban la introducción de alimentos a las instalaciones.

En conclusión para preservar la seguridad física de las instalaciones conviene crear una buena selección y combinación de los métodos antes mencionados. Así la probabilidad de falla será menor.

3.9 Seguridad física en las redes

En cuanto a la seguridad física en las redes existen diferentes aspectos para garantizar el correcto funcionamiento de los medios de transmisión de datos tanto en Lan como en Wan.

- El cable coaxial es más recomendable que el par trenzado debido a que, además de soportar mayores anchos de banda, éste no puede ser intervenido fácilmente y resulta ser tan flexible como el par trenzado.

- Para asegurar la buena condición de la señal, los terminadores del cable grueso deberá ser de 50 ohms. Estos terminadores ayudan a disipar la señal una vez que esta se propaga a lo largo del cable principal de la red (topología de bus) y así se evitan conflictos de transmisión.

- En cuanto a la fibra óptica, cabe mencionar que es mas ligera y de menores dimensiones que los otros medios de transmisión. Además, para cuestiones de seguridad de transmisión, es completamente insensible a la interferencia eléctrica y soporta anchos de banda muy grandes. Es más cara que el cable coaxial y su instalación es más sofisticada.

- Las redes pequeñas pueden utilizar el par trenzado. Aunque es sensible al ruido es muy económica y de fácil instalación.

- El cable coaxial delgado es mas fácil de manejar y de mejor costo. La desventaja es que cada segmento de cable coaxial delgado debe tener un largo máximo de 185 metros soportando hasta 30 nodos.

Para verificar el correcto funcionamiento del sistema de cableado, lo mínimo que debe hacerse es checar su continuidad. Esto puede hacerse con un voltímetro. El cual nos ayudara a garantizar que nuestra red no tiene falsos contactos y que las líneas se encuentran en condiciones óptimas para la transmisión.

Como una solución a la intervención de las líneas se recomienda el uso de detectores de nivel de señal o detectores de interferencia de onda, los cuales pueden ser utilizados para emitir una alarma al detectar cierta disminución en la potencia de la señal recibida. Si hay algún vampiro (dispositivo para conectar cables alternos) conectando en alguna parte de la

línea. El detector del nivel registrará una baja en la señal que indicará que el cable este siendo intervenido.
Para seleccionar el tipo de cable a ser utilizado, debe tomarse en cuenta el número de computadoras que se conectaran, la ubicación de cada una de ellas, los requerimientos de seguridad y el presupuesto con el que se cuenta. Una vez contemplado todo esto, se estará haciendo una decisión inteligente que redundara en los beneficios del centro de cómputo.

3.10 Control de accesos

El control de acceso a las instalaciones del centro de cómputo no debe visualizarse aisladamente, ya que forma parte de la totalidad de las instalaciones en una organización. Hablando específicamente del control de acceso a las instalaciones del centro de cómputo se pueden adoptar ciertas medidas como las siguientes:

Guardias. Los guardias sólo deben estar en las entradas o en el panel de control pero no deben estar caminando en el cuarto del centro de cómputo. Además deben de contar con una capacitación adicional que les permita controlar y monitorear el panel de control, ya que son los responsables de su adecuado manejo.

Registro. Se debe llevar un registro de los proveedores o visitantes que accesan al centro de cómputo, nombre, hora de entrada, salida, motivo, número de gafete que portará así como nombre y firma de quien autoriza la entrada.

Gafetes. En todo momento se debe portar el gafete, que permite identificar fácilmente si se trata de un empleado, proveedor o visitante, ya que los gafetes deben ser completamente diferenciables, a través del tamaño y/o color.

Sistemas de control de accesos. Estos sistemas permiten o restringen el acceso a determinadas áreas del centro de cómputo. Existen diferentes tipos de clase de sistemas como lo son:

Mecánico. Este tipo de sistema utiliza cerrojos, candados y/o la combinación de llaves. Es el más barato aunque no permite determinar ni quien, ni la hora en que se acceso a algún sitio, por lo que el nivel de seguridad es bajo.

Electrónico. Este sistema funciona a través de tarjetas con código que se insertan en las cajas electrónicas y a través de lectores ópticos o magnéticos sobre el código se permite o niega el acceso. Se puede usar en combinación con alarmas audibles o silenciosas en el panel de control para efectos de identificación de intrusos. En este caso sí se puede determinar la persona y hora en que se acceso a algún sitio. El nivel de seguridad es medio.

Electromecánico. Este tipo de sistema requiere un esfuerzo manual como presionar un botón en combinación con una lectora de tarjeta. Al igual que el sistema electrónico se puede utilizar en combinación con alarmas. El nivel de seguridad es medio.

Digital. Los dispositivos digitales permiten la digitación de cualquier combinación de código que se haya asignado o que el usuario haya elegido para permitir el acceso a determinado lugar. Este tipo de sistema de acceso proporciona un nivel de seguridad alto aunque también es más costoso que los anteriores.

Computarizado. Este tipo de sistemas es el más automático, ventajoso y sofisticado, permite el acceso a través de reconocedores de formas o sonidos, así como la utilización de lectoras de códigos y la digitalización de claves. Están equipados con alarmas audibles y silenciosas que se activan al detectar cualquier intento de acceso no autorizado o durante cambios

ambientales como la temperatura, humedad y corriente de aire. El nivel de seguridad es muy alto, aunque es de los más costosos.

Detectores de movimiento

-Circuito cerrado de televisión (CCTV).

Este tipo de dispositivos permite observar y detectar movimientos en lugares cercanos y remotos que requieren una constante vigilancia. Las cámaras se deben colocar en lugares estratégicos en toda la instalación. El monitoreo se realiza en un cuarto con paneles de control en donde existen pantallas que permiten observar la actividad captada por las cámaras.

-Cámaras infrarrojas.

Estos dispositivos son sensores que detectan el cambio de radiación térmica dentro del ambiente, generalmente solo se utilizan en áreas que requieren un alto grado de seguridad ya que son muy costosas.

La implementación de medidas de control de acceso físico dentro así como las relacionadas a la protección contra fuego o inundación dependerán del tamaño e importancia de las actividades de procesamiento electrónico de datos que se efectúen en una organización. Se deben establecer las medidas mínimas de seguridad mencionadas anteriormente.

CAPÍTULO 4

SEGURIDAD LÓGICA

4.1 Seguridad Lógica

Con el auge de las computadoras surgió la necesidad de implementar medidas de seguridad que mantuvieran protegidos tanto el hardware como las instalaciones de cualquier centro de cómputo contra agresiones externas, sin embargo la gran diseminación y diversidad de computadoras conectadas en diversos puntos a un host, aunado al gran número de sistemas multiusuarios generó, que se comenzaran a diseñar e implementar, características y mecanismos de seguridad de acceso lógico a fin de garantizar la integridad y confiabilidad de la información.

Entendiendo como seguridad lógica el conjunto de políticas y procedimientos que permiten controlar y garantizar la integridad y confiabilidad de la información.

Debido a la vulnerabilidad de los sistemas y a la falta de seguridad de acceso lógico en estos, ha sido factible destruir información accidental o deliberadamente, cometer fraudes, sabotajes o hacer uso de información altamente confidencial distinto al cual fue destinado, por otro lado el reconocimiento de efectos secundarios como perdida de confianza, perdida de imagen, perdida de activos o perdida de penetración en el mercado, ha concentrado la atención en buscar medidas para contrarrestar estos efectos. Así en la década de los 60's se comenzaron a realizar investigaciones y desarrollos en seguridad multiusuarios. Surge un concepto llamado monitoreo referenciador en que involucran cuatro entidades.

- Los objetos.
- Los sujetos.
- Una base de datos de autorizaciones.
- Un registrador de eventos.

Para comprender mejor este concepto sé entenderá por cada una de las entidades mencionadas lo siguiente:

Los objetos son entidades pasivas como dispositivos, volúmenes, cintas, archivos, programas, comandos, CISC transmisión de mensajes. Los sujetos son entidades activas como procesos iterativos o batch que requieren hacer uso de los objetos para lo cual se requiere verificar previamente la base de datos de autorizaciones que contiene los atributos de los sujetos y objetos, entendiéndose por atributos la determinación de uno o más privilegios o restricciones que un sujeto tiene al usar el sistema. Además se debe contar con un registro de eventos a fin de monitorear y auditar la actividad del sistema, entre ellos los accesos.

4.2 Seguridad en Redes

En la actualidad, la falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios en su labor de piratería.

La criptografía por sí sola no es suficiente para prevenir los posibles ataques que se perpetran sobre las redes, sino que es necesario establecer unos mecanismos más complejos que utilizan los distintos sistemas criptográficos en sus cimientos. Pero el problema no queda solucionado instalando en una serie de servidores herramientas de seguridad, porque ¿quién tendría acceso a esas herramientas?, ¿a qué aplicaciones se aplicarían?, ¿Qué sucedería si sólo uno de los dos interlocutores en una comunicación tiene

acceso a herramientas de seguridad? Por lo tanto, cuando se habla de seguridad en redes es necesario definir el entorno en el que se va a aplicar.

La definición de un entorno seguro implica la necesidad de estudiar varios aspectos y de establecer una infraestructura que dé soporte a los servicios de seguridad que se quieren proporcionar. Lo primero que hay que establecer es qué aplicaciones necesitan seguridad y cuántos servicios se necesitan. En segundo lugar hay que determinar cómo se van a proporcionar esos servicios, si van a ser transparentes al usuario, si se le va a dejar elegir el tipo de servicio, etc. También es necesario determinar en qué nivel se van a proporcionar, si en el nivel de aplicación o en niveles inferiores.

Para analizar el contexto de la seguridad en redes, debemos mencionar que los elementos principales a proteger en cualquier sistema informático son el *software*, el *hardware*, los datos/información y personal. Por hardware entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPU's, terminales, cableado, medios de almacenamiento secundario. Por software entendemos el conjunto de programas lógicos que hacen funcional al *hardware*, tanto sistemas operativos como aplicaciones, y por datos el conjunto de información lógica que manejan el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Y personal, ya que la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o sin intención, pueden causarnos enormes pérdidas. Como ya hemos mencionado en el capítulo 1, todos estos elementos son susceptibles de ser atacados y sobre ellos tenemos una serie de amenazas.

Amenazas lógicas

Entre las amenazas lógicas encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (*software* malicioso) o simplemente por error (*bugs* o agujeros).

Software incorrecto

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *exploits*.

Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo; de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque; tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada *Security through obscurity*, se ha demostrado inservible en múltiples ocasiones. Si como administradores no utilizamos herramientas de seguridad que muestren las debilidades de

nuestros sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas).

Algunos ejemplos de herramientas de seguridad:

- Red que supervisa las herramientas.

Argus: Es una red que supervisa la herramienta que utiliza un modelo cliente-servidor para capturar datos y asociarlos en "transacciones". Esta herramienta proporciona la revisión de la red; puede verificar la complacencia a un archivo de configuración de ruta, la información puede ser fácilmente adaptada a análisis del protocolo, detecciones de intrusos, y a necesidades de seguridad. Argus esta disponible en la siguiente dirección:

http://ftp.andrew.cmu.edu/pub/argus.

Swatch: Simple Watcher Program, es un fichero de registro filtro/monitor fácilmente configurable. Este programa supervisa archivos de registros y actúa para filtrar hacia fuera datos no deseados y tomar uno o más usuarios especificando acciones basadas en modelos del registro. Esta disponible en la dirección.

http://ftp.stanford.edu/general/security-tools/swatch/

- Herramientas de Autentificación de Password

CRACK es un programa libre para el diseño de la identificación, por el estándar que conjetura las técnicas. UNIX DES, encripta passwords que se pueden encontrar en diccionarios extensamente disponibles. Las técnicas especuladas están descritas en la documentación del Crack. Se ejecuta este programa como un sistema regular de procedimientos de administración y notifica a los dueños de las cuentas a quienes les han "crackeado" sus passwords. El Crack esta disponible en:

ftp://cpast.cspurdue.edu/pub/tools/unix/crack

- Herramientas de Servicio – Filtrado.

Programa de Capa TCP/IP este programa proporciona información de registros de una red adicional y le da la habilidad a un administrador del sistema de negar o de permitir el acceso de ciertos sistemas o dominios al host en el que el programa esta instalado. La instalación de este software no requiere ninguna modificación en el software existente en la red. Este programa esta disponible en:

ftp://ftp.porcupine.org/pub/security

- Herramientas para examinar Host

SATAN (Security Administrator Tools for Analyzing Networks) es una herramienta de prueba y reporte que colecciona una gran variedad de información sobre los hosts conectados a una red. Esta disponible en las siguientes direcciones: ftp://ftp.porcupine.org/pub/security

- Herramientas Multi - Propósitos

COPS (Computer Oracle and Password System). Son una colección de programas públicamente disponibles que procuran identificar problemas de seguridad en un sistema Unix. Este programa no intenta corregir cualquier diferencia encontrada, sino produce un informe de sus resultados. Esta disponible en:

ftp://coast.cspurdue.edu/pub/tools/unix/cops

- Herramientas de control de Integridad

Tripwire: verifica la integridad de los archivos y directorios; es una utilidad que compara un conjunto designado de archivos y directorios con la información almacenada en una base previamente generada. Cualquier diferencia es señalada por medio de una bandera y se registra, incluyendo entradas agregadas o suprimidas. Cuando corre contra los archivos del sistema sobre una base regular, Tripwire le permite que descubra los cambios en los archivos del sistema críticos y toma inmediatamente medidas apropiadas de los daños. Esta disponible en: ftp://coast.cspurdue.edu/pub/tools/unix/Tripwire

Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar “atajos” en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denominan puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos; por ejemplo, los diseñadores de un *software* de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave “especial”, con el objetivo de perder menos tiempo al depurar el sistema.

Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos archivos o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa.

Canales cubiertos

Los canales cubiertos (o canales ocultos, según otras traducciones) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

Virus

Un virus es una secuencia de código que se inserta en un archivo ejecutable (denominado *huésped*), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande. Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

Programas conejo o bacterias

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina. Hemos de pensar hay ciertos programas que pueden actuar como conejos sin proponérselo. El hecho de que el autor suela ser fácilmente localizable no debe ser ninguna excusa para descuidar esta política: no podemos culpar a un usuario por un simple error, y además el daño ya se ha producido.

Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hacen extremadamente difícil su detección. Las técnicas salami

no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya computadoras dedicadas a contabilidad, facturación de un departamento o gestión de nóminas del personal, comentamos esta potencial amenaza contra el *software* encargado de estas tareas.

Ataque a las redes

La mayoría de ataques a las redes (sistema de información) proviene de personas que nos puede causar enormes problemas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos. Pero con demasiada frecuencia se suele olvidar que los piratas `clásicos' no son los únicos que amenazan nuestros equipos: Es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su *software*, restringiendo servicios, utilizando cifrado de datos).

Se dividen a estas amenazas en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los *crackers* realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas y sus debilidades), lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de archivos.

Hackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Esto es en redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente más protegidos, como los militares.

Terroristas

Por terroristas que es en definición cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de archivos de un servidor que alberga páginas *web* de algún grupo religioso; en el caso de las redes de las universidades existen ataques para la destrucción de sistemas de prácticas o la modificación de páginas *web* de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos. Habitualmente los datos constituyen el principal elemento a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar. Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio "original" desde el que se pueda restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

Contra cualquiera de los elementos descritos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el "fabricado".

4.3 Seguridad de Acceso Lógico

Para obtener la información de destrucción deliberada o accidental y accesos no autorizados, se han investigado los métodos de accesos lógicos. Dichos métodos restringen la utilización de recursos del centro de cómputo, así como la forma de acceso por parte de los usuarios. Actualmente existen en el mercado efectivos métodos de acceso tanto a nivel hardware como software, generalmente consisten en user ids y passwords, que se caracterizan por sé un método práctico que ayuda a disminuir el riesgo de actividad no autorizada por medio de la identificación (user id) y verificación (passwords) durante el inicio de sesión o entrada al sistema, además de ser uno de los controles más funcionales y más económicos.

User ID

Los user id también llamados cuentas permiten firmarse al sistema así como permiten negar el acceso a algún recurso o dirigir la ejecución automática de un programa. En algunos de los sistemas establecen la contabilidad del usuario, que permite determinar quien acceso y para qué, establecer el uso ilícito de user ids, conocer el consumo de recursos del sistema como tiempo de procesamiento, utilización de espacio y memoria. Esta identificación de usuario puede formarse con las iniciales del nombre y/o número de empleado o una combinación de su primer nombre y apellidos, dependiendo del número de usuarios y complejidad del sistema.

Los user ids pueden funcionar sólos o en combinación de passwords que es la práctica más común, ya que conservando el user id y passwords confidencialmente permiten implementar un buen nivel de seguridad ya que es más difícil descubrir los dos.

Para mayor seguridad se deben asignar user ids y passwords únicos para cada usuario en lugar de asignarlos a grupo de personas. Esto permite tener bien identificados a los recursos del sistema, entre ellos los usuarios, y limita los efectos colaterales que pudieran tener cuando alguna persona del grupo promovida de puesto o deja la compañía, ya que se tendría que cambiar inmediatamente el password y dar aviso a los demás compañeros, por otro lado no se puede determinar exactamente quien acceso algún recurso por lo que no se puede establecer los limites de responsabilidad de un usuario al haber accesado el sistema.

Passwords

El password permite verificar la identificación provista por algún usuario al checar que el password corresponda al usuario ingresando previamente. Los passwords esta formados por cadenas de caracteres que en combinación con un user id o cuenta permite el acceso a alguna aplicación o lugar físico del centro de computo. Básicamente se distinguen dos tipos de passwords, passwords de user ids y passwords de recursos. Los primeros siempre están ligados al user id, los segundos protegen el acceso a recursos como consulta subsistemas, ejecución de programas, lectura de archivos o ejecución de comandos entre otros.

Para el uso y administración de passwords se deberán tomar en cuenta algunas características que permitirán que su uso sea eficiente a fin de mantener un buen nivel de seguridad.

Algunas características son las siguientes:

- Dificultad de adivinar. Para ser difíciles de adivinar los passwords deberían tener una longitud enorme, sin embargo nadie va a perder el tiempo aprendiéndoselos o tecleándolos, para evitar esto, la dificultad de adivinar los debe reforzar con su composición y longitud, tomando en cuenta que deben ser fáciles de recordar.

- Composición. Deben estar formados por cadenas de caracteres, en algunos casos sólo alfabéticos o numéricos, una combinación de éstos o cualquier otro caracter.

- Longitud. Los passwords de longitud mayor son más seguros pero toma tiempo ingresarlos y es más fácil cometer errores. La longitud mínima que se recomienda son cuatro caracteres, aunque puede tomar un rango mayor o menor. Sin embargo la organización mundial de estándares establece que el password debe tener una longitud de ocho caracteres.

- Expiración. La expiración del password es la característica que obliga al usuario a cambiarlo por uno nuevo que sólo sea de su conocimiento. Normalmente los passwords que se asignan por primera vez son pre-expirados así como cuando se habilita de nuevo algún user id. La expiración puede tener definido un periodo de tiempo determinado como rango, de esta forma al cumplirse dicho lapso se obliga al usuario a teclear y confirmar un nuevo password que a partir de ese momento sólo será conocido por él.

- Políticas. Los password pueden ser adivinados y en algunos casos pueden ser susceptibles de ser conocidos durante su almacenamiento o transmisión. Para evitar el riesgo de que esto ocurra se debe tomar en cuenta lo siguiente:

- No utilizar passwords fáciles de adivinar, como las iniciales de un nombre, del mes, fechas o palabras que puedan relacionarse fácilmente con el usuario.

- No escribirlos en papeles o documentos que son susceptibles de ser observados por otra persona o que puedan perder.

- No imprimir reportes o registros aún cuando estos son confidenciales.

- Considerar los procedimientos para firmarse (sign-on), estos procedimientos deben ser amigables para el usuario sin contradecir los procedimientos de seguridad. Deben proporcionar la fecha y ahora del último acceso.

- Considerar el número de intentos fallidos permitidos para accesar al sistema, puede ser de una vez hasta n veces dependiendo de las necesidades de seguridad y características del software de seguridad. Es recomendable que al tercer o quinto intento fallido se cierre el acceso para ese user id.

- Considerar el intervalo de tiempo para cambiar el password._Igualmente dependiendo de las características y necesidades de seguridad se debe establecer el periodo de tiempo en que estará activo un user id antes de solicitar automáticamente su cambio de password. Este intervalo puede ser variable, abarcando un rango de 1 a 365 días, aunque también puede determinar que el password nunca expire, es decir que nunca solicite cambiarlo dejando a criterio del usuario cambiarlo en cualquier momento. Es recomendable que el password expire cada mes, excepto cuando los user ids están en bits y no puedan ser cambiados, en este caso se debe especificar que no expire el password.

- Cambiar el password inmediatamente si por alguna razón de emergencia se presto el user id.

- Forma de distribución del password a los usuarios correspondientes para constatar que reciban su propio password, ya sea vía telefónica, fax, correo electrónico o en persona.

Consideraciones administrativas.

La implementación de los users ids y passwords es un control eficaz y muy económico, sin embargo se deben tomar en cuenta sus características y principalmente determinar y seguir las políticas establecidas alrededor de estos controles.

Algunos lineamientos que se pueden establecer para una mejor administración de user ids son los siguientes:

1. Establecer el procedimiento para la alta, modificación y depuración de users ids.

2. Concienciar al usuario de que el user ids y passwords son personales e intransferibles, cada uno tiene un acceso autorizado hasta cierto nivel en aplicación y consulta en los diferentes sistemas de acceso, por lo que no deben prestarse por ningún motivo, ya que el titular es totalmente responsable del uso que le dé.

3. Realizar auditorías periódicas y al azar, del uso que se le esta dando a determinados user id y en caso de encontrar alguna anomalía se deberá notificar al usuario y a su superior inmediato.

4. Establecer un período de tiempo, en él cual si un user id no utilizado se da de baja.

5. Realizar cruces contra nómina y proceder a dar de baja aquellos users id de personal que ya no labore en la compañía. De esta forma no es necesario esperar la notificación por otra parte de personal de la liquidación o retiro de algún empleado ya que se puede aunar

la clave de empleado al user id, hacer un match con el archivo de empleados periódicamente y borrar automáticamente aquellos que ya no se encuentran en dicho archivo.

4.4 Criptografía

Se entiende por criptología el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor.

La criptografía es la parte de la criptología que estudia como cifrar efectivamente los mensajes. La criptografía (del griego Kryptos, "escondido" y Graphein, "escribir") es el arte de enmascarar mensajes con signos normales que sólo tienen sentido a la luz de una clave secreta, esta es tan antigua como la propia escritura pues nació con ella, su rastro en el tiempo se encuentra ya en las tablas cuneiformes, y los papiros de los antiguos egipcios, hebreos, babilónicos y asirios que conocieron y aplicaron sus inescrutables técnicas que alcanzan hoy su máxima expresión gracias al desarrollo de los sistemas informáticos y de las redes mundiales de comunicación.

Dentro de las clases de criptografía más comunes podemos mencionar dos: la transposición y la substitución.

El método de la transposición se caracteriza por cambiar el orden original del mensaje de entrada. Un ejemplo muy común de este método es escribir el mensaje al revés, por ejemplo la palabra “requerimiento” resultaría como “otneimireuqer”. Una variante de este método es el llamado “RAIL FENCE”, en este método el mensaje 4pm london av quedaría como la siguiente secuencia:

4 m o d n v
p l n o a

Posteriormente se toman bloques de 5 caracteres quedando finalmente como:

4MODN VPLNO A

En el método de substitución los elementos del mensaje de entrada conservan su posición relativa siendo reemplazados por letras o por símbolos. Uno de los métodos de substitución mas conocidas es el sistema “Cesar”, el cual reemplaza cada letra del alfabeto por la tercera letra siguiente en la secuencia del alfabeto. El alfabeto correspondiente seria:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

En este método el mensaje de entrada HOLA quedaría como KROD.

De igual manera el método Cesar tiene algunas variantes, una variación de dicho método es la utilización de un alfabeto cifrado al revés de la secuencia original del alfabeto.

Otra variación adicional a este método es la utilización de una palabra llave al inicio de la secuencia del alfabeto cifrado al revés de la secuencia del orden alfabético sin repetir letras que se encuentren en la palabra llave.

Obviamente este tipo de técnicas tradicionales de criptografía fueron desarrolladas muchísimo tiempo atrás al advenimiento de las computadoras por lo que no son

particularmente apropiadas a estas. Por otro lado las cantidades de información que se manejan han variado considerablemente. Actualmente la utilización de criptografía computacional se basa en operaciones aritméticas y/o lógicas.

Algoritmo de encriptación DES

Uno de los algoritmos disponibles más importantes es el DES (Data Encryption Standard) desarrollado por IBM en la década de los 70's y aprobado como un estándar federal en Estados Unidos. Este algoritmo es simétrico, lo que significa que usa la misma llave secreta para encriptar y descifrar los datos. El proceso de este algoritmo es lento y caro, y sólo puede ser realizado por procesadores con microchip. Del mismo modo las transmisiones deben criptográfiarse a través de equipos cuyo hardware este destinado a esto.

Técnicas criptográficas

Los sistemas de criptografía son una forma de transmitir información sobre un sistema de comunicación no-seguro de modo confuso y oculto para evitar que el resto de la gente los pueda leer.

La criptografía proporciona confidenciabilidad y puede también demostrar que una transmisión ha sido o no alterada.

Hay dos técnicas de clave criptográfica:

- La clave privada o llamada Cifradores Simétricos:

La información se encripta con una clave que tanto el remitente como el receptor tienen privadamente. La seguridad del sistema reside en que ambas partes tienen que intercambiar las claves de modo seguro.

Este modo de encriptación es también una técnica usada para asegurar la información almacenada en disco. Encripta los archivos de datos con una clave.

- La clave pública o llamada Cifradores Asimétricos:

Esta clave consiste en dos claves separadas y relacionadas: una pública y otra privada. Esta clave pública es la que se da a conocer y además esta en los servidores o se puede usar en los demás servicios de autorización o certificación como un Commerce Net.

4.5 POLÍTICAS DE SEGURIDAD

Para lograr un efectivo control sobre todos los componentes que conforman la red y asegurar que su conectividad a otras redes no sea frágil, es necesario primero que todo se deba de establecer con exactitud qué recursos de la red y servicios desea proteger, de tal manera que esté preparado para conectar su red con el resto del mundo. Esto implica el estudio y definición de los aspectos necesarios para la planeación de la seguridad de la red, análisis de riesgos, identificación de recursos y amenazas, uso de la red y responsabilidades, planes de acción o contingencia, etc.

Definición

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan cómo una organización maneja, protege y distribuye información sensitiva. Este documento se convierte en el primer paso para construir barreras de protección efectivas.

Una política de seguridad en una declaración formal de las reglas a través de las cuales daremos acceso a la tecnología e información en donde residen los recursos de la organización.

Las políticas de seguridad son el primer elemento a considerar cuando una organización tiene el interés de forjar una infraestructura de recursos de cómputo y de redes seguras.

Por medio de las políticas será posible definir los derechos y obligaciones del personal, además de definir las sanciones que se aplicaran en caso de que estas políticas no sean respetadas.

¿Por que?, ¿Para que?, ¿Para quien?, ¿Para que ocasiones?, etc.

Una política de seguridad en un sitio es requerida para establecer a lo largo de la organización un programa de cómo usuarios internos y externos interactúan con la red de computadores de la empresa, cómo se implementará la arquitectura de la topología de red y dónde se localizarán los puntos especiales de atención en cuanto a protección se refiere.

La definición de una política de seguridad de red no es algo en lo que se pueda establecer un orden lógico o secuencia aceptada de estados debido a que la seguridad es algo muy subjetivo, cada negocio tiene diferentes expectativas, diferentes metas, diferentes formas de valorar lo que va por su red, cada negocio tiene distintos requerimientos para almacenar, enviar y comunicar información de manera electrónica; por esto nunca existirá una sola política de seguridad aplicable a dos organizaciones diferentes.

Además, así como los negocios evolucionan para adaptarse a los cambios en las condiciones del mercado, la política de seguridad debe evolucionar para satisfacer las condiciones cambiantes de la tecnología. Una política de seguridad de red efectiva es algo que todos los usuarios y administradores pueden aceptar y están dispuestos a reforzar, siempre y cuando la política no disminuya la capacidad de la organización, es decir la política de seguridad debe ser de tal forma que no evite que los usuarios cumplan con sus tareas en forma efectiva.

Principios de seguridad

- Privacidad o Confidenciabilidad

La información únicamente debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.

- Integridad

La información no debe ser borrada, ni modificada por alguien que carezca de autorización para hacerlo.

- Autentificación

Únicamente debe ingresar al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos.

- Disponibilidad

La información debe estar siempre disponible en el lugar y tiempo requeridos.

- Consistencia

El sistema debe comportarse como uno espera que lo haga.

- Control de Acceso (Autentificación)

Debe conocerse en todo momento quien entra al sistema y cual es su procedencia.

- Auditoría

Debe conocerse en todo momento las actividades de los usuarios dentro del sistema.

¿Porqué utilizar políticas de seguridad?

Existen muchos factores que justifican el establecimiento de políticas de seguridad para un sitio específico, pero los más determinantes son:

- Ayudan a la organización a darle valor a la información.
- Es una infraestructura desde la cual otras estrategias de protección pueden ser desarrolladas.
- Proveen unas claras y consistentes reglas para los usuarios de la red corporativa y su interacción con el entorno.
- Contribuyen a la efectividad y direccionan la protección total de la organización. Pueden ayudar a responder ante requerimientos legales.
- Ayudan a prevenir incidentes de seguridad.
- Proveen una guía cuando un incidente ocurre.
- Es una planeación estratégica del papel que juega la arquitectura de red al interior de la organización.
- Ayudan a tomar decisiones.
- Ayuda en la culturización de los usuarios para el uso de servicios de red e inculca el valor real que ellos representan.
- Conducen a la creación de manuales de procedimientos.
- Determinan las acciones a tomar bajo ciertas circunstancias.
- Establecen a quien recurrir en momentos críticos
- Pueden ser requeridas durante una Auditoria.
- Define los principios no la implementación.

¿Para qué sirven?

- Establecen las reglas y principios de cómo la organización debe lidiar con los problemas que la pueden afectar.
- Definen las condiciones de uso de los equipos de cómputo y de redes.
- Establecen los derechos de los dueños de los recursos, administradores y usuarios.

Características de las políticas

Una política de seguridad es un plan elaborado de acuerdo con los objetivos generales de la organización y en el cual se ve reflejado el sentir corporativo a cerca de los servicios de red y recursos que se desean proteger de manera efectiva y que representan activos importantes para el normal cumplimiento de la misión institucional. Por esto la política de seguridad debe cumplir con ciertas características propias de este tipo de planes, como son:

Las políticas deben ser:

- Debe ser escritas.

- Deben ser simples y entendibles (específica).
- Debe estar siempre disponible.
- Revisadas por las autoridades de la organización.
- Comprendidas y firmadas por los usuarios.
- Se puede aplicar en cualquier momento a la mayoría de situaciones contempladas.
- Debe estar implementada.
- Se debe poder hacer cumplir.
- Actualizadas.
- Debe ser consistente con otras políticas organizacionales.
- Debe ser estructurada.
- Se establece como una guía, no como una cadena a la cual se tenga que atar para siempre.
- Debe ser cambiante con la variación tecnológica.
- Una política debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas como una unidad corporativa.

Las ventajas de tener políticas son las siguientes:

- Parte fundamental de un esquema de seguridad.
- Permiten actuar de manera rápida y acertada en una contingencia.
- Indican la manera adecuada e inadecuada de usar el sistema.
- Indican lo que pueden hacer o no hacer.
- Establece los derechos y obligaciones tanto para usuarios y administradores.
- Facilitan la introducción del nuevo personal.
- Facilitan la auditoría.

Desarrollo de una política de seguridad

El objetivo perseguido para desarrollar una política de seguridad de red oficial corporativa es definir las expectativas de la organización a cerca del uso de la red y definir procedimientos para prevenir y responder a incidentes de seguridad provenientes del cada día más avanzado mundo de la comunicación global.

Definir una política de seguridad de red significa desarrollar procedimientos y planes que salvaguarden los recursos de la red contra pérdidas y daños, por lo tanto es muy importante analizar entre otros los siguientes aspectos:

- Determinar los objetivos y directrices de la organización.
- La política de seguridad debe estar acorde con otras políticas, reglas, regulaciones o leyes ya existentes en la organización; por lo tanto es necesario identificarlas y tenerlas en cuenta al momento de desarrollar la política de seguridad de redes.
- Identificación de los recursos disponibles.
- ¿Qué recursos se quieren proteger?.
- ¿De quién necesita proteger los recursos?.

- Identificación de posibles amenazas.
- ¿Qué tan reales son las amenazas?.
- ¿Qué tan importante es el recurso?.
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?.
- Verificación frecuente de la política de seguridad de red para ver si los objetivos y circunstancias han cambiado.

En general, el costo de proteger las redes de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad. La política de seguridad debe ser comunicada a cada cual que usa un computador en la red con el fin de que sea ampliamente conocida y se pueda obtener una retroalimentación de los usuarios de la misma para efectos de revisiones periódicas y detección de nuevas amenazas o riesgos.

¿Qué deben de contener las políticas?

- Ámbito de aplicación
- Análisis de riesgos.
- Enunciado de políticas.
- Sanciones
- Sección de uso ético de los recursos de cómputo.
- Sección de procedimientos para manejar incidentes.

Identificación de los elementos a proteger

El primer paso en la creación de la política de seguridad es crear una lista de todas las cosas que necesitan ser protegidas, esta lista debe ser regularmente actualizada. Algunos elementos a considerar son entre otros:

Auditoría y revisión

Es necesario contar con herramientas que ayuden a determinar si hay una violación a las políticas de seguridad, para ello se debe aprovechar al máximo las herramientas incluidas en los sistemas operacionales y utilidades de la red. La mayoría de sistemas operacionales cuentan con bastantes rastros o archivos de "log" con el fin de informar de la actividad del sistema, examinar estos "logs" son el primer paso efectivo para detectar el uso no autorizado del sistema. Para tal efecto se pueden tomar acciones como:

- Comparar listas de usuarios actualmente conectados con listas históricas, para detectar anomalías o comportamientos irregulares.

- Examinar las facilidades de "log" del sistema para checar mensajes de error inusuales del software del sistema operacional como por ejemplo, un número grande de intentos fallidos de conexión a un usuario específico.

- Comparación de los procesos que están siendo ejecutados en las máquinas a tiempos diferentes pueden mostrar diferencias que lleven a detectar programas no autorizados o extraños en ejecución, quizás lanzados por intrusos.

Comunicación a los usuarios

La política de seguridad debe ser informada a todos los usuarios de la red para que conozcan a cerca del uso apropiado que rige su acceso o estación de trabajo específica. También debe ir acompañada por una campaña educacional que indique como se espera que sean usados todos los recursos involucrados en la red corporativa y cómo se pueden proteger por ellos mismos de accesos no autorizados.

Implantar una política de seguridad de red efectiva es un esfuerzo colectivo y como tal se debe proveer los medios para que los usuarios participen activamente en la definición de la misma y hagan aportes de lo que ellos mismos perciben de su interacción con la red.
Si los usuarios perciben que la política reduce su productividad, se debe permitir que participen. Si es necesario se pueden añadir recursos adicionales a la red para asegurar que los usuarios pueden continuar haciendo su trabajo sin pérdida en la productividad. Para crear una política de seguridad de red efectiva es necesario encontrar un balance entre la protección y la productividad.

Asegurar responsabilidades en torno a la política de seguridad

Un aspecto importante en torno a la política de seguridad de red es asegurar que todos saben cuál es su responsabilidad para mantener la seguridad, por lo tanto la política debe poder garantizar que cada tipo de problema tiene a alguien que puede manejarlo de manera responsable.

Así mismo pueden existir varios niveles de responsabilidad asociados con una política de seguridad de red. Por ejemplo cada usuario de la red está responsabilizado por su clave de acceso, un usuario que pone en riesgo su cuenta de acceso aumenta la probabilidad de comprometer otras cuentas y recursos. Por otro lado los administradores de red y de sistema son responsables de mantener la seguridad general de la red.

Las políticas y los procedimientos.

Las políticas de seguridad indican el “que” se va hacer mientras que los procedimientos él “como”, estos últimos permiten llevar a la práctica las políticas.

Los procedimientos:

- Otorgan cuentas (acceso a shell, e-mail)
- Conectar una maquina en red.
- Actualización del sistema operativo.
- Instalación del Software localmente y vía red.
- Actualizar software crítico.
- Respaldar y restaurar información.
- Manejar incidentes de seguridad.

Existen diferentes tipos de políticas de seguridad:

- De cuentas.

Establecen que es una cuenta de usuario, como esta conformada, a quien se le otorga, quien es el encargado de asignarlas, como deben ser creadas, etc.

Una cuenta de usuario debe esta conformada por un nombre de usuario y su contraseña asociada.

- De contraseñas.

Establecen quien asigna las contraseñas, que longitud tendrá, como será comunicada, etc.

Todas las contraseñas deben contener al menos siete caracteres y deben ser difíciles de adivinar.

- De control de acceso.

Especifican como deben los usuarios acceder al sistema, desde dónde y de que manera deben autenticarse.

Los usuarios deben acceder al sistema utilizando un programa que les permita una conexión segura y con su propia cuenta.

- De uso adecuado.

Considerar el uso adecuado e inadecuado del sistema por parte de los usuarios, lo que esta permitido y lo que no dentro del sistema de cómputo.

Por ejemplo:

"Todo lo que no este explícitamente prohibido esta permitido"

Permisivo.

"Todo lo que no este explícitamente permitido esta prohibido"

Paranoico.

- De respaldos.

Especifican que información debe respaldarse, la periodicidad, los medios a utilizar, la forma de restauración, el área de almacenamiento de respaldos.

Cada treinta días el administrador del sistema realizara respaldos completos del sistema y debe almacenarlo en un lugar distante al trabajo.

- De correo electrónico.

Establece el uso adecuado e inadecuado del servicio de correo electrónico así como los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto.

El usuario es la única persona autorizada en leer su correo y esta prohibido usar la cuenta para propósitos ajenos a las actividades laborales.

- De contabilidad del sistema

Establecen lineamientos bajo las cuales pueden ser monitoreadas las actividades de los usuarios del sistema de cómputo.

Se deben registrar bitácoras en todos los comandos emitidos por los usuarios del sistema para propósitos de contabilidad.

Ciclo de vida de las políticas de seguridad

Las políticas de seguridad tienen un ciclo de vida en la que nos podemos apoyar:

- Preparación

Recopilación de todo tipo de material que se relacione con cuestiones de seguridad en la organización.

- Manuales de procedimientos.
- Planes de contingencia.
- Cartas compromiso.
- Redacción.

Escribir las políticas de una manera clara, concisa y estructurada. Requiere de la labor de un equipo conformado por: directivos, administradores y usuarios.

- Edición.

Reproducción de las políticas de manera formal para ser sometidas a revisión y aprobación.

- Aprobación.

Es uno de los más difíciles procesos, ya que las personas afectadas por las políticas son renuentes a aceptarlas por lo que en esta etapa el apoyo del directivo es primordial.

- Difusión.

En este paso se dan a conocer las políticas al personal de la unidad u organización, mediante proyecciones de video, WWW, correo electrónico, cartas compromiso, memos, etc.

- Aplicación (Implementación)

Es el instante en que las políticas adquieren vigencia para ser aplicadas y cumplirse predicando con el ejemplo.

- Actualización

Las políticas deben ser revisadas y actualizadas periódicamente y el momento ideal es justamente después de un incidente de seguridad.

CAPÍTULO 5

MEDIDAS DE SEGURIDAD Y SANCIONES

5.1 Análisis de Riesgos

El análisis de Riesgos es un proceso para determinar las amenazas y sus daños potenciales. Se inicia con una lista de todas las vulnerabilidades del sistema. Después, para cada amenaza, se plantean una serie de medidas preventivas, así como el costo que representaría aplicarlas. Y por último se realiza lo que es un análisis costo-beneficio en donde hacemos un estudio de cuanto costaría la implementación de las herramientas de seguridad o en caso contrario no hacer dicha implementación aceptando los riesgos.

Un análisis de riesgo, como su nombre lo implica, es un estudio de los riesgos de hacer algo. Algunos riesgos son simplemente parte del costo de los negocios, en algunas ocasiones se toma como parte normal de la operación.

Las medidas preventivas pueden reducir la seriedad de una amenaza. Las empresas muy grandes qua tienen centros de cómputo en muchos lugares, no pueden determinar fácilmente los riesgos, ni de las medidas que deben ser tomadas en sus centros de cómputo.

5.1.1 Razones para Realizar un Análisis de Riesgo

Algunos de los beneficios de un buen análisis de riesgo son:

Usuarios Responsables.- el hacer público las características de la seguridad y los beneficios de esta, hace que los usuarios se vuelvan más responsables y cooperen con las medidas tomadas, fortaleciendo con esto la seguridad.

Identificar los bienes, sus vulnerabilidades y las medidas de seguridad.- algunas empresas y/o centros de cómputo de las instituciones no saben manejar la información sin la menor precaución, esto puede representar un gran riesgo para su estabilidad. Un análisis sistemático y conciente nos proporciona una lista de la información importante, que tiene riesgos y la cual debe ser protegida.

Toma de decisiones.- en ocasiones la productividad sufre un decremento, por las medidas excesivas de control y las inconveniencias de los usuarios. También, algunos riesgos no pueden ser justificados desde la perspectiva de protección que proveen, por lo que se tiene que buscar otra forma de control, menos problemática.

Gastos justificados para obtener seguridad.- muchas medidas de seguridad son muy caros y no tiene ningún beneficio importante. Un análisis de riesgo puede ayudar a identificar los casos que valen la pena el tener este tipo de seguridad.

5.1.2 Pasos de un Análisis de Riesgo.

El análisis de riesgo es un proceso ordenado, que se tiene que dar en el manejo de sistemas. Muchos de los puntos son flexibles para ser adaptados a cada sistema de cómputo, porque no todos tienen que proteger el mismo tipo de información o tiene las mismas debilidades.

Los pasos básicos son:

a) Identificar los bienes importantes a ser protegidos

Este es el primer paso a ser tomado en un análisis de riesgo, es el identificar los principales puntos de ataque de un sistema, como lo pueden ser:

- Hardware: procesadores centrales, tarjetas, teclados, monitores, terminales, microcomputadoras, estaciones de trabajo, unidades de lectura-escritura, impresoras, cables, conexiones, controladores de comunicaciones y medios de comunicación.

- Software: programas fuente, programas objeto, programas de utilidad, sistemas operativos, compiladores y programas de diagnóstico y mantenimiento.

- Datos: Los datos utilizados durante la ejecución, los datos almacenados en medios magnéticos, los datos impresos, los datos archivados, los registros de auditoria, etc.

- Documentación: La documentación de programas, hardware, sistemas procedimientos administrativos y de todo el sistema.

- Materiales: papel, formas, cartuchos láser, medios magnéticos, etc.

- Gente: La gente que se encarga de correr los procesos o almacenar información, administrar los recursos.

Un análisis de riesgos empieza con una lista de todos los bienes que componen un sistema de cómputo, como si fuera un inventario del sistema.

b) Determinar las Vulnerabilidades

El hacer la lista de los bienes que componen el sistema, es relativamente fácil, porque muchos de estos bienes son tangibles o fácilmente identificados. Lo siguiente es determinar las vulnerabilidades de esos bienes. Se necesita hacer visualización desde muchos ángulos y perspectivas, para poder hacer una predicción de los daños que pudieran ocurrir, quienes estarían en posibilidad de efectuarlos y bajo que circunstancias.

Un sistema para ser seguro, debe tener las siguientes características *Confidencialidad, Integridad y Disponibilidad.* Una amenaza es la posible pérdida de algunas de estas tres características. Las posibles vulnerabilidades pueden ser identificadas considerando las situaciones que pueden causar pérdida de la confidencialidad de un objeto, la pérdida de integridad o la pérdida de disponibilidad.

A continuación se presenta la tabla 5.1 en la que se pueden organizar los bienes y anotar las posibles amenazas que podrían afectar de acuerdo a las 3 características de seguridad, esta tabla, al igual que la Lista de Evaluación no es rígida, y se puede adecuar a las características de cada sistema.

Bien	Confidencialidad	Integridad	Disponibilidad
Hardware			
Software			
Datos			
Gente			
Documentación			
Materiales			

Tabla 5.1 Lista de Evaluación.

Y los cuestionamientos a realizarnos serían:

¿Cuáles son los efectos de errores no intencionales? Por ejemplo. Teclear el comando equivocado, datos equivocados, borrar la información equivocada, etc.

¿Cuáles serían los efectos de intrusiones premeditadas, por parte de gente interna a la empresa? Considerando a los empleados descontentos o ambiciosos.

¿Cuáles serían los efectos para intrusos externos? Pensando en acceso por medio de red, acceso vía módem, crackers, gente que busca en la basura, etc.

¿Cuáles serían los efectos de accidentes naturales? Fuego, tormentas, inundaciones, descargas eléctricas o fallas del equipo.

Al llenar la tabla con la respuesta a éstas preguntas, nos muestra los problemas más comunes que pueden afectar el sistema.

c) Estimar la probabilidad de explotación de estas debilidades

El siguiente paso es determinar las probabilidades de que una amenaza se convierta en un ataque al sistema. La probabilidad va a ser el resultado del tipo de amenaza, la facilidad con la que sería detectada por los atacantes y la posibilidad de que sean burladas las medidas de control tomadas para disminuir los riesgos. Puede que algunos eventos sean imposibles de pronosticar, de cualquier manera existen métodos por los que la probabilidad de que un ataque ocurra puede ser calculada. Probabilidad, existe información por la que se puede determinar las posibilidades de que un empleado cometa fraude, robo o algún otro crimen, así como de posibles errores intencionales o no. También se puede hacer una encuesta de un determinado sistema, para localizar sus posibles fallas en los sistemas operativos, en el hardware, en los intentos fallidos de conectarse con identificaciones falsas, el número de accesos, el tamaño de los archivos y fecha de modificación, etc.

d) Estimar el tamaño o los efectos de la posible pérdida.

Estimar el costo estimado de cada ataque es el siguiente paso. Así como la probabilidad de ocurrencia, este valor también es difícil de determinar. Algunos costos, como el de remplazar una pieza de hardware, es fácil de determinar, incluso el costo de reemplazar una pieza de software es fácil de obtener, pero el valor de los datos no se calcula tan fácilmente, porque son muchos intereses los afectados. Algunos datos necesitan ser protegidos por razones legales. Los datos de índole personal, como la información de impuestos, datos del censo, información médica. La información referente a la empresa y/o institución es confidencial. Así que por lo visto anteriormente, realmente resulta difícil valuar los datos.

En un sistema de cómputo, una pieza de software, o una clave personal son incalculables, ya que pueden ocasionar que un servicio se retrase provocando grandes pérdidas.

Las siguientes preguntas pueden llevar a un análisis de ramificaciones de una falla de seguridad del sistema de cómputo. Las respuestas a estas preguntas pueden ayudar a identificar los costos.

¿Qué obligaciones legales existen para preservar la confidencialidad y la integridad de los datos?

El divulgar determinada información, ¿podría de alguna forma causar daños a una organización o a un particular?

¿Existe la posibilidad de alguna acción legal?

¿Podría algún acceso no autorizado a la información causar algún daño en una futura oportunidad de negocio de la empresa?

¿Podrían los competidores ganar una ventaja desleal?

¿Cuál sería el daño estimado?

¿Cuál sería el efecto psicológico de la falta de servicio de cómputo?

¿Cuántos clientes y/o usuarios podrían ser afectados?

¿Cómo se vería afectada la productividad o el servicio que se brinda?

¿Qué valor tiene el accesar determinados datos o programas?

¿Podrían ejecutarse después los procesos, o en algún otro lugar o alquilar otro equipo?

¿Qué costo tendría el ejecutarse después o en algún otro lugar, o con otro equipo?

¿Qué problemas traería la pérdida de información?

¿Sería reemplazada o construida?

¿Cuál sería el costo de reemplazarla o construirla?

Estos costos no son fáciles de evaluarse sin embargo, deben ser evaluados para determinar el daño que podría ser causado. Las amenazas en la seguridad de cómputo, suelen ser poco valoradas. Estimaciones reales del daño que puede ser potencial, elevan la preocupación en cómputo e identifica los lugares donde debe existir atención especial. El costo generalmente es estimado por un año, por lo que este debe de ser multiplicado por el número de incidentes por año.

e) Buscar las posibles medidas de control y sus costos

Los cálculos reflejan la situación de una empresa y/o institución en un momento determinado y si estos cálculos reflejan una pérdida considerable, es tiempo de cambiar las medidas de seguridad o implementar las que sean necesarias.

Una forma de identificar las medidas de control adecuadas para cada amenaza es revisando la lista de medidas preventivas:

- Controles de encriptación.
- Protocolos de seguridad.
- Programas de control de desarrollo.
- Programas de control de ambiente de ejecución.
- Protección de los sistemas operativos.
- Identificación.
- Autenticación.
- Control de acceso a las bases de datos.
- Controles de inferencia de las bases de datos.
- Multiniveles de control de seguridad para los datos, las bases de datos y los sistemas operativos.

- Controles de computadora personales: procedimientos, protección física, protección de hardware y software.
- Control de acceso de red.
- Control de integridad de las redes.
- Controles físicos.

f) ¿Cuales serían los beneficios de estas medidas de control?

Para finalizar el análisis de riesgos es conveniente realizar un análisis de costo-beneficio de las medidas de control para prevenir los ataques. Para esto se obtendrían las pérdidas anuales a las cuales les restamos el porcentaje en que se reducirían las pérdidas esperadas más el costo de las medidas.

5.2 Plan de Contingencia

Un Plan de Contingencia de Seguridad Informática consiste en los pasos que se deben seguir, luego de un desastre, para recuperar; aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas.

El elaborar un Plan de Contingencia implica realizar un análisis de todos los posibles riesgos a los cuales puede estar expuesta la información y el equipo de cómputo. Es muy importante que el Plan de Contingencia incluya *Estrategias de Recuperación de Desastres*, ya que las medidas de seguridad nunca serán suficientes para cuando ocurra un siniestro.

Planeación de Estrategias de Recuperación de Desastres.

Esta planeación es muy importante ya que se definen acciones y objetivos para cada unidad o departamento de la organización, enfoca a éstas en la preparación de sus necesidades específicas para y durante un desastre; por lo que el proceso de recuperación puede realizarse eficientemente.

Se deberá conformar un grupo encargado de elaborar, probar e implementar el plan de contingencias, el cual deberá estar a cargo del administrador del centro de cómputo. Deberá de conformarse un plan de emergencias, determinando los procedimientos a llevar acabo para cada contingencia identificada. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.

Para el desarrollo del plan de contingencias se deben tomar en cuenta ciertas características que se mencionan a continuación:

- Aprobación. El plan debe de ser aceptable para auditores, el director, clientes y proveedores.
- Flexibilidad. El plan deberá ser especificado en guías, en lugar de relacionar los detalles ó situaciones individuales del desastre.
- Mantenimiento. Omitir detalles innecesarios para actualizarlo fácilmente.
- Costo-Efectividad. Se deberá enfatizar en la necesidad de minimizar los costos del plan, respaldo redundante del procesamiento de la suscripción de honorarios, mantenimiento y costo de pruebas.

- Continuidad de la empresa. En el plan debe de asegurar la continuidad, durante un periodo de recuperación de desastres.

- Respuesta organizada. Debe contar el plan con una lista de verificación de salidas que necesitan atención inmediata que sigue al desastre.

- Responsabilidad. Se deberá asignárseles la responsabilidad a individuos específicos de cada salida que requiera atención durante la emergencia y el tiempo del periodo del procesamiento interno.

- Prueba. La prueba con los usuarios para revisar los procedimientos de verificación de respaldo debe de realizar algo específico en los intervalos de tiempo. De tal forma, que el plan cuente con un estado de frecuencias de prueba y documente la metodología de prueba.

Se deben definir aspectos muy importantes que deberá tener el plan de contingencia como son las responsabilidades que tiene cada uno de los sectores de la organización ante la contingencia y cómo se alteran los procedimientos habituales para dar lugar a los procedimientos de contingencia.

Los recursos que se necesitan para operar en el modo contingencia y cuáles de los recursos habitualmente utilizados no se deben utilizar. Esto debe estar debidamente documentado y verificado lo más exhaustivamente posible.

La capacitación al personal que debe intervenir en la contingencia, ya que es necesario que el personal involucrado sepa cómo se saca de servicio cualquier componente que, según el Plan de Contingencia, no debe seguir operando ante alguna falla; que pueda darse cuenta de qué debe hacer y que esté en capacidad de hacerlo cuando sea preciso.

Y por ultimo la contingencia solo es en caso de desastres por lo que no es permanente. Se deberán prever mecanismos para recuperar los datos de operación durante la contingencia y aplicar las instrucciones necesarias para que las operaciones no sufran una interrupción alguna después de la contingencia.

5.3 Políticas de Respaldo

Es de gran importancia contar con políticas de respaldo ya que no es ninguna novedad el valor que tiene la información y los datos para los centros de cómputo. Ya que siempre se deben tomar precauciones al confiar al núcleo de nuestros datos e información al sistema de almacenamiento de un equipo de cómputo. Por ejemplo, si el monitor, la memoria e incluso la CPU de un equipo de cómputo dejan de funcionar, simplemente lo reemplazamos, y no hay mayores dificultades. Pero si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información. Es principalmente por esta razón, por la que debemos respaldar la información importante. Si esto llegará a ocurrir en una empresa o en un centro de cómputo, las pérdidas económicas podrían ser cuantiosas. Los negocios de todos los tipos y tamaños confían en la información computarizada para facilitar su operación. La tecnología no está exenta de fallas o errores, y los respaldos de información son utilizados como un plan de contingencia en caso de que una falla o error se presente.

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, etc. Y aunque no se pueda prevenir cada una de estas interrupciones, la empresa o institución, sí puede prepararse para evitar las consecuencias

que éstas se puedan tener. Del tiempo que tarde en reaccionar una empresa o centro de cómputo dependerá la gravedad de sus consecuencias.

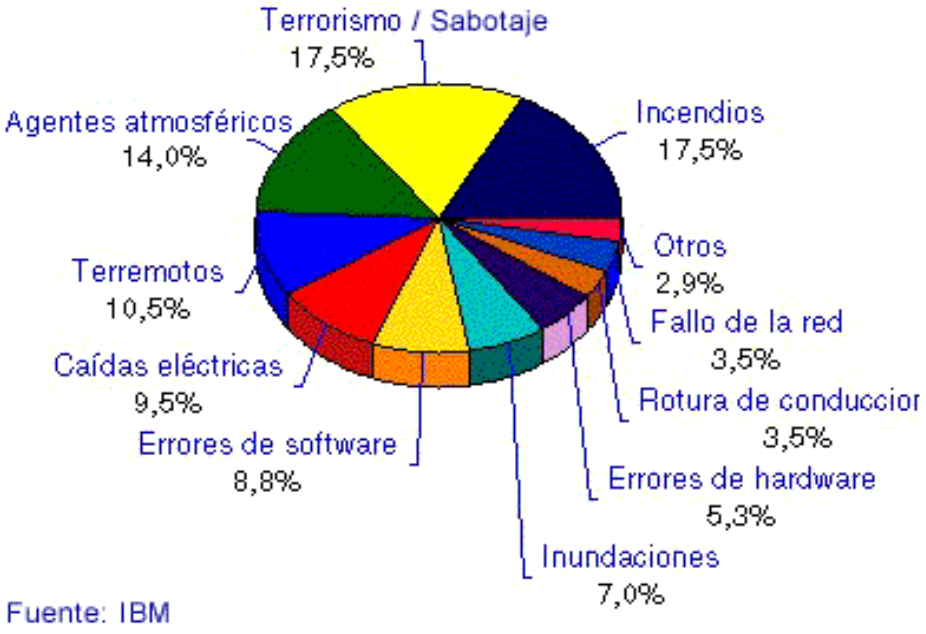


Figura 5.1 Riesgo a los cuales se encuentran inmersos los Sistemas de Información.

Respaldar la información significa copiar el contenido lógico de nuestro sistema informático a un medio que cumpla con una serie de exigencias:

1. Ser confiable: Es minimizar las probabilidades de error. Muchos medios magnéticos como las cintas de respaldo, los disquetes, o discos duros tienen probabilidades de error o son particularmente sensibles a campos magnéticos, elementos todos que atentan contra la información que hemos respaldado allí.

Otras veces la falta de confiabilidad se genera al rehusar los medios magnéticos. Las cintas en particular tienen una vida útil concreta. Es común que se subestime este factor y se reutilicen más allá de su vida útil, con resultados nefastos, particularmente porque vamos a descubrir su falta de confiabilidad en el peor momento: cuando necesitamos RECUPERAR la información.

2. Estar fuera de línea, en un lugar seguro: Tan pronto se realiza el respaldo de información, el soporte que almacena este respaldo debe ser desconectado de la computadora y almacenado en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica. No es de gran utilidad respaldar la información y dejar el respaldo conectado a la computadora donde potencialmente puede haber un ataque de cualquier índole que lo afecte.

3. La forma de recuperación sea rápida y eficiente*:* Es necesario probar la confiabilidad del sistema de respaldo no sólo para respaldar sino que también para recuperar. Hay sistemas de respaldo que aparentemente no tienen ninguna falla al generar el respaldo de la información pero que fallan completamente al recuperar estos datos al sistema informático. Esto depende de la efectividad y calidad del sistema que realiza el respaldo y la

recuperación. Esto nos lleva a que un sistema de respaldo y recuperación de información tiene que ser probado y eficiente.

5.3.1 Copias de Seguridad

Las copias de seguridad son uno de los elementos más importantes y que requieren mayor atención a la hora de definir las medidas de seguridad del sistema de información, la misión de las mismas es la recuperación de los ficheros al estado inmediatamente anterior al momento de realización de la copia. La realización de las copias de seguridad se basará en un análisis previo del sistema de información, en el que se definirán las medidas técnicas que puedan condicionar la realización de las copias de seguridad, entre los que se encuentran:

Volumen de información a copiar

Condicionará las decisiones que se tomen sobre la política de copias de seguridad, en una primera consideración está compuesto por el conjunto de datos que deben estar incluidos en la copia de seguridad, sin embargo, se pueden adoptar diferentes estrategias respecto a la forma de la copia, que condicionan el volumen de información a copiar, para ello la copia puede ser:

- *Copiar sólo los datos.-* poco recomendable, ya que en caso de incidencia, será preciso recuperar el entorno que proporcionan los programas para acceder a los mismos, influye negativamente en el plazo de recuperación del sistema.
- *Copia completa.-* recomendable, si el soporte, tiempo de copia y frecuencia lo permiten, incluye una copia de datos y programas, restaurando el sistema al momento anterior a la copia.
- *Copia incremental.-* solamente se almacenan las modificaciones realizadas desde la última copia de seguridad, con lo que es necesario mantener la copia original sobre la que restaurar el resto de copias. Utilizan un mínimo espacio de almacenamiento y minimizan el tipo de desarrollo, a costa de una recuperación más complicada.
- *Copia diferencial.-* como la incremental, pero en vez de solamente modificaciones, se almacenan los ficheros completos que han sido modificados. También necesita la copia original.

Tiempo disponible para efectuar la copia

El tiempo disponible para efectuar la copia de seguridad es importante, ya que el soporte utilizado, unidad de grabación y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas, y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar accesos o modificaciones sobre los datos objeto de la copia, este proceso ha de planificarse para que suponga un contratiempo en el funcionamiento habitual del sistema de información.

Soporte utilizado

Es la primera decisión a tomar cuando se planea una estrategia de copia de seguridad, sin embargo esta decisión estará condicionada por un conjunto de variables, tales como la frecuencia de realización, el volumen de datos a copiar, la disponibilidad de la copia, el tiempo de recuperación del sistema, etc. Entre los soportes más habituales, podemos destacar las cintas magnéticas, discos compactos, grabadoras de CD-ROM o cualquier dispositivo capaz de almacenar los datos que se pretenden salvaguardar.

La estimación del coste de un soporte de almacenamiento para las copias de seguridad no se basa simplemente en el precio de las unidades de cinta o de disco, el coste de la unidad de grabación es también muy importante, ya que puede establecer importantes diferencias en la inversión inicial.

La unidad será fija o extraíble, es otra decisión importante, ya que la copia de seguridad se puede realizar sobre otro disco duro del sistema de información, o bien, mediante los elementos descritos anteriormente. Una vez definidas las medidas de índole técnica, quedan por definir las medidas organizativas, ya que de nada sirve el mejor soporte si las copias no se realizan de acuerdo a un plan de copias de seguridad.

La política de copias de seguridad debe garantizar la reconstrucción de los archivos en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Frecuencia de realización de copias de seguridad

La realización de copias de seguridad ha de realizarse diariamente, éste es el principio que debe regir la planificación de las copias, sin embargo, existen condicionantes, tales como la frecuencia de actualización de los datos, el volumen de datos modificados, etc, que pueden hacer que las copias se realicen cada más tiempo.

Planificación de la copia

Las copias de seguridad se pueden realizar en diferentes momentos día, incluso en diferentes días, pero siempre se han de realizar de acuerdo a un criterio, y este nunca puede ser "cuando el responsable lo recuerda", si es posible, la copia se debe realizar de forma automática por un programa de copia, y según la configuración de éste, se podrá realizar un día concreto, diariamente, semanalmente, mensualmente, a una hora concreta, cuando el sistema esté inactivo, etc, todos estos y muchos más parámetros pueden estar presentes en los programas que realizan las copias de seguridad y deben permitirnos la realización únicamente de las tareas de supervisión.

Responsable del proceso

La mejor forma de controlar los procesos que se desarrollan en el sistema de información, aunque estos estén desarrollados en una parte importante por el propio sistema, es que exista un responsable de la supervisión de que " lo seguro es seguro", para ello se debe designar a una persona que incluya entre sus funciones la supervisión del proceso de copias de seguridad, el almacenamiento de los soportes empleados en un lugar designado a tal fin e incluso de la verificación de que las copias se han realizado correctamente.

Por último, se debe considerar en la realización de las copias de seguridad, el uso de diferentes soportes para almacenar los datos, entre las diferentes posibilidades que se presentan en función del número de soportes empleados, se puede considerar la siguiente:

Un posible esquema de copia de seguridad sería realizar una copia de seguridad completa cada mes y se guarda la cinta durante un año (preferentemente en algún sitio seguro ajeno a la empresa), una copia de seguridad completa semanalmente que se guarda durante un mes y copias de seguridad diarias, que se guardan durante una semana y que pueden ser completas, increméntales o diferenciales. Con este sistema se pueden utilizar 7 soportes que garantizan un alto nivel de seguridad en cuanto a recuperaciones de datos.

También se recomienda guardar las copias de seguridad en un lugar alejado, como, por ejemplo, una caja de seguridad o cualquier otro sitio asegurado contra incendios, para que, en caso de que se produzca algún desastre como un incendio, los datos se encuentren protegidos.

5.3.2 Clasificación de respaldos

Copias de Información (Backups).

Estos respaldos son sólo duplicados de archivos que se guardan en "Tape Drives" de alta capacidad. Los archivos que son respaldados pueden variar desde archivos del sistema operativo, bases de datos, hasta archivos de un usuario común. Existen varios tipos de Software que automatizan la ejecución de estos respaldos, pero el funcionamiento básico de estos paquetes depende del denominado archive bit. Este archive bit indica un punto de respaldo y puede existir por archivo o al nivel de "Bloque de Información" (típicamente 4096 bytes), esto dependerá tanto del software que sea utilizado para los respaldos así como el archivo que sea respaldado. Este mismo archive bit es activado en los archivos (o bloques) cada vez que estos sean modificados y es mediante este bit que se llevan acabo los tres tipos de respaldos comúnmente utilizados:

Respaldo Completo ("Full"): Guarda todos los archivos que sean especificados al tiempo de ejecutarse el respaldo. El archive bit es eliminado de todos los archivos (o bloques), indicando que todos los archivos ya han sido respaldados.

Respaldo de Incremento ("Incremental"): Cuando se lleva acabo un Respaldo de Incremento, sólo aquellos archivos que tengan el archive bit serán respaldados; Estos archivos (o bloques) son los que han sido modificados después de un Respaldo Completo. Además cada Respaldo de Incremento que se lleve acabo también eliminará el archive bit de estos archivos (o bloques) respaldados.

Respaldo Diferencial ("Differential"): Este respaldo es muy similar al "Respaldo de Incremento", la diferencia estriba en que el archive bit permanece intacto.

Respaldo	Archivos en respaldo	Archive bit	Ventajas	Desventajas
Completo ("Full")	Todos	Eliminado en todos los archivos	Con este respaldo únicamente es posible recuperar toda la información	Tiempo de Ejecución
De Incremento ("Incremental")	Archivos con archive bit activo.(Aquellos que hayan cambiado desde el último Respaldo Completo)	Eliminado en los archivos que se respaldan	Velocidad	Requiere del último Respaldo Completo y de todos los Respaldos de Incremento que le siguieron para recuperar el Sistema
Diferencial ("Differential")	Archivos con archive bit activo.(Aquellos	Intacto	Sólo requiere del último Respaldo Completo y del	Ocupa mayor espacio en discos

	que hayan cambiado desde el último Respaldo Completo)		último respaldo Diferencial	comparado con Respaldos de Incremento

Tabla 5.2 Tabla de Respaldos.

Secuencia de Respaldo GFS (Grandfather-Father-Son)

Esta secuencia de respaldo es una de las más utilizadas y consiste en Respaldos Completos cada semana y Respaldos de Incremento o Diferenciales cada día de la semana. Suponiendo la siguiente semana:

Domingo (1)	Lunes (2)	Martes (3)	Miércoles(4)	Jueves (5)	Viernes(6)	Sábado (7)
Diferencial/ de Incremento o NADA	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ de Incremento	Completo	Diferencial/ de Incremento o NADA
Domingo (8)	Lunes (9)	Martes(10)	Miércoles (11)	Jueves (12)	Viernes(13)	Sábado (14)
Diferencial/ de Incremento o NADA	Diferencial/ de Incremento	Diferencial/ de Incremento	Diferencial/ De Incremento	Diferencial/ de Incremento	Completo	Diferencial/ de Incremento o NADA

Tabla 5.3 Tabla de Secuencia de Respaldos.

En caso de fallar el Sistema en jueves (12):

- Será necesario el Respaldo completo del Viernes(6) y
- Si se utilizaron Respaldos Diferenciales: Sólo el Respaldo Diferencial del Miércoles (11).
- Si se utilizaron Respaldos de Incremento: Se necesitaran todos los Respaldos de Incremento desde el Sábado(7) hasta el Miércoles(11)
- Claro esta que los respaldos completos de cada Viernes pasan a formar parte del "Archivo" mensual de Información

Duplicado de Información en Línea (RAID)

RAID ("Redundant Array of Inexpensive Disks") en palabras simples es: un conjunto de 2 o más "Discos Duros" que operan como grupo y logran ofrecer una forma más avanzada de respaldo ya que:

- Es posible mantener copias en línea ("Redundancy").
- Agiliza las operaciones del Sistema (sobre todo en bases de datos.)
- El sistema es capaz de recuperar información sin intervención de un Administrador.

Existen varias configuraciones de Tipo RAID, sin embargo, existen 4 tipos que prevalecen en muchas Arquitecturas:

RAID-0: En esta configuración cada archivo es dividido ("Striped") y sus fracciones son colocadas en diferentes discos. Este tipo de implementación sólo agiliza el proceso de lectura de archivos, pero en ningún momento proporciona algún tipo de respaldo ("redundancy").

RAID-1: En orden ascendente, este es el primer tipo de RAID que otorga cierto nivel de respaldo; cada vez que se vaya a guardar un archivo en el sistema éste se copiara integro a DOS discos (en línea), es por esto que RAID-1 también es llamado "Mirroring".Además de proporcionar un respaldo en caliente ("hot") en dado caso de fallar algún disco del grupo, RAID-1 también agiliza la lectura de archivos (si se encuentran ocupadas las cabezas de un disco "I/O") ya que otro archivo puede ser leído del otro disco y no requiere esperar a finalizar el "I/O" del primer disco.

RAID-3: Esta configuración al igual que RAID-0 divide la información de todos los archivos ("Striping") en varios discos, pero ofrece un nivel de respaldo que RAID-0 no ofrece. En RAID-0 si falla un disco del grupo, la Información no puede ser recuperada fácilmente, ya que cada disco del grupo contiene una fracción del archivo, sin embargo RAID-3 opera con un disco llamado "de paridad" ("parity disk"). Este "disco de paridad" guarda fracciones de los archivos necesarias para recuperar toda su Información, con esto, es posible reproducir el archivo que se perdió a partir de esta información de paridad.

RAID-5: El problema que presenta RAID-3 es que el "disco de paridad" es un punto crítico en el sistema; ¿qué ocurre si falla el disco de paridad? Para resolver este problema RAID-5, no solo distribuye todos los archivos en un grupo de discos ("Striping"), sino también la información de paridad es guardada en todos los discos del sistema ("Striping"). Esta configuración RAID suele ser usada en sistemas que requieren un "alto nivel" de disponibilidad, inclusive con el uso de "Hot-Swappable Drives" es posible sustituir y recuperar la Información de un disco dañado, con mínima intervención del Administrador y sin la necesidad de configurar o dar "reboot" al sistema.

5.3.3 Dispositivos de almacenamiento

Existen diferentes tipos de dispositivos de almacenamiento, los cuales se pueden utilizar en función de las necesidades de cada empresa y persona y será de acuerdo al volumen de información que se maneje, entre los que están los siguientes:

Unidades de disquete

Por muy antiguo que sea un computador, siempre dispone de al menos uno de estos aparatos. Su capacidad es insuficiente para las necesidades actuales, pero cuentan con la ventaja que les dan los muchos años que llevan como estándar absoluto para almacenamiento portátil. Los precios son variados. Los disquetes tienen fama de ser unos dispositivos muy poco fiables en cuanto al almacenaje a largo plazo de la información; y en efecto, lo son. Les afecta todo lo imaginable: campos magnéticos, calor, frío, humedad, golpes, polvo.

Discos duros

Son otros de los elementos habituales en los computadores, al menos desde los tiempos del 286. Un disco duro está compuesto de numerosos discos de material sensible a los campos magnéticos, apilados unos sobre otros; en realidad se parece mucho a una pila de disquetes sin sus fundas y con el mecanismo de giro y el brazo lector incluido en la carcasa. Los precios son muy variados, dependiendo de la tecnología.

Dispositivos removibles

Estos dispositivos no aparecen actualmente de manera estándar en la configuración de un PC. Se denominan removibles porque graban la información en soportes (discos o cartuchos) que se pueden remover, extraer. La clasificación hace referencia a su capacidad de almacenamiento, por ser ésta una de las principales características que influyen en la compra o no de uno de estos periféricos, pero para hacer una compra inteligente se deben tener en cuenta otros parámetros que se comentan en la explicación como velocidad, durabilidad, portabilidad y el más importante de todos: su precio.

Dispositivos hasta 250 MB de capacidad

Son dispositivos que buscan ofrecer un sustituto de la disquetera, pero sin llegar a ser una opción clara como backup (copia de seguridad) de todo un disco duro. Hoy en día muchos archivos alcanzan fácilmente el megabyte de tamaño, y eso sin entrar en campos como el CAD o el tratamiento de imagen digital, donde un archivo de 10 MB es muy común. Por ello, con estos dispositivos podemos almacenar fácil y rápidamente cada proyecto en un disco o dos, además de poder realizar copias de seguridad selectivas de los datos del disco duro, guardando sólo los archivos generados por las aplicaciones y no los programas en sí.

Zip - 100 MB

Ventajas: portabilidad, reducido formato, precio global, muy extendido. Desventajas: capacidad reducida, incompatible con disquetes de 3,5". Estos discos son dispositivos magnéticos un poco mayores que los clásicos disquetes de 3,5 pulgadas, aunque mucho más robustos y fiables, con una capacidad sin compresión de 100 MB una vez formateados. Este tamaño les hace inapropiados para hacer copias de seguridad del disco duro completo, aunque idóneos para archivar todos los archivos referentes a un mismo tema o proyecto en un único disco. Su velocidad de transferencia de datos no resulta comparable a la de un disco duro actual, aunque son decenas de veces más rápidos que una disquetera tradicional (alrededor de 1 MB/s para la versión SCSI). En todo caso, los discos son bastante resistentes, pero evidentemente no llegan a durar lo que un CD-ROM o un magneto-óptico.

SuperDisk LS-120 - 120 MB

Ventajas: reducido formato, precio global, compatibilidad con disquetes 3,5". Desventajas: capacidad algo reducida, menor aceptación que el Zip. Estos discos son la respuesta a la cada vez más común desesperación del usuario que va a grabar su trabajo en un disquete y se encuentra con que supera los 1,44 MB. El SuperDisk, que aparenta ser un disquete de 3,5" algo más grueso, tiene 120 MB de capacidad. Sin embargo existen rumores sobre la descontinuación de estos dispositivos.

Dispositivos hasta 2 GB de capacidad

A estos dispositivos se les podría denominar multifuncionales; sirven tanto para guardar grandes archivos o proyectos de forma organizada, como para realizar copias de seguridad del disco duro de forma cómoda e incluso como sustitutos de un segundo disco duro, o incluso del primero.

Grabadores de CD-ROM

No hace falta enumerar las ventajas que tiene el poseer uno de estos aparatos, sobre todo en casa. Las velocidades de lectura y escritura han aumentado mucho, y su precio los hace accesibles.

Jaz - 1 GB ó 2 GB

Ventajas: capacidad muy elevada, velocidad, portabilidad. Desventajas: inversión inicial, no tan resistente como un magneto-óptico, cartuchos relativamente caros. Las cifras de velocidad son: poco más de 5 MB/s y menos de 15ms. Esto es porque es prácticamente un disco duro al que sólo le falta el elemento lector-grabador, que se encuentra en la unidad. Por ello, posee las ventajas de los discos duros: gran capacidad abajo precio y velocidad, junto con sus inconvenientes: información sensible a campos magnéticos, durabilidad limitada en el tiempo, relativa fragilidad.

Dispositivos de más de 2 GB de capacidad

En general podemos decir que en el mundo PC sólo se utilizan de manera común dos tipos de dispositivos de almacenamiento que alcancen esta capacidad: las cintas de datos y los magneto-ópticos de 5,25". Las cintas son dispositivos orientados específicamente a realizar copias de seguridad masivas a bajo coste, mientras que los magneto-ópticos de 5,25" son mucho más versátiles, y muchísimo más caros.

Cintas magnéticas de datos - hasta más de 4 GB

Ventajas: Precios accesibles, extendidos, enormes capacidades.
Desventajas: extrema lentitud, útiles sólo para backups.

Las cintas de datos no tienen un tamaño mayor a las de música o las cintas de vídeo de 8mm. Los datos se almacenan secuencialmente, por lo que si quiere recuperar un archivo que se encuentra a la mitad de la cinta se deberá esperar varias decenas de segundos hasta que la cinta llegue a esa zona; y además, los datos no están en exceso seguros, ya que como dispositivos magnéticos les afectan los campos magnéticos, el calor, etc, además del propio desgaste de las cintas. A continuación veremos algunos modelos.

Las cintas DAT (Digital Audio Tape)

El acceso sigue siendo secuencial, pero la transferencia de datos continua (lectura o escritura) puede llegar a superar 1 MB/s. Sin embargo, el precio resulta prohibitivo para un uso no profesional, ya que su costo es alto.

Dispositivos magneto-ópticos

Ventajas: versatilidad, velocidad, fiabilidad, enormes capacidades. Desventajas: precios elevados. Los magneto-ópticos de 5,25" se basan en la misma tecnología que sus hermanos pequeños de 3,5", por lo que atesoran sus mismas ventajas: gran fiabilidad y durabilidad de los datos a la vez que una velocidad razonablemente elevada.

Software de respaldo y respaldo "On Line"

Algún software y servicios que nos ayudan a mantener un orden en nuestros respaldos, los cuales podemos clasificarlos en:

- Software de respaldo tradicional: Con estos productos, podemos elegir los archivos o carpetas a guardar, seleccionar un dispositivo de almacenamiento, y ejecutar el respaldo sin ayuda.

- Software de respaldo de fondo: Ideal para los usuarios que no tienen una "disciplina" en respaldar su información. Estos programas hacen una copia de los archivos en forma automática, "sin molestar".

Los servicios de respaldo en Internet tienen muchas ventajas: guardan la información fuera del lugar de trabajo y evitan tener que intercambiar medios.

5.4 Crímenes y Criminales de la Información (Hackers)

Las leyes relacionadas a los contratos y empleados son difíciles, pero por lo menos tanto los objetos como los contratos y los propietarios son entidades para las cuales existen precedentes legales. En cambio los crímenes que se relacionan con computadoras están en una área de ley que es menos clara que con las otras. Por lo que si son características anteriores las leyes se tienen que adecuar para caber dentro de estos nuevos objetos. Con respecto a los crímenes se deben considerar crear nuevas leyes.

El crimen se clasifica de gente y otros objetos. Se considera crimen a un acceso no autorizado a un sistema de cómputo.

Hasta ahora no ha sido claro, que la comunidad legal no se ha podido acomodar a los avances en la tecnología de la manera en que el reto de la sociedad lo ha hecho. Algunas personas en el proceso legal no entienden de computadoras ni de computación, así que no están capacitados para darle un seguimiento adecuado a los crímenes que se cometen en contra de los sistemas de cómputo. El crear y cambiar las leyes es un proceso lento; y si se les agrega el dinamismo con el que cambia la tecnología, este proceso se retarda aún más. Otro concepto que se debe considerar, es que la computadora puede tomar varios roles en un crimen:

- Una computadora puede ser objeto, medio o sujeto de un crimen
- Una computadora puede ser atacada, utilizada para atacar o para realizar un crimen.

Algunas de las principales razones por las que los crímenes computacionales son difíciles de determinar son:

- Comprensión. Ni las cortes, ni los abogados, ni los policías o el jurado son muy sabios en cómputo.
- Huellas. Policías y la corte por años han dependido en evidencias tangibles, tales como las huellas de los dedos.
- Bienes. El robo de un disquete con información valiosa no es lo mismo que el robo de un diamante.
- Jóvenes. Muchos crímenes se relacionan con jóvenes y sus crímenes se toman como una inmadurez, sin dárseles un seguimiento adecuado.

Las victimas de los crímenes analizando la situación en que se encuentra la ley, prefiere no acudir a ella, porque en muchos casos seria perdida de tiempo además de que pocos abogados conocen del tema y podría ser muy difícil y costoso llevar un juicio. Sin mencionar la publicidad negativa que se ineraria en su contra, donde el publico perdería la confianza en sus sistemas de computo y por lo tanto en ellos.

Muchos ataques mencionados caen en la categoría de crímenes y esta va a depender en quien lo comete y las intenciones que pueda tener. A veces estas categorías se traslapan.

Hacker

Hacker es una expresión idiomática inglesa cuya traducción literal al español tiene varios significados, siendo el más popular el atribuido a "una persona contratada para un trabajo rutinario" y que por la naturaleza del mismo su trabajo es tedioso, entregado, hasta se diría que maniático.

La palabra "hack" en inglés significa "hacha" en español. Como si fuesen taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo.

La palabra hacker aplicada en la computación se refiere a las personas que se dedican a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen "un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".

"La revolución de la computación ha sido lograda gracias a los hackers", afirman categóricamente los famosos estudiosos e investigadores pioneros de los virus de computadoras Rob Rosenberg y Ross Greenberg.

"Un Hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar distinto, alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, solo le importa las bellezas que pueda crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental... Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos métodos. Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa."

Hacker es un aficionado a los ordenadores o computadoras, un usuario totalmente cautivado por la programación y la tecnología informática. En la década de 1980, con la llegada de las computadoras personales y las redes de acceso remoto, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar o alterar los programas o los datos almacenados en las mismas. También se utiliza para referirse a alguien que, además de programar, disfruta desmenuzando sistemas operativos y programas para ver cómo funcionan. Además hacker se define como una persona que aprende los detalles de los sistemas de cómputo y como extender sus capacidades, opuesto a la mayoría de los usuarios, quienes prefieren aprender el mínimo necesario.

El Hacking se considera una ofensa o ataque al Derecho de la gente, y no tanto un delito contra un Estado concreto, sino más bien contra la humanidad. El delito puede ser castigado por los tribunales de cualquier país en el que el agresor se halle. La esencia del Hacking consiste en que el pirata no tiene permiso de ningún Estado soberano o de un Gobierno en hostilidades con otro. Los hackers son considerados delincuentes comunes en toda la humanidad, dado que todas las naciones tienen igual interés en su captura y castigo.

Desde hace algún tiempo el FBI de los Estados Unidos emplea el software "Carnivore" que espía a los usuarios de Internet y recientemente el Senado norteamericano le concedió la facultad de utilizarlo sin autorización judicial.

5.5 Leyes aplicables y Sanciones

El sistema legal se ha adaptado en la medida a sus posibilidades a la tecnología de la computación, reutilizando algunas viejas formas de protección legal y creando leyes donde las existentes no se pueden adecuar. Las leyes y la seguridad de cómputo se relacionan en varias formas.

Las leyes regulan al aplicar los derechos de individuos para mantener asuntos personales en forma privada, también se regula el uso, desarrollo de programas dados. Patentes, Derechos de Autor y Secretos de Mercado son mecanismos legales que protegen los derechos de desarrolladores y propietarios de datos y de programas. Un aspecto muy importante en la seguridad del cómputo es controlar el acceso a los programas y los datos; tales mecanismos son soportados por la ley.

Las leyes también tienen acciones que pueden ser tomadas para proteger los secretos, integridad y disponibilidad de la información y servicio de cómputo. La ley no siempre provee de un control adecuado, de en los asuntos de cómputo, ni en otros. En lo referente a la computación, la ley se desenvuelve lentamente, debido a que las computadoras compradas con otros bienes son totalmente nuevas.

Gracias a esto su lugar dentro de la ley esta muy bien establecido. Conforme los casos se van presentando la ley se va definiendo. Pero aun la ley no alcanza cubrir todos los actos impropios que se cometen a través de las computadoras. Además tanto los jueces, abogados y la policía no entienden la forma como opera y funciona una computadora, así que es muy difícil que determinen como la computación se relaciona con otras partes de la ley.

Las leyes referentes a la seguridad de sistemas de cómputo afectan a programadores, diseñadores, usuarios y a quienes mantienen los sistemas de cómputo, así como las bases de datos. Estas leyes proveen de protección pero también regulan el comportamiento de la gente que usa las computadoras. Es indispensable entender las diferencias fundamentales entre el tipo de protección que estas tres leyes proveen y como se deben aplicar. Es mejor prevenir una violación del sistema que procesarlo por el delito ocurrido.

Protección de objetos de cómputo.

En la protección legal para los objetos relacionados con la computación, a continuación describiré como se aplican.

Protección de Hardware.

Tanto a los chips, como los drives o los discos de almacenamiento pueden ser patentados al igual que toda la computadora, y si alguien inventa algo nuevo proceso de manufactura también puede obtener una segunda patente.

Protección del Firmware.

La situación se hace menos clara en lo concerniente al microcódigo. Si bien los mecanismos físicos en los que el microcódigo es almacenado pueden ser patentados, como es el caso de un chip de propósito especial que realiza una tarea especifica. Los datos que están contenidos en los mecanismos generalmente no son patentados.

La ley de protección más apropiada para este tipo de mecanismos seria el de Secreto de mercado.

El Secreto de Mercado es la información que da una compañía sobre sus competidores. La característica principal es que siempre debe mantenerse en secreto. Si alguien obtiene un Secreto de Mercado de manera inapropiada y tiene los beneficios con ellos. El dueño puede demandar para recobrar los beneficios ganados por el otro, así como daños y perjuicios y los costos legales.

Derecho de Empleado y Contratantes

Las empresas contratan empleados para generar ideas y hacer productos. La protección ofrecida por derechos de Autor, Patentes y Secreto de Mercados aplica a las ideas y productos. Pero el considerar quien es dueño de la idea es más complejo. La propiedad es una característica de la seguridad en cómputo, porque se relaciona con los derechos de un patrón a proteger.

Propiedad de los productos

La interpretación de la ley de propiedad es muy difícil ya que se tiene que considerar varios aspectos como:

- La capacitación dada al empleado
- El tiempo laboral que dedico para elaborarlo (en casa o el trabajo)
- La idea de elaboración.

La persona que tiene la propiedad de un trabajo patentado es inventor. Si la empresa lo permite el empleado es quien puede patentar el invento, pero generalmente es la empresa quien lo patenta porque es ella quien paga al empleado para que realice el invento.

Leyes aplicables en un centro de cómputo

La Unidad de Servicios de Cómputo Académico de la Secretaria General tiene como objetivo fundamental, proporcionar servicios de cómputo para la Facultad de Ingeniería y es la encargada de coordinar las salas.

Las actividades que desarrollen los usuarios dentro de las instalaciones, deben ser de carácter académico y de manera personal, por lo cual queda estrictamente prohibido el uso de juegos de computadora, letreros en sistemas multiusuarios a los demás usuarios, imágenes, texto o dibujos que no cumplan con el carácter de académico que es el fin especifico dentro de las actividades que desarrollan los usuarios.

Cualquier actividad que ponga en peligro la integridad de las personas dentro de las instalaciones será sancionada severamente conforme a la Legislación Universitaria.

Solo tendrán acceso a las salas los usuarios que cuenten con equipo asignado por los asesores.

Si un usuario detecta alguna falla en el equipo que se le asigno al inicio de su sesión, deberá reportarlo al control de las salas. Si un usuario provoca un desperfecto, deliberadamente o por desconocimiento, será sancionado.

Queda absolutamente prohibido ejecutar cualquier ejercicio, programa o actividad que por su naturaleza pudiera atentar contra la seguridad de los sistemas, aunque tales actividades tuvieran carácter académico.

A los usuarios que sean sorprendidos haciendo uso indebido de los equipos se les cancelara el servicio por el resto del semestre.

Sanciones

1. Se les cancelará el servicio permanente si se usa el equipo, para editar imágenes que no tengan relación con actividades académicas o se haga mal uso del mismo.

2. Se les cancelara el servicio permanente si se daña el equipo (a nivel software o hardware), o se extraiga algún accesorio.

3. A toda persona que sea sorprendida modificando, dañando o haciendo mal uso del equipo de hardware, software, o que viole los lineamientos establecidos en los reglamentos universitarios, se le cancelará el servicio definitivamente. En el caso dado deberá restituir los bienes dañados, o será remitido ante las autoridades universitarias correspondientes.

4. Queda estrictamente prohibido el uso de chat o cualquier software o página parecida, visitar paginas pornográficas o que no tengan fin académico.

5. No esta permitido cambiar el papel tapiz, cambiar la configuración o instalar algún software.

6. Esta prohibido cambiarse de maquina o andar recorriendo las salas.

CAPÍTULO 6

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD

CASO: LABORATORIO DE LA UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO DE LA FACULTAD DE INGENIERÍA

6.1 Unidad de Servicios de Cómputo Académico (UNICA)

En este capítulo se abordará la problemática particular del caso de UNICA; en base al análisis realizado y a las medidas que se tomaron para su mejor funcionamiento y seguridad de la sala.

Primero hablaremos lo que es UNICA, que se define así mismo en varios aspectos que a continuación se describen:

Historia

Surge en el año de 1994 cuando se decide reestructurar el Centro de Cálculo de acuerdo a sus objetivos y funciones, con la finalidad de proporcionar una mayor eficiencia en el desempeño del personal. Con base a esto se crean dos Unidades para desempeñar el trabajo que realizaba el Centro de Cálculo. La Unidad de Servicios de Cómputo Académico (UNICA) y la Unidad de Servicios de Cálculo Administrativo (USECAD), son las dos unidades creadas para llevar a cabo las tareas Académicas y Administrativas de la Facultad de Ingeniería.

Organización

La Unidad de Servicios de Cómputo Académico se compone del Departamento de Servicios Académicos (DSA), el Departamento de Investigación y Desarrollo (DID), el Departamento de Redes y Operación de Servidores (DROS), la Coordinación de Salas de Cómputo (CSC) y el Departamento de Seguridad y Cómputo.

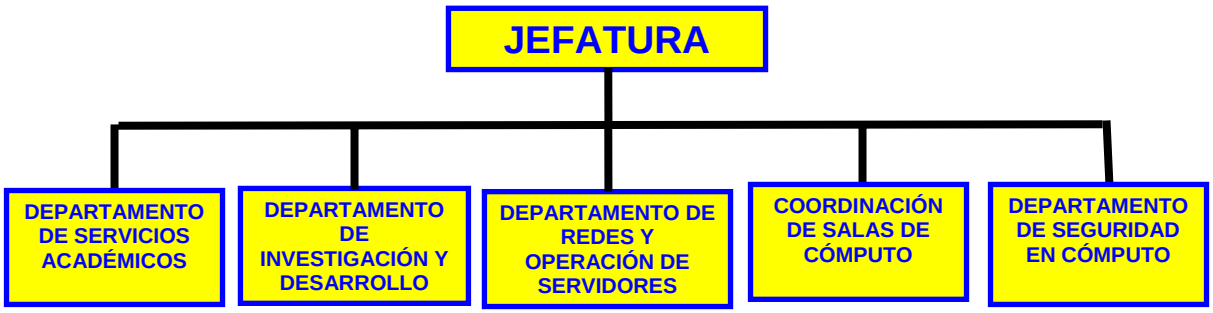


Figura 6.1 Organigrama de UNICA

Misión

La Unidad de Servicios de Cómputo Académico (UNICA) es una dependencia de la Secretaría General de la Facultad de Ingeniería, cuya finalidad principal es la de proporcionar, en el ámbito institucional, los servicios de apoyo en cómputo que la comunidad de la Facultad requiere, recursos de cómputo comerciales y de alta especialización que el avance de la educación, el desarrollo de la informática y el ejercicio profesional demanden.

Política de Calidad

En UNICA, el objetivo principal es cumplir con los requerimientos de los clientes en el área de cómputo, teniendo como meta elevar la calidad de sus productos y servicios, para ello se comprometen en un proceso de mejora continua.

Coordinación de Salas de Cómputo (CSC)

Su función principal es la de proporcionar el servicio de cómputo y de impresión a los alumnos de la Facultad, para que éstos puedan realizar sus trabajos y tareas de investigación, para lo cual además les proporciona servicio de correo electrónico, acceso a Internet y servicios varios de apoyo en materia de cómputo.

Al efecto se cuenta con cuatro salas de atención a usuarios, una en el edificio principal, dos en el anexo de ingeniería y una en el edificio de Posgrado; en las que se cuenta con un total de 253 computadoras personales, 13 impresoras y 5 estaciones de trabajo, como equipo al servicio exclusivo de los alumnos, el cual se complementa con 9 servidores y las computadoras necesarias para la administración y control del servicio.

Las salas funcionan de lunes a viernes de 9 de la mañana a 9 de la noche, y se cuenta además con el servicio de asesoría especializada, brindada por becarios instructores, prácticamente durante todo el día. Los servicios se ofrecen en plataforma Windows, plataforma Linux y plataforma Solaris; y se cuenta con la paquetería de uso y aplicación más frecuentes, la cual se actualiza y complementa constantemente.

6.2 Políticas de UNICA

INTRODUCCIÓN

En este apartado se presentan las políticas existentes dentro de la Facultad de Ingeniería principalmente en la sala No. 2 de UNICA del Anexo de la Facultad de Ingeniería, las cuales tienen por objetivo un alcance institucional, que permiten crear y establecer una educación y una filosofía sobre la postura que en materia de seguridad en cómputo debe tener la institución respecto a los riesgos que la rodean.

Dentro de las políticas que existen en la sala de cómputo se definen lineamientos los cuales establecen los derechos y obligaciones de lo que está permitido y lo que no esta permitido a los usuarios tanto dentro de la institución, así como fuera de ella, esto es con el propósito de proteger la información, los equipos y en general las instalaciones donde se encuentran los sistemas de cómputo.

Un principio fundamental de la seguridad dentro de la Facultad de Ingeniería es “Lo que no se permite expresamente, está prohibido".

Es benéfico para cualquier estudiante o miembro de la comunidad universitaria contar con una conexión a Internet ya que a través de ella se puede tener acceso a un vasto mundo de recursos de información ya que las oportunidades que tenemos con esta conectividad son casi ilimitadas, mas no así los recursos computacionales y de conectividad disponible dentro de la Universidad. Por lo que se requiere de reglas y precauciones, para asegurar un uso óptimo y correcto de los recursos. En lo que concierne a la Facultad de Ingeniería y explícitamente en la Unidad de Servicios de Cómputo Académico se cree firmemente en que el desarrollo de políticas que sean bien entendidas, que circulen ampliamente y que sean efectivamente implementadas, con llevará a hacer de la red de cómputo y el Internet en UNICA dentro de la Facultad un ambiente más seguro y productivo para estudiantes y miembros en general de la comunidad universitaria.

6.2.1 Políticas de seguridad

Las políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos que tanto usuarios como administradores deben seguir ante un incidente de seguridad.

La política que seguiremos será prohibitiva: "Lo que no este explícitamente permitido queda prohibido."

Los usuarios del equipo de cómputo explícitamente dentro de la red de UNICA en la sala de cómputo ubicado en la División de Ciencias Básicas deben ser:

- La comunidad universitaria vigente de la Facultad de Ingeniería que hayan realizado su trámite de registro.
- El personal que labora realizando actividades académicas y de investigación legitimas, que hayan tramitado permiso para utilizar los equipos de cómputo por parte del Jefe de UNICA.

Por otra parte no esta permitido el uso de la red de UNICA por individuos u organizaciones que no sean parte del personal, estudiantes o afiliados legítimos, sin previa autorización del jefe de UNICA.

6.2.2 Políticas de Seguridad Física

Las medidas que se usan para proteger las instalaciones en las que se encuentra una red de cómputo son muchas como lo son: llaves, candados, tarjetas de acceso, puertas, ventanas, alarmas, vigilancia, etc.; y las políticas físicas que existen actualmente, se basan en las Políticas Generales de la Facultad de Ingeniería y están por parte del CACFI (Comité Asesor de Cómputo de la Facultad de Ingeniería) en la salas de cómputo de UNICA son:

- Mantener las computadoras libres de polvo y temperaturas extremas.
- Colocar las computadoras fuera del alcance de rayos solares, vibraciones, insectos, ruido eléctrico y filtraciones de agua, etc.
- Todos los servidores deberán estar ubicados en lugares de acceso físico restringido y tener puertas con chapas para acceder a ellos.
- Se prohíbe el consumo de alimentos y bebidas donde se encuentre equipo de cómputo.
- El lugar donde se encuentran los servidores cuenta con instalación eléctrica adecuada, entre sus características se puede mencionar que son con tierra física. Y dichos equipos cuentan con no-breaks.
- El lugar donde se encuentran los servidores mantienen condiciones de higiene.
- Se cuenta con extinguidores en las salas de cómputo, los cuales son revisados periódicamente en cuanto a su nivel de carga.
- Las salas de cómputo de UNICA cuenta con una salida de emergencia.
- En caso de falla del equipo, sé reportar inmediatamente al Jefe del CSC.

- Se apagan los equipos personales cuando se abandona temporal o definitivamente el área de trabajo.

6.2.3 Políticas de Cuentas

Estas políticas establecen las características y requisitos que deben tener las cuentas de las máquinas y como pueden ser usadas por la comunidad de la Facultad de Ingeniería, así como a quién le pueden ser otorgadas, y quién es el encargado de asignarlas. En las Salas de cómputo de UNICA no existen cuentas de usuarios, sólo existen cuentas máquina. Las políticas existentes en las salas de cómputo de UNICA son:

- Las cuentas son otorgadas únicamente a usuarios autorizados.
- Una cuenta esta conformada por un nombre de usuario.
- La asignación de cuentas es realizada por el administrador de los servidores de UNICA.
- Las cuentas máquina son estrictamente personales e intransferibles.

6.2.4 Políticas de Contraseñas

Son políticas muy importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez única manera de autenticación y, por tanto, la única línea de defensa contra ataques. Las políticas existentes en las salas de cómputo de UNICA son:

- Los administradores de los servidores son responsables de asignar las contraseñas a los equipos que utiliza el personal que labora en las salas de cómputo de UNICA así como de los servidores.
- Se cuenta con contraseñas no débiles para los servidores y equipos del personal de la sala.

6.2.5 Políticas de Control de Acceso

Especifican cómo deben acceder los usuarios al sistema, desde dónde y de qué manera deben autentificarse. Las políticas existentes en las salas de cómputo de UNICA son:

- El acceso a áreas críticas será restringido solo al personal encargado de la Administración de las Salas de Cómputo (CSC) y personal del Departamento del (DROS).
- Todos y cada uno de los equipos son asignados a un usuario, por lo que es responsable hacer buen uso de los mismos.
- Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que UNICA emita.
- Los administradores son responsables de proporcionar a los usuarios el acceso a los recursos informáticos con aplicaciones que permitan una comunicación segura y cifrada.
- El Departamento de Servicios Académicos es el responsable de difundir el reglamento para las salas de cómputo de UNICA.
- El acceso a Internet en la Facultad de Ingeniería debe hacerse desde una estación debidamente registrada y / o autorizada por el grupo de Servicios de Redes. Dicho de

otra forma, la computadora debe estar registrada dentro del DNS *(Domain Name Server)* primario de la universidad y estar localizado con una dirección IP legitima.

- Tendrá acceso a los sistemas administrativos solo el personal de UNICA que es responsable de los servidores.

- El control de acceso a cada sistema de información de UNICA será determinado por el DROS.

- Corresponde al DROS administrar, mantener y actualizar la infraestructura de la Red de UNICA.

6.2.6 Políticas de Uso Adecuado

Especifican lo que se considera un uso adecuado o inadecuado del sistema por parte de los usuarios, así como lo que está permitido y lo que está prohibido dentro del manejo de los sistemas de cómputo. Las políticas existentes en las salas de cómputo de UNICA son:

- Realizar sus tareas con fines académicos que estén asociadas con los programas académicos de Ingeniería.

- Utilizar software de aplicación ya instalado.

- Utilizar los servicios de impresión donde se brinden.

- La cuenta de un usuario es personal e intransferible, por lo cual no se permite que este comparta su cuenta ni su contraseña con persona alguna, aún si ésta acredita la confianza del usuario.

- Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como: programas que rastrean vulnerabilidades en sistemas de cómputo propio o ajeno.

- Está estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador.

- No se permite instalar programas y software propio, en caso de requerirse deberá solicitarlo al administrador del sistema.

- No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro. Por lo cual se prohíbe descargar (o proveer) música, imágenes, videos, chatear, etc., con fines de ocio.

6.2.7 Políticas de Correo Electrónico

Establece el uso adecuado del servicio de correo electrónico, los derechos y obligaciones que el usuario debe hacer valer y cumplir al respecto. Las políticas existentes en las salas de cómputo de UNICA son:

- El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo, donde el administrador del sistema podrá auditar dicha cuenta.

6.2.8 Políticas de Uso De Direcciones IP

El área responsable en representar a la Facultad de Ingeniería ante DGSCA es la Secretaría General. Las políticas existentes en las salas de cómputo de UNICA son:

- El administrador de red deberá contar con un registro de sus direcciones IP utilizadas.
- Ninguna área puede hacer uso de una dirección IP que no le corresponda, sin autorización expresa y escrita del administrador del área en cuestión.
- En el campus de C.U. No se permiten el uso de servidores de DHCP con direcciones IP homologadas.
- No se permiten utilizar en subredes de una zona, rangos de otras zonas. Por ejemplo de la en la zona A, utilizar, rangos de la zona C.
- Cada equipo que se incorpore a la red Internet deberá tener autorización del administrador de red del área en cuestión.
- Las direcciones IP que podrán otorgarse serán homologadas o privadas. Las homologadas sólo serán otorgadas si se justifican su uso y disponibilidad. Para asignar una dirección IP deberá justificarse su utilización y solicitarla al administrador o responsable de cómputo para su autorización.
- El administrador de red podrá realizar reasignaciones de los rangos de las direcciones IP homologadas y privadas para un mejor desempeño de la red.

6.2.9 Políticas de Contratación y Finalización de Relaciones Laborales de Recursos Humanos en Sistemas Informáticos.

Las políticas existentes en las salas de cómputo de UNICA son:

- No podrán ser contratados personas como administradores de sistemas o en áreas de seguridad informática que hayan tenido responsabilidades en incidentes graves de seguridad en cómputo.
- Al finalizar una relación laboral los administradores o encargados de sistemas deberán entregar todas las cuentas y passwords de los sistemas críticos.
- Los responsables de sistemas deberán cambiar todos los passwords críticos cuando un administrador de su área deje de prestar sus servicios.

6.2.10 Políticas de Sanciones

En caso de algún incidente de seguridad grave, es decir cuando se pone en riesgo la seguridad de un sistema de cómputo, como:

- Borrar, modificar Información.
- Difundir información confidencial.
- Copiar Información confidencial.
- Ataques maliciosos a equipos de cómputo.

- Ejecución de Programas para obtener privilegios y que sean exitosos.
- Entrar a correos de cuentas ajenas.
- Un incidente donde este involucrado un administrador de sistema u trabajador de la UNAM.
- Infectar intencionalmente un servidor con virus.
- Modificar Configuraciones de Switches y routeadores sin ser responsables del equipo.
- Daño físico intencional a los medios de comunicación de la red, como fibra óptica, UTP, Switches, hubs, routeadores, transceivers.

Si llegase a ocurrir un incidente grave se reporta al Departamento de Seguridad de la Facultad de Ingeniería y se procede al Departamento de Seguridad de DGSCA y se seguirán los procedimientos establecidos por ellos. Como medida precautoria y teniendo como prioridad el mantener la seguridad de los sistemas, las cuentas y equipos involucrados se deshabilitarán en toda la Facultad hasta que se deslinden las responsabilidades del incidente.

Las sanciones existentes en las salas de cómputo de UNICA son:

ACTIVIDAD NO LÍCITA	SANCIÓN
Consumo de alimentos, bebidas, utilización de los servicios por ocio.	Suspensión del servicio por un día. Reincidencia. Cancelación de los servicios por un mes en todas las áreas de la Facultad de Ingeniería
Acceso con una cuenta diferente a la propia, con permiso del propietario	Suspensión por un mes de los servicios en la Facultad de Ingeniería, del que presta y del que usa la cuenta. Reincidencia. Suspensión por un semestre.
Ejecución de programas que intenten adivinar cuentas y passwords locales o remotos	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. Cese definitivo de los servicios de cómputo, durante toda su carrera.
Ejecución de herramientas para rastrear vulnerabilidades en sistemas de cómputo propio u ajeno.	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. Cese definitivo de los servicios de cómputo, durante toda su carrera.
Hacer uso de programas que explotan alguna vulnerabilidad del sistema.	Suspensión de los servicios por un año en todas las áreas de la Facultad. Reincidencia. Cese definitivo de los servicios de cómputo, durante toda su carrera.

Tabla 6.1 Sanciones existentes en UNICA.

Ahora para realizar el estudio del caso practico el cual es la sala No. 2 de UNICA, F. I., se vera lo que es la problemática, el análisis particular, para así poder dar la propuesta de soluciones, para la cual nos basaremos en el método octave-s.

Este modelo nos sirve dado que la metodología que se utilizará se basa en la descrita por operación de amenaza crítica, recurso y evaluación de vulnerabilidad (octave) desarrollada por el grupo survivable enterprise management (sem) perteneciente al computer emergency response team (cert) http://www.cert.org/octave.

El método OCTAVE-S se desarrolla en tres fases, como lo vimos en el capítulo 2, que se conforman por varios pasos, para analizar los aspectos organizacionales y tecnológicos; y obtener una visión de las necesidades requeridas en cuanto a seguridad.

Recordando cada fase se desarrolla de la siguiente forma:

Fase 1: Desarrolla una lista de elementos a proteger y ataques que los afectan.

En esta fase se determinan qué recursos o elementos son los más importantes, qué es lo que se hace actualmente para protegerlos y cómo pueden ser amenazados.

Fase 2: Identifica los puntos vulnerables en la infraestructura.

A través de esta fase se conocerán cuales son los puntos vulnerables dentro de la infraestructura actual que puedan permitir acciones no autorizadas a los elementos que se desean proteger.

Fase 3: Desarrollo de planes y estrategias de seguridad.

En esta fase se analizarán los riesgos que pueden afectar a los elementos críticos y se decidirá cómo protegerlos de dichos riesgos.

El método octave-s se puede utilizar para evaluar toda la infraestructura de tecnologías de información de cualquier institución, como pueden ser información, sistemas, software y hardware.

A continuación empezaremos con el estudio.

6.3 Planteamiento de la Problemática

Al realizar el estudio de la sala No. 2 de UNICA, nos dimos cuenta de que existen varios aspectos por mejorar, tanto a nivel físico como a nivel lógico y administrativo.

Dentro de los puntos de mejoras que se tienen a nivel físico se pueden mencionar los siguientes donde hay que poner mucha atención en el mejoramiento de la sala.

1. Falta de aire acondicionado. Ya que tanto a los usuarios como al personal que ahí labora les es incomodo trabajar, debido al calor que se encierra dado que en algunas ocasiones es muy elevado.

2. Dentro de la sala No. 2 de UNICA encontramos que los cables de conexión de las computadoras, no se encuentran adecuadamente sujetados en su lugar, por lo que cuando la gente pasa entre las filas se puede tropezar con los mismos ya sean de corriente o cables de red de las máquinas ya que estos no están en las canaletas lo que puede provocar accidentes, o desconexión de la máquina.

3. Se observa que las señalizaciones dentro de la sala necesitan estar en lugares mas visibles, y colocar otras más que indiquen las salidas de emergencia, accesos sólo al personal autorizado, señales de no comer, no fumar, etc.

4. Se encontraron ventanas en el interior de la sala a las cuales se les había retirado las ventilas, se nos informo que tuvieron que retirarse por un accidente que hubo. Citando el caso de que un usuario abrió la ventila y se le cayó una rejilla de vidrio provocándole una lesión.

5. En la temporada de lluvias se filtra el agua en las salas, esto puede causar algún accidente. (que alguien se resbale o que provoque un corto circuito debido al piso mojado)

6. Se necesita capacitación al personal en caso de siniestro, en la utilización de extinguidores, o en su defecto que hacer en caso de alguna emergencia, ya que no se cuenta con una brigada o equipos para responder en caso de emergencia.

7. Se carece de un formato de préstamo de equipo dentro de la misma sala. En el cual se indique hacia donde va dirigido el equipo, quien lo presta y quien se va hacer responsable durante el préstamo y en que condiciones esta el equipo a la hora del préstamo.

8. Se carece de una bitácora de fallas donde se tengan reportados los eventos de los equipos, o ante una contingencia poder contar con registros.

Dentro de los puntos de mejoras que se tienen a nivel administrativo son:

9. Cuando se inscribe al usuario no se le entrega un reglamento por escrito de las salas. Siendo esto causa de una falta de conocimiento sobre dicho reglamento, lo que provoca malos entendidos o confusiones. Aunque se encuentra publicado.

10. En las impresiones los usuarios se quejan de que en el reglamento no se especifica claramente en muchas de las restricciones que se tienen. (Como no imprimir en hojas de rehusó, o de color, membretadas, o por ambos lados).

11. No se aplican políticas de contraseñas, dado que no se cuenta con los requerimientos y características que deben de cumplir estas mismas. Tanto a administradores como a usuarios (máquinas).

A nivel lógico encontramos las siguientes deficiencias:

12. No se cuenta con un esquema de respaldos.

13. Las auditorías no se realizan de manera periódica.

14. No se cuenta con una consola de antivirus la cual permita las actualizaciones automáticas.

15. No se encuentra instalado en el servidor un firewall, ni tampoco se cuenta con un firewall externo (es un sistema de defensa que se basa en la instalación de una “barrera” entre la computadora y la red, por la que circulan todos los datos. El tráfico entre la red y la computadora es autorizado o negado por el Firewall, todo esto de acuerdo con la configuración del mismo). Tampoco se encuentra un Firewall de tipo externo.

16. Falta un Sistema Detector de Intrusos (es una herramienta de seguridad que intenta monitorizar eventos ocurridos en determinado sistema informático o red en busca de intentos de comprometer la seguridad del sistema).

17. En las máquinas de los usuarios no se cuenta con un programa que funcione como limpiador de temporales y de virus troyanos.

18. Falta más actualización de las directivas de configuración de las máquinas. (Windows Configurator y del Poledit).

19. Las auditorías en los servidores no se realizan de manera periódica.

20. Un problema es el cambio o robo de direcciones IP's. Como es el caso de que en una de las máquinas se le cambio la dirección IP y en otra se le cambio la contraseña a la máquina.

Después de haber estudiado las posibles opciones de mejora de la sala No. 2 de UNICA, procederemos a realizar el análisis particular del mismo.

6.4 Análisis Particular

Después de haber analizado la problemática de la Sala No. 2 de UNICA observamos la necesidad de proteger y reforzar sus recursos de cualquier amenaza.

Para realizar esto necesitamos analizar y reforzar la seguridad física, lógica y administrativa. A continuación presentamos un resumen de la situación actual:

- Reforzar la seguridad a nivel físico (señalizaciones, cables fuera de su lugar, aire acondicionado, capacitación al personal ante casos de siniestros, entre otros).

- Aplicar más control a usuarios, así como en el servicio de impresión y de asesorías.

- Reforzar la seguridad a nivel lógico (ya que las actualizaciones no son tan periódicas, en los antivirus, paquetería, sistemas operativos, respaldo de servidores ni depuración de los mismos, no hay instalados firewall, ni detector de intrusos).

- Las políticas de seguridad o no se aplican, o les hace falta actualización ya que no son aplicables en estos días, además se encontraron cuentas de usuarios o administrativos que ya caducaron y ese personal ya no se encuentra laborando, además de contraseñas débiles, etc.

- Sesiones abiertas de usuarios o de algunos administrativos que al momento de revisar sus correos o alguna máquina se van y se les olvida cerrar sus sesiones.

- Se necesita el contar con un plan de contingencia.

- Son débiles los procedimientos que se tienen que hacer respecto al caso de incidentes con el servidor para restablecer su servicio.

- Dada la zona geográfica en la que se encuentra la sala, existe la posibilidad de que ocurra algún terremoto, aunque es mínima y no se tienen considerado que hacer en caso de uno, es mas alto el riesgo que se corre en caso de inundación o de incendio, por lo que hay que reforzar la seguridad y tomar medidas mas especificas para resolverlos.

Para poder analizar a detalle cada uno de los puntos anteriores necesitamos evaluar los riesgos de la red y la estructura que tiene UNICA. Para poder realizar esto nos basamos en el método OCTAVE-S, en su primera y segunda fase las cuales nos indican lo siguiente:

Fase 1: Desarrolla una lista de elementos que proteger y ataques que lo afectan.

Fase 2: Identificar los puntos vulnerables en la infraestructura.

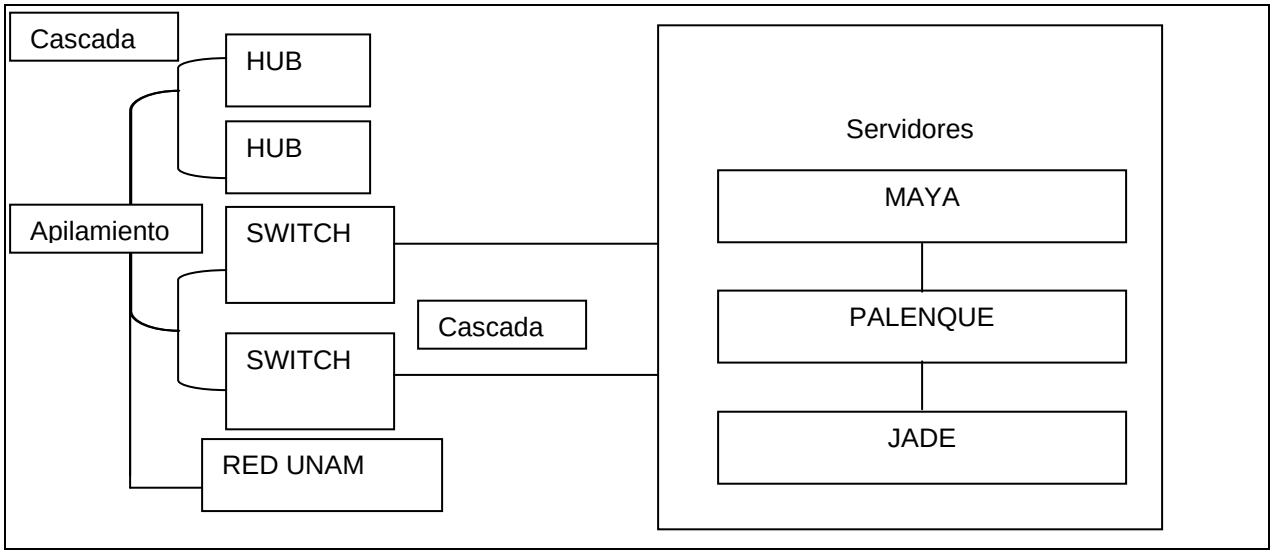


Figura 6.2 Distribución de los Switches, Hubs y Servidores

En UNICA se cuenta con 2 switches conectados a 2 hubs y estos a los 3 servidores (MAYA, JADE Y PALENQUE). Estos servidores dan los siguientes servicios:

- MAYA - Es un servidor principal, este valida las cuentas de usuarios, administrativos, además de almacenar la paquetería que se encuentra instalada en la Sala 2 de UNICA.

- PALENQUE - Es el respaldo de Maya en caso de haber un problema con el servidor principal este entra en automático a validar las cuentas y a seguir brindando el servicio. En el también se encuentra paquetería que se ocupa en la misma sala.

- JADE – Es el servidor que se esta migrando de Windows NT a Windows 2000, además de administrar la sala D que se encuentra la sala No. 2 de UNICA. Este contiene los antivirus, firewall y programas de seguridad que se ocupan en esta Sala.

Como se puede observar y de acuerdo con la segunda fase del método octave-s nuestro punto vulnerable es el que tiene mas riesgos, el cual es el servidor Maya y Jade que son los servidores que se encargan de validar las cuentas del personal administrativo y de las cuentas de los equipos, este da acceso al programa SCOSU[11] que se encuentra en la máquina de control, para dar atención a los usuarios que hagan uso del equipo de la sala No. 2.

[11] Sistema de Control de Salas de UNICA

Con respecto a los hubs y a los switchs se encuentran en un lugar seguro y bajo llave, a estos se les da mantenimiento externo y la persona que se encarga de la configuración es el jefe del DROS[12].

Las máquinas para los usuarios es menor el riesgo que se corre, ya que se cuenta con las imágenes de la paquetería que contienen las máquinas de las sala 2 y solo se necesita instalarla para seguir brindando el servicio.

El riesgo que hay con el servidor Palenque no es tan alto, porque solo es respaldo del servidor Principal, si acaso Maya tuviera problemas, este servidor entra en forma automática a validar las cuentas.

De acuerdo al Método Octave-S el o los servidores que hay que proteger son Maya y Jade, por tener el riesgo más elevado.

También es necesario la implementación y aplicación de políticas de seguridad, planes de contingencia, existe un reglamento y las políticas de seguridad que como se puede observar en la problemática y en las investigaciones que se le realizaron a la sala.

Hay que hacer conciencia tanto al personal administrativo de que no dejen sus sesiones de trabajo abiertas y a los usuarios no dejen abiertas sus sesiones de correo cuando hagan uso de los equipos, ya que hay gente maliciosa que puede hacer mal uso de sus sesiones.

Después de estudiar la problemática y el análisis particular en el siguiente capítulo se presentan las posibles soluciones, para el mejoramiento de la Sala No. 2 de UNICA.

6.5 Propuesta de Soluciones

Después de haber realizado el Análisis Particular, proponemos estas posibles soluciones basándonos en el Modelo de Seguridad del OCTAVE-S, en su tercera fase que nos indica lo siguiente:

Fase 3: Desarrollo de planes y estrategias de seguridad. En esta fase se analizarán los riesgos que pueden afectar a los elementos críticos y se decidirá cómo protegerlos de dichos riesgos.

El método OCTAVE-S se puede utilizar para evaluar toda la infraestructura de tecnologías de información de cualquier institución, como pueden ser información, sistemas, software y hardware, y las soluciones que se proponen de acuerdo al método y para este tema de tesis se dividen en 3 ramas:

- Propuesta a Nivel Físico: En ellas se recomendará que medidas preventivas y correctivas se pueden llevar a cabo ante un desastre (sismo, incendio, inundación), la protección que deben tener los equipos y la Sala.

- Propuesta a Nivel Administrativo: Se hacen recomendaciones de cómo administrar el equipo de cómputo y las reglas que rigen el mismo, tanto para los usuarios como al personal que ahí labora.

- Propuesta a Nivel Lógico: Aquí se presenta que tipo de protección deben tener los equipos y el servidor a nivel software.

[12] Departamento de Redes y Operación de Servidores

A continuación se explicará a detalle cada una de las propuestas de soluciones a la problemática en particular.

Recomendaciones a la sala, podemos mencionar de acuerdo con la problemática analizada:

1. Para el área de servidores, si no es posible contar con aire acondicionado, al menos se recomienda tener ventiladores, ya que es necesario que el lugar este a una temperatura regulada entre los 18 º y los 22º C, para el correcto funcionamiento de los equipos.
2. Para el caso de los cables de las computadoras en necesario realizar su correcto amarre formando mazos con cinchos en las partes donde estén expuestos y sea imposible cubrirlos con canaleta o con alguna parte del mobiliario par prevenir accidentes.

3. En cuanto a las señalizaciones se deben tener en lugares claros y sin obstrucciones de las cuales podemos mencionar, los de salidas de emergencia, de acceso solo a personal autorizado, señales de no comer, no fumar, extinguidores, etc.

4. Para el caso de las ventanas que son de estilo persianas horizontales se recomienda poner ventanas ya sean abatibles completas o que se abatan a la mitad para seguir contando con ventilación y así poder evitar posibles accidentes con las ventilas.

5. Se recomienda que los equipos no estén expuestos al sol, ni mucho menos al agua, por lo que se ha solicitado impermeabilizar, así como también el sellado de las ventanas y de las puertas para evitar filtraciones.

6. Se propone el caso de la capacitación al personal en caso de siniestro, que sea una capacitación continua. Se recibió una capacitación con el curso que brindo el Centro de Docencia de la Faculta de Ingeniería, impartido por la Coordinación del Grupo “Ingenio” de Protección Civil de la Facultad de Ingeniería.

7. Al llevar el control de formato de préstamo de equipo dentro de la sala se evitará la pérdida o daño del mismo al estar plenamente identificado, quien es el responsable, además se recomienda que dichos formatos estén foliados para llevar un consecutivo y tener mejor control sobre los mismos.

8. Se recomienda entregar el reglamento de la sala al momento de inscribir a cualquier usuario, esto con el fin de que el usuario conozca sus derechos y obligaciones y evitar malos entendidos al aplicarlo.

9. Es recomendable abrir una bitácora en la cual se indiquen los acontecimientos como son las causas, fecha y hora así como la o las soluciones que se aplicaron con el fin de que cualquier persona autorizada tenga una idea del historial de fallas y le sea mas fácil para la identificación y solución de los problemas.

10. Para la parte de los respaldos en los servidores es importantes contar con unidades DLT (Digital Linear Tape), donde se recomienda hacer un respaldo completo cada mes, y posteriormente los incrementales cada semana.

11. En lo que respecta a las actualizaciones de antivirus es aconsejable contar con una consola de antivirus en donde automáticamente se actualicen tanto los equipos conectados a la red como los servidores.

12. Se aconseja la adquisición de un firewall físico donde solo permanezcan abiertos los puertos más utilizados de comunicación como lo es el puerto 80. Este Firewall ya se esta implementando por el Departamento de Seguridad.

13. Es importante contar con un sistema Detector de Intrusos ya que es bien sabido que los espías son programas que se instalan sin autorización con la finalidad de buscar ya sea lista de direcciones de correos, contraseñas e instalación de barras como lo son Search Bar o Toolbar en los programas de Outlook o el navegador de Internet, se propone la instalación de paquetes que ayuden a eliminar dichos espías como son el Adware, Spy Sweeper, etc.

14. Dentro de las máquinas de usuario es necesario el constante monitoreo para su correcto funcionamiento en cuanto a virus troyanos y limpiadores de temporales por lo que se sugiere la instalación de un programa antivirus para lo cual se instaló el Panda Antivirus y un limpiador de temporales como lo es el Temp Clean.

15. Se proponen realizar auditorias bimestrales para contar con un registro de las actividades y funcionamiento de los equipos servidores, así como para prevenir posibles anomalías en su operación.

16. Es recomendable se implemente una política de contraseñas que cuenten con ciertas características como son el número de caracteres, alfanuméricas incluyendo minúsculas y mayúsculas, además de cambiarlas por lo menos cada 2 ó 3 meses en los servidores y cada 6 meses para los usuarios máquinas.

A Nivel Físico

1.- En caso de ocurrir un incendio lo que se propone es lo siguiente:

- Contar con extinguidores que sean de gas halón, CO_2 y de espuma. Los extinguidores de gas halón no dañan el equipo de cómputo ni el material eléctrico al igual que el CO_2. el único inconveniente es que es nocivo para los humanos. La espuma sólo humedece lo que se este quemando, por lo que daña el equipo electrónico, este es bueno para papel, madera y cartón.

- Los extinguidores deben estar en un lugar de fácil acceso.

- Contar con las señalizaciones de las salidas de emergencia. Además se recomienda que se capacite al personal en primeros auxilios y que hacer en caso de siniestro.

- Capacitación al personal en el uso de extinguidores.

- La pintura de la Sala se recomienda que no sea inflamable, al igual que las canaletas, el techo y piso falso o de que sean de un material resistente al fuego.

- Deben existir detectores de humo en la sala, y estos detectores deben poder distinguir los distintos tipos de gases que desprendan los cuerpos en combustión.

2.-Para el caso de ocurrir una inundación o sismo las medidas a tomar son las siguientes:

- Que los contactos no estén al nivel cerca del suelo.

- Que el cableado de los equipos esté bien amarrados para que la gente no se tropiece cuando evacuen.

- Dar instrucciones para que la salida de la sala sea con calma en el caso de sismo.

- Para evitar el daño físico a los equipos se recomienda que no estén cerca ó en el suelo, por lo menos a una altura adecuada.

A Nivel Administrativo

Para el mejor funcionamiento de la sala, en cuanto al control de equipos (prestamos, reparación y poder evitar extravíos o robos). Se proponen las siguientes medidas físicas y lógicas a nivel administrativo, para que no haya pérdida de archivos, instalación de programas que no sean de la sala, etc.

De todo esto se hará cargo el encargado de la sala y el personal de seguridad.

- El responsable tendrá las llaves de la Sala, del área de Servidores y de la Bodega.

- Se recomienda realizar un chequeo periódico a las instalaciones del suministro eléctrico, con la finalidad de mantener adecuadamente el balanceo de cargas en las fases, para no provocar una sobrecarga.

- Se recomienda la instalación de equipo adecuado para las variaciones de voltaje como banco de capacitores y supresor de picos.

- Se recomienda el chequeo de la polarización de la instalación eléctrica con el fin de asegurar la correcta operación de los equipos eléctricos.

- El responsable contará con los inventarios de los equipos con lo que cuenta la Sala, tanto para los usuarios como los del personal que ahí labora. Así como del equipo que se va a dar de baja.

- Cuando se realice el préstamo de equipo interno o externo, el responsable entregará un formato firmado, como comprobante del préstamo realizado.

- Se sugiere llevar una bitácora de incidentes, de reparación de equipo el cual tendrá el responsable, y servirá de ayuda y guía para posibles incidentes.

- Cualquier tipo de mantenimiento que se realice en la Sala, el responsable debe tener conocimiento y dar autorización del mismo.

- En cuanto al acceso a la sala los usuarios solo lo podrán realizar, siempre y cuando ya se hayan dado de alta en el sistema.

- Sólo el personal autorizado tendrá acceso al área de trabajo y con previa identificación.

También realizaremos una aportación a las políticas que administran la Salas de UNICA.

Políticas de Seguridad Física

- La puerta donde se encuentran los servidores y la bodega deben permanecer cerrada y con candados.

- El lugar donde se encuentran los servidores debe contar con aire acondicionado y buena ventilación.

- Al cerrar el área de servidores, bodega y máquinas todos los equipos tienen que estar apagados o conectados a sus no-breaks.

- El personal cuando abandone el equipo temporalmente debe apagar el equipo o bloquear su sesión de trabajo.

Políticas de cuentas

- Las cuentas que se le asignen al personal, además de las cuentas máquina tendrán una vigencia máxima de 6 meses.

Políticas de contraseñas

- Las contraseñas de los administradores, servicio social, empleados y máquinas tendrán una vigencia máxima de 6 meses.

- Las contraseñas deben ser alfanuméricas combinadas de mayúsculas y minúsculas, además de contener caracteres especiales.

Políticas de control de acceso

- El acceso a los servidores sólo es para el personal autorizado con identificación.

- El acceso a la paquetería, instalación y actualizaciones de software será de uso exclusivo de los administradores de las salas de UNICA.

- Todo el personal que se encuentre dentro de las salas de UNICA deberán portar su gafete de identificación.

Políticas de sanciones

Dentro de estas políticas mencionaremos otros casos en los cuales son incidentes de seguridad grave, es decir cuando se pone en riesgo la seguridad de un sistema de cómputo.

Esto se mostrara en una tabla ya con la sanción y si hubiera reincidencia, como:

ACTIVIDAD NO LÍCITA	SANCIÓN
Acceso a las salas de cómputo con una identificación falsa.	Suspensión del servicio por un semestre. Reincidencia. Cancelación de los servicios por el resto de la carrera en todas las áreas de la Facultad de Ingeniería
Imprimir en hojas de rehusó, membretadas.	Suspensión por una semana. Reincidencia. Suspensión por un semestre.
Imprimir sin autorización de los encargados	Suspensión del servicio por un mes. Reincidencia. Suspensión del servicio por un semestre.
Faltarle al respeto al personal.	Suspensión del servicio por un mes. Reincidencia. Cancelación de los servicios por un el resto del semestre.

Tabla 6.3 Tabla de sanciones sugeridas a UNICA.

Políticas de impresión

- El usuario debe avisar a los responsables o encargados de la unidad de que va hacer uso de las impresoras.
- El usuario solo podrá imprimir documentos de carácter académico y que sean propios.
- Las impresiones solo se podrán hacer en hojas blancas por ambos lados.

Políticas de inscripción a las salas de cómputo

- Sólo se podrán inscribir alumnos de la Facultad de Ingeniería.
- En la inscripción deberán presentar su comprobante de inscripción e identificación de la Facultad.

Políticas del Reglamento

- A todos los alumnos que se inscriban o se reinscriban a la salas de cómputo se les entregará el reglamento vigente.
- El reglamento de las salas lo deberá saber el personal.
- El reglamento deberá estar en un lugar visible en las salas.

A Nivel Lógico

En esta parte aconsejaremos las herramientas para el mejor funcionamiento del servidor y de los equipos, para que estén bien protegidos debemos de cuidar que la protección empiece desde el servidor y los clientes. Primero hablaremos del servidor y después los clientes:

- Es un servidor Windows NT 4.0 el cual primero lo vamos a proteger de manera interna con consejos prácticos de instalación y configuración para asegurar sistemas de cómputo con Microsoft Windows NT 4.0 y a si ya luego protegerlo y monitorizarlo desde afuera con diferentes herramientas.
- Aconsejamos migrar el Servidor Maya de Windows NT a Windows 2000 Server, ya que se tiene una mejor administración técnica, así como la facilidad en el mantenimiento y en conseguir las actualizaciones y parches que requiere el sistema. Es un sistema operativo más amigable en la instalación y como antes se menciono en la administración. Contiene mayores herramientas de Seguridad para el mismo Servidor y para sus clientes. Y cumple con las características de seguridad en los servicios que ofrece en la red. Proporciona mayor compatibilidad con las diferentes versiones de sistemas operativos.
- Se recomienda que también se instale un firewall o muro de fuego, que es una herramienta que actúa como una barrera protectora entre la red y el mundo exterior; también se usa para proteger del acceso a los recursos internos desde el exterior, así como para controlar los recursos que son accedidos desde la red. Recomendamos el Zone Alarm. Además de que se instale un Firewall externo que analice toda la red.
- También recomendamos el uso de un programa para monitorizar el sistema, es una herramienta que realiza un análisis automático del sistema en busca de posibles vulnerabilidades y fallos de seguridad, además, de ver si esta bien configurado y tener

instaladas las últimas actualizaciones, parches, que indique que puertos están abiertos, como lo es el Microsoft Baseline Security Analyze o el programa GFI LANguard Network Security Scanner. Este programa puede ser instalado desde un cliente y monitorizar a los clientes y al servidor. Se hace la recomendación de este software ya que es el que mas se utiliza en las salas.

- Para un mejor funcionamiento aconsejamos instalar un Sniffer que es un programa o dispositivo (puede ser un elemento de hardware, no necesariamente tiene que ser un programa), el cual analiza un determinado punto de la red con fines muy diversos. Un sniffer, analiza el tráfico de datos que pasa por un punto de la red en la que está instalado.

- Es recomendable utilizar un programa antiespias como lo puede ser el Ad-aware o el Spy Sweeper. Ambos programas sirven para limpiar todo tipo de spyware, adware, troyanos, archivos y programas espía y herramientas de monitorización como Gator. Los programas hacen uso de una extensa base de datos que va renovando periódicamente, ofreciendo siempre la mejor protección contra las amenazas más recientes. Tiene dos modalidades de análisis, una más rápida y superficial, y otra más lenta y completa. Una vez escaneado el sistema, el programa muestra los archivos de spyware detectados (en caso de tenerlos), y los lugares exactos donde se localizan. Además de ello, permite desactivarlos sin que por ello dejen de funcionar algunas aplicaciones que los llevan incorporados.

- Utilizar un antivirus el cual es un programa que suele incorporar mecanismos para prevenir, detectar y eliminar virus. Para la prevención se suelen usar programas residentes que alertan al usuario en todo momento de cualquier acceso no autorizado o sospechoso a memoria o a disco, por lo que resultan sumamente útiles al impedir la entrada del virus y hacerlo en el momento en que este intenta la infección, facilitándonos enormemente la localización del programa maligno. El antivirus que recomendamos para el servidor, la máquina que va a supervisar el servidor y los clientes es el siguiente, para los tres equipos y que sea de respaldo es el Antivirus AVG. De antivirus principal para el servidor es el Symantec Norton Antivirus y para los clientes es el Panda Antivirus. Se recomienda la instalación de dos antivirus ya que ambos antivirus se complementan ya que no existe un solo antivirus q cubra todo un sistema.

- Ponerle directiva de configuración para los clientes utilizando el software Tweak para XP y el Windows Configurator para Windows 95 y 98, esto para tener más control en los ajustes de Windows, y poder ser capaz de cambiar herramientas y accesos en Windows y no las pueden cambiar desde adentro del sistema. También sirve para realizar cambios los usuarios en el sistema operativo que sólo se pueden hacer editando directamente el registro y modificar más de un centenar de funciones de Windows.

- Aplicar las auditorias internas de los sistemas operativos del diferente Windows que se tengan instalados, para tener un control de los movimientos de los servidores y de los principales equipos que estén administrando la sala.

- En los clientes instalar un programa para la limpieza de los temporales. En los clientes con Windows 9x/NT muchos programas usan archivos temporales que a menudo se quedan después del cierre del programa. Y es causa de que Windows crezca y mientras se vea disminuido el espacio de disco duro y la interpretación de sistema provoque errores. Se instala para que limpie directorios temporales o búsqueda para archivos temporales a través de su disco duro, así no se llenara de basura. Se puede fácilmente añadir un WINDOWS/TEMP, la historia del documento o cualquier otro directorio así sí se quiere se limpiará cada inicio de Windows (es sólo para usuarios registrados) y además es un programa cuya función es simple: eliminar todos los archivos inútiles de nuestro disco

duro. Su interfaz es excelente, y su utilización carece de dificultad. Para ello recomendamos el programa TempClean y el Super Cleaner.

6.6 Implementación de las Medidas de Seguridad

En este capítulo aplicaremos los programas y mejoras propuestas para el caso práctico de la sala No. 2 de UNICA.

Antes de mostrar la tabla con el resumen de las aportaciones e implementaciones realizadas, mostraremos la forma en la que se instalaron algunas de las herramientas para proteger al Servidor Maya.

A continuación mostraremos la bitácora de instalación, así como las herramientas de seguridad que se implementaron.

Primero la forma de proteger el servidor Maya (Windows NT) desde sus propias herramientas de el programa Windows NT.

Renombrar el Directorio por Default.

Un problema que necesita ser corregido durante la instalación es el directorio por default. No se recomienda instalar los archivos de sistema en directorio \WINNT. Renombre el directorio con cualquier otro nombre como \FREEBSD, \REDHAT u otro nombre que no sea fácil, esto prevendrá al sistema de ataques que vayan dirigidos a este directorio.

6.6.1. Instalación de las Herramientas de Windows NT.

Los puntos importantes a considerar para realizar una instalación segura son los siguientes:

- *Protección Física*.

Es importante asegurar físicamente el sistema para prevenir accesos no autorizados desde la consola, una buena solución es establecer un password al BIOS. Se recomienda que las unidades externas con el formato de archivos NTFS sean protegidas físicamente para que el personal no autorizado no pueda removerlo.

- *Verificar el Archivo ROLLBACK.EXE.*

Se debe verificar la existencia del archivo ROLLBACK.EXE en el disco duro y eliminarlo en el caso de que este presente, este archivo puede destruir información crítica del sistema incluyendo el *registry*, e información de cuentas de usuario.
Para recuperarse del daño generado por el archivo ROLLBACK.EXE, se tiene que disponer de una copia de seguridad de todo el sistema completo, el disco de reparación de emergencia no nos sirve en este caso.

- *Service Pack y Hotfixes*.

Se recomienda instalar todos los *Service Pack* y Hotfixes que son una colección de actualizaciones y parches para Windows NT y que se pueden descargar desde sus sitios Web. Puede descargar el último Service Pack en:

http://www.microsoft.com/ntserver/nts/downloads/recommended/

Los *Hotfixes* son soluciones intermedias liberadas entre los Service Packs y representan un parche para un problema específico.

Puede descargar o consultar en:

http://www.microsoft.com/technet/security/notify.asp

2. Proteger Archivos y Directorios

Entre los archivos y directorios a proteger se encuentran aquellos que son utilizados por el sistema operativo.Se deben asignar permisos en el cuadro de diálogo *Permissions* de la etiqueta *Security*, en las propiedades de cada directorio o archivo en el Windows Explorer.

Entre los archivos colocados en el directorio raíz del sistema, se deben proteger los siguientes:

Archivo:
Todos los archivos en el directorio raíz
Permisos:
Administrators: Full Control
SYSTEM: Full Control
Everyone: Read

****

Archivo:
\Boot.ini
\Ntdetect.com
\Ntldr
Permisos:
Administrators: Full Control
SYSTEM: Full Control

****

Archivo:
\io.sys
\msdos.sys

Permisos:
Administrators: Full Control
SYSTEM: Full Control
Everyone: Read

****

Archivo:
\Autoexec.bat
\Config.sys

Permisos:
Administrators: Full Control
SYSTEM: Full Control
Everyone: Read

Entre los directorios a proteger se encuentran los siguientes:

Directorio:

Directorio de Instalación (\WINNT por default) y todos los subdirectorios.

Permisos:

Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
Server Operators *: Change
SYSTEM: Full Control

* Aplica a servidores únicamente.

Dentro del Directorio de Instalación de se deben aplicar las siguientes excepciones:

Directorio:
\%SystemRoot%\repair\

Permisos:
Administrators: Full Control

Nota:
Permite que solo los miembros del grupo *Administrators* puedan extraer datos de este directorio, utilizados por la utilidad RDISK encargada de crear un Disco de Reparación de Emergencia para Windows NT 4.0.

****

Directorio:
\%SystemRoot%\System32\config\

Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: List
SYSTEM: Full Control

Nota:
Cuando estas configuraciones son propagadas a subdirectorios, los grupos *Everyone* y *Users*, serán capaces de crear un perfil, pero no serán capaces de leer otros perfiles de usuario.

****

Directorio:
\%SystemRoot%\System32\cursors\
\%SystemRoot%\System32\fonts

Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Add & Read
SYSTEM: Full Control

****

Directorio:
\%SystemRoot%\System32\help\
Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Add & Read
SYSTEM: Full Control

Directorio:
\%SystemRoot%\System32\inf\
Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control
****
Directorio:
\%SystemRoot%\System32\media\

Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control
****
Directorio:
\%SystemRoot%\System32\spool

Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
Power Users: Change
SYSTEM: Full Control
****
Directorio:
\%SystemRoot%\cookies
\%SystemRoot%\forms
\%SystemRoot%\history
\%SystemRoot%\occache
\%SystemRoot%\profiles
\%SystemRoot%\sendto
\%SystemRoot%\Temporary Internet Files
Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Special Directory Access – Read, Write and Execute
Special File Access – Not Specific
SYSTEM: Full Control
****
Directorio:
\%SystemRoot%\System32\profiles\All Users
Permisos:
Administrators: Full Control

CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control

Directorio:
\%SystemRoot%\System32\profiles\Default

Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Read
SYSTEM: Full Control

****

Directorio:
\TEMP

Permisos:
Administrators: Full Control
CREATOR OWNER: Full Control
Everyone: Special Directory Access– ead, Write and Execute
Special File Access – Not Specific
SYSTEM: Full Control

3. Asegurar la cuenta administrador.

Como medida de seguridad, se aconseja que nadie utilice la cuenta *Administrador* para trabajar en el sistema, a menos que se necesite hacer trabajo administrativo. Se debe crear una cuenta para trabajar en el sistema como usuario normal.

La cuenta *Administrador* nunca puede ser bloqueada a pesar de varios intentos fallidos al tratar de iniciar sesión en el sistema, aún si las políticas de cuenta en el *User Manager* o *User Manager for Domains* hayan sido establecidas a “Lockout After Bad Logon Attempts”. Esta es una cuenta muy atractiva para los intrusos que intentan ingresar al sistema.

Además, nunca se debe compartir la cuenta a*dministrador* bajo ninguna circunstancia. Con el grupo Built-in *Administrators*, no se puede restringir el acceso o capacidades a estos miembros.

Se deben seguir los siguientes pasos para asegurar la cuenta *Administrador:*

- Renombrar la cuenta *Administrador* con un nombre no obvio.
- Crear una cuenta *Administrador* sin privilegios.
- Habilitar el bloqueo de la cuenta *Administrador* real utilizando la utilidad *passprop*.
- Deshabilitar la cuenta *Administrador* del sistema local.
- Establecer un password fuerte.

4. Asegurar la cuenta Guest.

Se debería renombrar la cuenta de *Guest* y deshabilitarla.

Utilice *User Manager* o *User Manager for Domains* para realizar lo anterior.

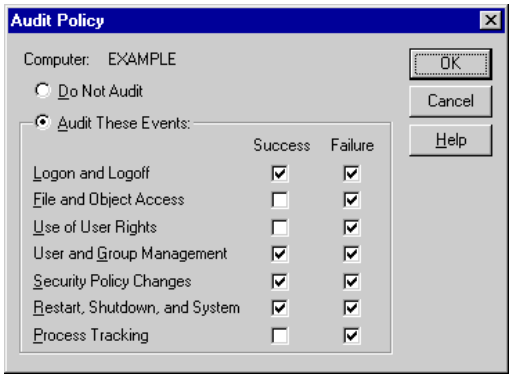
5. Aplicar Auditoría.

Habilitando la auditoria de Windows NT puede proporcionar información acerca de posibles riesgos de seguridad, así como detectar posibles intrusiones. Las particiones donde se habilite la auditoria deben tener el sistema de archivos NTFS.

Para activar el *Security Log* de Windows NT, se debe realizar lo siguiente:

- Iniciar sesión como *Administrator* del Servidor o Workstation local.
- Seleccionar el botón *Start*.
- Seleccionar *Programs,Administrative Tools, User Manager o User Manager for Domains*.
- Del menú *Policies* seleccionar *Audit.*
- Seleccionar la opción *Audit These Events.*
- Seleccionar las opciones a auditar.

Las siguientes opciones están disponibles



Log on/Log off:

Un usuario ha iniciado o cerrado una sesión o ha establecido una conexión de red.

File and Object Access:

Un usuario ha tenido acceso a un directorio o archivo cuya auditoria se ha establecido en el Administrador de archivos o a enviado un trabajo de impresión a una impresora cuya auditoria se ha establecido en el Administrador de impresión.

Use of User Rights:

Un usuario ha utilizado un derecho, excluyendo los relacionados con el inicio y cierre de sesión. Un intento de acceder a un archivo o aplicación no otorgado a un usuario será detectado.

User and Group Managed:

Se ha creado, modificado o eliminado un grupo o cuenta de usuario; se ha desactivado, activado o cambiado el nombre de una cuenta de usuario; o bien se ha establecido o modificado una contraseña.

Security Policy Changes:

Se ha modificado las políticas de derechos de usuario o de auditoria.

Restart, Shutdown, and System:

Un usuario ha reiniciado o apagado el sistema, o bien ha ocurrido un suceso que afecta a la seguridad del sistema o al registro de seguridad.

Process Tracking:

Estos sucesos proporcionan información de seguimiento detallada acerca de sucesos como activación de programas, algunas formas de duplicación de identificadores, acceso indirecto a objetos y salida de procesos.

Se recomienda auditar los siguientes eventos:

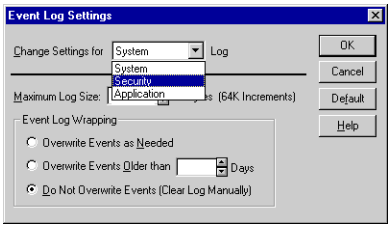
Evento	***Sucess***	***Failure***
Log on/off	Si	Si
File and Object Acces	No	Si
Use of User Rights	No	Si
User and Group Managed	Si	Si
Security Policy Changes	Si	Si
Restart, Shutdown, and System	No	Si

Tabla 6.4 Eventos a auditar

6. Incrementar el Tamaño de los Archivos de Registro.

Se deben incrementar el tamaño de los archivos de registro, con el objeto de que se tenga segura la información que reportan. Se deben seguir los siguientes pasos:

- *Start, Programs, Administrative Tools* y seleccionar *Event Viewer*.
- Seleccionar del menú *Log* la opción *Log Settings.*
- Seleccionar cada uno de los tipos de registro: *System, Security* y *Application*.
- Establecer el tamaño a 10 MB (10240 KB) y establecer la opción *Do Not Overwrite Events*.

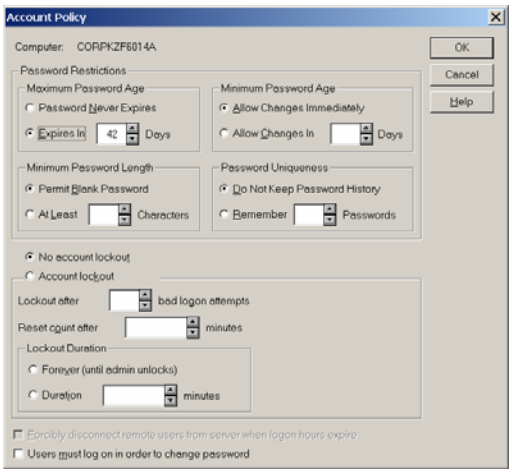


7. Establecer Políticas de Cuentas.

Para establecer políticas de cuentas se deben tener privilegios de *Administrator* y se deben seguir los siguientes pasos:

- *Start, Programs, Administrative Tools* y seleccionar *User Manager o User Manager for Domains*.

- Del menú *Policies* seleccionar Account.



Establecer las siguientes políticas:

Maximum Lenght: 40 días

Minimum Change: 2 días

Minimum Lenght: 8 caracteres

Remember: 10 passwords

Lockout Account: 3 a 5 intentos

Reset Count After: 30 minutos

Lockout: Forever Until Administrator Unlocks

8. SYSKEY

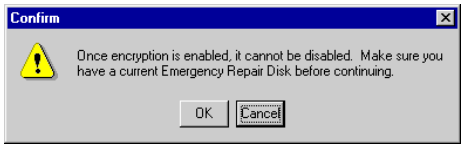
Windows NT introduce una nueva utilidad que permite que se tenga una encriptación más avanzada para la base de datos del SAM para proporcionar protección llamada SYSKEY (System Key). Esta utilidad agrega una segunda capa de encriptación para el LanManager y MD4 hashes del SAM.

Para ejecutar SYSKEY se debe realizar los siguientes:

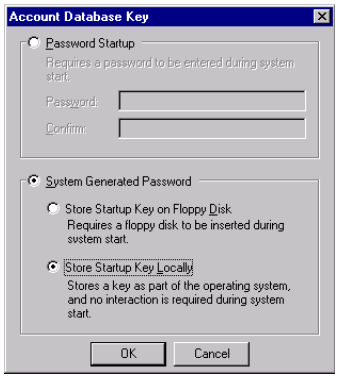
- Start, Run y escriba SYSKEY.

- Seleccionar *Encriptation Enabled* y dar seleccionar *OK.*

- Seleccionar en OK.



- En el cuadro de diálogo *Account Database Key* seleccione el método de encriptación de la llave de encriptación.



- Existen tres métodos a seleccionar:

Password Startup:

La llave del sistema puede ser generada (MD5) de un password de hasta 128 caracteres, que debe ser introducida al iniciar el sistema, y es también utilizado para encriptar la base de datos del SAM. Esta llave es generado cada vez que el sistema reinicia, de esta manera no es necesario tener un respaldo.

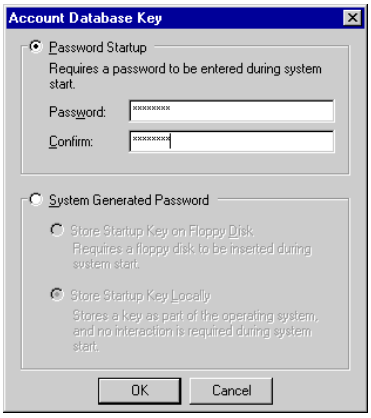
Store Startup Key on Floppy Disk:

El sistema genera una llave segura, que es almacenada en un disco flexible y debe proporcionarse durante el inicio o reinicio del sistema y no esta almacenada localmente.

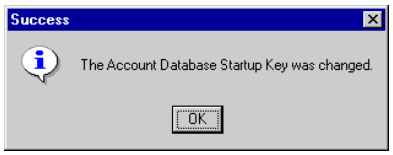
Store Startup Key Locally:

El sistema genera una llave segura, que esta oculta en el sistema con una “complex obscuring function” para ocultarla en el caso de un inicio de sistema desatendido. Esta llave es almacenada localmente y esta sujeta a ser comprometida.

- En el caso de que se seleccione *Password Startup:*



- Si no existe error en la confirmación del password, aparecerá el siguiente mensaje:



- Seleccionar OK y reiniciar el sistema.

- Cuando el sistema reinicie, aparecerá un cuadro de diálogo, solicitando el password de inicio. Una vez que el password es introducido, el proceso de inicio del sistema continúa normalmente.

9. Limitar el Acceso.

- *Cerrar Sesión o Bloquear el Sistema.*

Los usuarios deberían cerrar su sesión o bloquear el sistema si van a estar ausentes en un periodo considerable de tiempo. Cerrando la sesión permite que otros usuarios inicien sesión en el sistema y bloqueando el sistema no.

- *Ocultar el Username del Ultimo Usuario*

Cuando un usuario inicia sesión en un sistema NT, el *username* del usuario es mostrado por default la próxima vez que alguien intenta iniciar sesión. Conociendo los *usernames* de un inicio de sesión satisfactorio, pueden ayudar a los intrusos a realizar ataques de diccionario o fuerza bruta.

Para prevenir que el *username* del último usuario sea mostrado en el próximo inicio de sesión, utilice la siguiente configuración:

Hive: *HKEY_LOCAL_MACHINE*
Key: *\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon*
Value Name: *DontDisplayLastUserName*
Type: *REG_SZ*
Value: *1*

- *Deshabilitar el botón de Shutdown.*

Para evitar que gente desconocida apague el sistema NT, desactive el botón de *Shutdown* en la pantalla de inicio de sesión inicial. Esto hace que el usuario tenga que iniciar sesión para apagar el sistema. Si se tiene una buena política de auditoria, el administrador puede determinar quien reinicio el sistema.

Establezca la siguiente directiva:

Hive: *HKEY_LOCAL_MACHINE*
Key: *\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon*
Value Name: *ShutdownWhitoutLogon*
Type: *REG_SZ*
Value: *0*

10. Servicios de Red

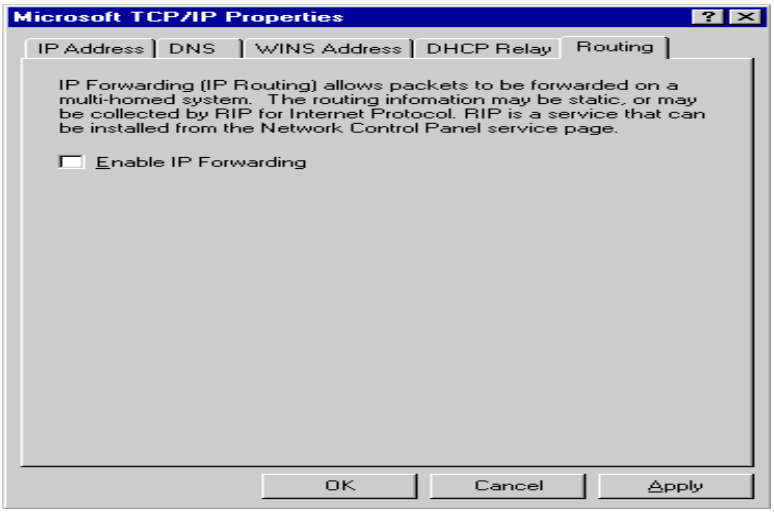
- *Deshabilitar IP Routing*

Verificar que la opción *Enable IP Forwarding* en la etiqueta *Routing* de las propiedades de TCP/IP de Microsoft no este habilitada.

Deshabilitando *IP Forwarding* previene que paquetes IP no autorizados se infiltren en la red y evita que el sistema este expuesto

Se deben seguir los siguientes pasos:

1. *Seleccionar Start*
2. Seleccionar *Settings*, después
3. Seleccionar Control Panel
4. Seleccionar el icono NetWork
5. Seleccionar la etiqueta *Protocols*.
6. Seleccionar *Properties* para mostrar las Propiedades TCP/IP de Microsoft.
7. Seleccionar *Routing*.
8. Asegurarse de que *Enable IP Forwarding* no este habilitado.



- *Deshabilitar los Servicios Innecesarios.*

Debido a que muchas vulnerabilidades pueden ser encontradas en cualquier servicio hoy en día, es importante limitar los servicios que se ejecutan en el sistema.

A continuación se mencionan los servicios y sus riesgos:

ClipBook Server.

Permite que usuarios tengan acceso a los contenidos del portapapeles sobre la red. Esto es utilizado para invadir la privacidad y comprometer la seguridad.

Computer Browser.

Debería siempre estar desactivado (o establecer su inicio manualmente) en Workstations, mantiene una lista actualizada de equipos y la ofrece a las aplicaciones que lo solicitan. Causa reducción en la actividad de la red y problemas de resolución de nombres.

DHCP client.

Se debe deshabilitar si se tiene una IP estática, de otra manera se debe tener habilitado.

Event Log.

Registra los sucesos de sistema, seguridad y aplicación en los registros de sucesos. Debe estar habilitado.

Net Logon.

Requerido para la autenticación en la red. Debe estar habilitado.

Network DDE y DDE DSDM:

Se debe verificar si se necesita intercambio de datos dinámicos. Deshabilitar estos servicios si es posible.

Remote Procedure Call Locator and Services.

Rpc es un protocolo que permite llamadas a funciones sobre la red. Probablemente se necesitará este servicio, se debe dejar habilitado.

Routing and Remote Access Service.

Este servicio es necesario para acceso y ruteo remoto. Debería ser deshabilitado en Windows NT Workstation para prevenir accesos no autorizados.

Schedule.

Requerido para trabajos AT. Se debe deshabilitar si no se utiliza AT para ejecutar tareas programadas.

Server.

Requerido si se quieren compartir recursos desde el sistema a otros en la red. La mayoría de los usuarios dejan este servicio habilitado pero en ambientes de seguridad altos se debería deshabilitar.

Spooler.

Requerido para imprimir en la red.

TCP/IP NETBIOS Helper.

Requerido por Net Logon. Se debe dejar habilitado este servicio.

Telephony Server.

Requerido para RAS. Se debe deshabilitar si no se utiliza RAS.

Time Service.

Para tener al reloj del sistema sincronizado con buenas fuentes conocidas.

UPS.

Administra una fuente de alimentación ininterrumpida conectada al sistema. Si no esta utilizando UPS, se debe deshabilitar este servicio.

Workstation.

Requerido si se quiere acceder a recursos a otros sistemas Windows NT.

- No ejecutar Servicios Vulnerables

No se deben ejecutar servicios que se saben que pueden ser vulnerables o que tienen asociadas una serie de vulnerabilidades. Entre estos se encuentran:

- Web
- FTP
- Telnet
- Gopher

6.6.2. Plan de Contingencia

El Plan de Contingencia se sale del presente trabajo de Tesis, pero se esboza de manera general lo siguiente:

Para la prevención de cualquier incidente que ocurra se cuenta con un plan de contingencia el cual nos ayudara para la protección, disponibilidad e integridad de nuestra información en el cual hemos identificado como recursos críticos nuestros servidores (Maya, Palenque y Jade), así como la infraestructura de la red, como son los switches, cableado estructurado y equipo eléctrico, lo que traerá como consecuencia que cuando estemos ante un incidente de tipo físico sepamos como solucionarlo o en su caso como escalarlo, es decir que realizaremos para que nuestro sistema se mantenga en operación.

Para el caso de los servidores, se cuenta con un servidor de respaldo el cual nos apoyará mientras exista el problema, en el caso de los no-breaks, se pedirían al responsable de la sala el Ing. Cruz Sergio Aguilar Díaz y de no conseguirse con él se le solicitará al Ing. Noé Cruz Marín.

Para el caso en que surga algún acontecimiento de tipo lógico primero será revisado por el personal de la misma sala, si todavía existe el problema lo recomendable es escalarlo con el Departamento de Seguridad de la Facultad y si aún así continua el problema se escalara a Dirección General de Servicios de Cómputo Académico (DGSCA).

No obstante si nos enfrentamos a una problemática administrativa se turnara como primera instancia a la gente responsable de la misma sala, dependiendo del acontecimiento se vera si se reporta o no con la gente de Dirección de UNICA, F.I. y si se tuviese que llegar más lejos, este sería al Tribunal Universitario.

Esto nos garantiza como se dijo al principio la integridad, confidencialidad y disponibilidad de nuestra información.

6.6.3 Implementación e Instalación del Firewall Físico Zona C

El Departamento de Seguridad como habíamos señalado ha implemento el firewall físico de la zona C en la sala No. 2 UNICA, F.I., aquí nosotros mostramos los objetivos del proyecto y el esquema de seguridad en cómputo para el segmento de red C, que se implemento.

Objetivos

- Fortalecer la seguridad en cómputo del segmento de red de la zona C de la Facultad de Ingeniería.
- Disminuir significativamente los incidentes de seguridad en cómputo, hacia y desde el segmento de red de la zona C de la Facultad de Ingeniería.
- Mantener la confidencialidad, integridad y disponibilidad de la información dentro del segmento de red de la zona C.
- Ser proactivo y preventivo ante los incidentes de seguridad en cómputo
- Generar reportes y estadísticas para evaluar el uso de la red en cuanto a seguridad en cómputo se refiere.

- Contar con una mayor organización y administración en cuanto a los servicios que ofrezcan los equipos y redes del segmento de red de la zona C de la Facultad de Ingeniería.

A continuación se presenta el esquema de seguridad lógica para el segmento de red de la zona C de la Facultad de Ingeniería, donde se detendrá el tráfico en la red que en la actualidad se considera hostil, y además permitirá monitorear continuamente las tramas de red para prevenir incidentes.

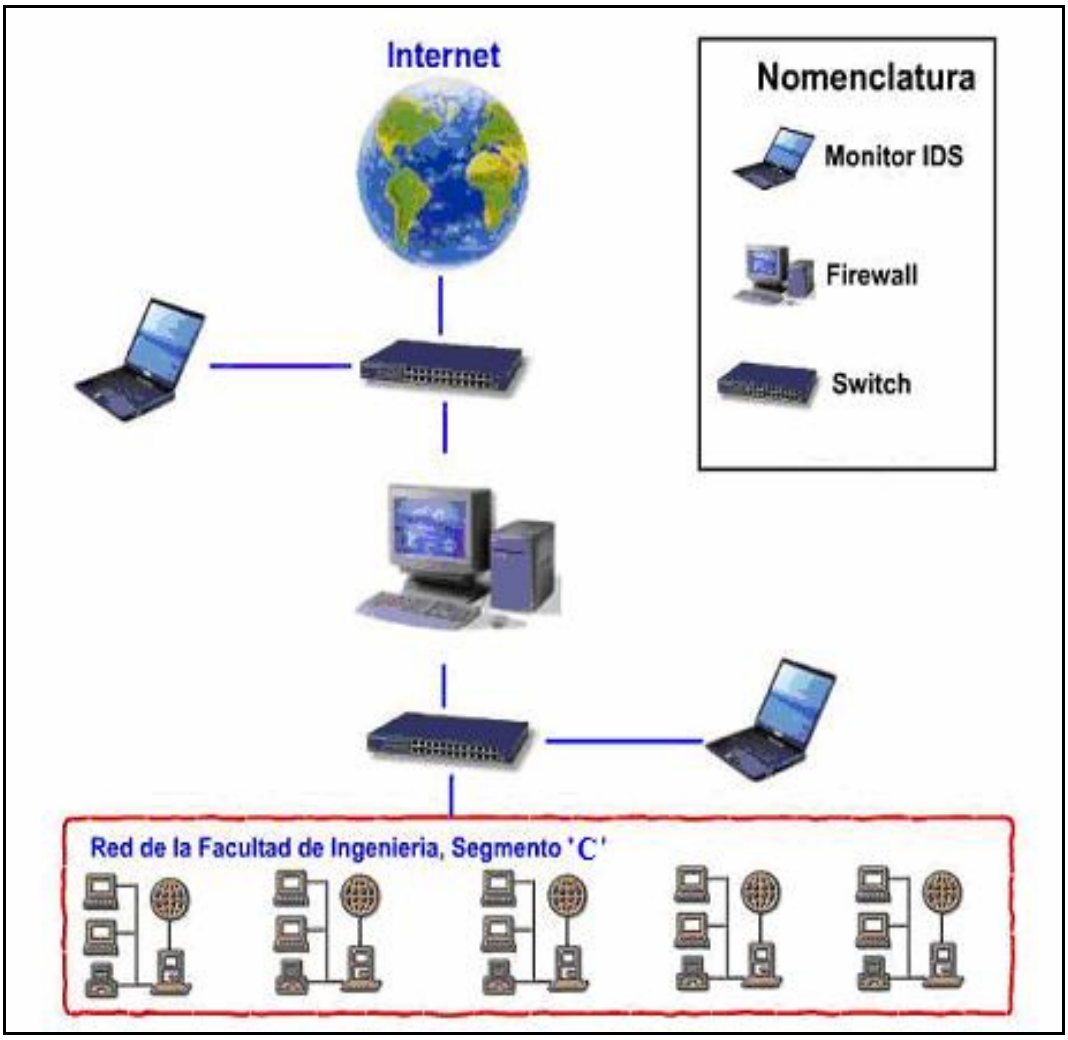


Fig. 6.3 Esquema de Seguridad para el segmento de red de la zona C de la Facultad de Ingeniería

Los dispositivos de los que se compone el proyecto son:

- 1 computadora que actuará como firewall**.**

Características del equipo:

Procesador Intel Pentium 4 de 2.80 GHz con caché L2 de transferencia de datos avanzada de 512 Kb integrada al procesador, bus frontal de 800 Mhz. Chip Set Intel 865 CON KHS. RAM de 256 Mb DDR Non-ECC SDRAM a 333 Mhz expandible a 4Gb. Teclado Gray DELL ps/2, keyboard español. Mouse DELL ps/2 de 2 botones. Disco duro de 40 Gb IDE Ultra ATA/100, 7200 rpm. Unidad de 48X CD-RW EIDE. Unidad de Floppy de 3.5 pulgadas a 1.44 Mb. Tarjeta de Video integrada video INTEL DVMT. Tarjeta de Sonido AC97 integrada compatible con Sound Blaster. Tarjeta de Red Integrada Gigabit NIC 10/100/1000 con conector RJ45 autosensing wake on Lan. 1 puerto serial, 1 puerto paralelo, 2 puertos ps/2, 6 puertos USB, Ranuras de expansión: 4 PCI y 1 AGP (ocupada por la tarjeta de video); bahías externas: 2 de 3.5 pulgadas (1 ocupada por el floppy) y 2 de 5.25 pulgadas (1 ocupada por el CD-ROM). 1 bahía interna para disco duro, fuente de poder de 250 watts. Monitor DELL de 17 pulgadas modelo M783S.

- 2 computadoras que actuarán como detectores de intrusos.

Mismas características que el equipo para el Firewall.

- 1 switch (externo)

Conmutador Ethernet apilable de 10/100 Mbps. Permite conexiones en cascada, gigabit ethernet o fast ethernet fiber cuando se instalan los módulos de expansión. Tiene 24 puertos con conectores RJ45, todos los puertos permiten utilizar los modos de half duplex y full duplex, y permiten el auto negociación.

- 3 tarjetas de red adicionales

Tarjetas de red 3Com Gigabit NIC Modelo 3C200T. 10/100/1000 Mbps.

6.6.4. Resumen

Esta parte se dividirá en tres como se hizo en el análisis, explicaremos la implementación a nivel físico, a nivel administrativo además de mencionar la aportación de nuevas políticas y mejoras a nivel lógico, todo esto se presenta como un resumen en la siguiente tabla:

	PROPUESTA DE MEDIDAS DE SEGURIDAD	IMPLEMENTACIÓN
NIVEL FÍSICO	- Capacitar al personal para la atención ante un desastre, así como para el uso adecuado de Extinguidores.	- Se capacitó al personal en el uso de extinguidores y como actuar ante un desastre ó siniestro y dar primeros auxilios. Este se impartió en el Centro de Docencia, F.I. Impartido por el Ing. de Protección Civil. Se cuenta con extinguidores de Gas Halón y de CO_2.
	- Señalización de las salidas de emergencia.	- Se colocaron señalizaciones en lugares más visibles.
	- Colocar protecciones en puertas y ventanas exteriores. - Acceso restringido al área de servidores.	- Se cambiaron las chapas que estaban mal y las ventanas cuentas con protecciones exteriores. - En el área de servidores y en la bodega se colocaron chapas con candados, además de que el acceso es con identificación.
	- Se les recomendó que sujetaran bien los cables de las computadoras y de los cables de red.	- Se realizaron amarres formando mazos seguros en los cables de red y de las conexiones de las computadoras para dejar libre acceso.
	- Poner aire acondicionado.	-El contar con aire acondicionado (minisplit) se encuentra en trámite. Por lo que mientras se cuenta con ventiladores en cada sala y en el área de servidores.
	- El personal debe contar con identificaciones.	- Todo el personal cuenta con identificación en las salas de UNICA.

	PROPUESTA DE MEDIDAS DE SEGURIDAD	IMPLEMENTACIÓN
NIVEL ADMINISTRATIVO	- Se recomienda llevar el control de inventarios de los equipos.	- Se realizan los inventarios de los equipos al final de cada semestre donde cada hoja de registro esta foliada para tener mejor control en el consecutivo de los inventarios.
	- Se aconseja llevar un inventario del equipo dado de baja.	- Se lleva un control de los equipos dados de baja en donde de igual forma se lleva un consecutivo de las hojas de registro donde se dan de baja los equipos.
	- Se recomienda llevar un control de préstamo de equipos.	- Se cuenta con un formato de préstamo de equipo que de igual forma va foliado.
	- Se recomienda tener una bitácora de incidentes.	- Se lleva una bitácora de incidentes. La cual permite detectar y analizar rápidamente la solución de un problema.
	- Se recomienda notificar de cualquier mantenimiento preventivo o correctivo al encargado.	- Se le notifica al encargado de la sala que mantenimiento se va ha realizar en las máquinas de la sala.
	- Se recomienda reforzar las contraseñas del personal, así como, las de usuario máquina.	- Ya se cuenta con contraseñas seguras en las cuentas del personal y de los usuarios-máquina. - Todas las contraseñas del personal, usuario-máquina y de los servidores cumplen con las características de contar como mínimo con 6 caracteres, son alfanuméricas combinadas con mayúsculas y minúsculas, además de contener caracteres especiales. - Se realiza el cambio de contraseñas en servidores, cuentas del personal y de usuario-máquina cada seis meses.
	- Se recomienda hacer respaldos periódicos.	- Se realizan respaldos de los servidores cada mese se realizan los completos y cada semana los incrementales.
	- Se aconseja contar con servidores de respaldo.	- Se cuenta con 2 servidores Palenque y Jade en caso de que Maya no funcione, estos dos servidores de respaldo se levantan de manera automática.

	PROPUESTA DE MEDIDAS DE SEGURIDAD	IMPLEMENTACIÓN
A NIVEL ADMINISTRATIVO	Se recomienda reforzar las políticas existentes en las salas de UNICA.	- Las siguientes políticas que se aconsejan están en platicas para su aceptación:
		Políticas De Seguridad Física - La puerta donde se encuentran los servidores y de la bodega debe permanecer cerrada y con candados. – Al cerrar el área de servidores y máquinas todos los equipos tienen que estar apagados o conectados a sus no-breaks.
		Cuando el personal abandonen temporalmente su lugar deben apagar el equipo o bloquear su sesión de trabajo.
		Políticas de cuentas – Las cuentas que se le asignen al personal, además de las cuentas máquina tendrán una vigencia de 6 meses.
		Políticas de contraseñas – Las contraseñas de los administradores, servicio social, empleados y máquinas tendrán una vigencia de 6 meses. – Las contraseñas deben ser alfanuméricas combinadas de mayúsculas y minúsculas, además de contener caracteres especiales.
		Políticas de control de acceso – El acceso a los servidores solo es para el personal autorizado con identificación. – El acceso a la paquetería y actualizaciones del software será de uso exclusivo de los administradores de las salas de UNICA. - Todo el personal que se encuentre dentro de las salas de UNICA deberá portar su gafete de identificación.

	PROPUESTA DE MEDIDAS DE SEGURIDAD	IMPLEMENTACIÓN
A NIVEL ADMINISTRATIVO		Políticas de impresión – El usuario debe avisar a los responsables o encargados de la unidad el que van hacer uso de la impresora. – El usuario solo podrá imprimir documentos de carácter académico y que sean propios. – Las impresiones solo se podrán hacer en hojas blancas por ambos lados.
		Políticas de inscripción a las salas de cómputo – Sólo se podrán inscribir alumnos de la Facultad de Ingeniería o Posgrado. – En la inscripción deberán presentar su comprobante de inscripción e identificación de la Facultad o del IFE.
		Políticas del reglamento – A todos los alumnos que se inscriban o se reinscriban a la salas de cómputo se les entregará el reglamento vigente. – El reglamento de las salas lo deberá saber el personal. - El reglamento deberá estar en un lugar visible en las salas.

<table>
<tr><th></th><th>PROPUESTA DE MEDIDAS DE SEGURIDAD</th><th>IMPLEMENTACIÓN</th></tr>
<tr><td>A Nivel Administrativo</td><td></td><td>
Políticas de Sanciones

Dentro de estas políticas mencionaremos otros casos en los cuales son incidente de seguridad grave, es decir cuando se pone en riesgo la seguridad de un sistema de cómputo, esto se mostrara en una tabla ya con la sanción y si hubiera reincidencia, como:
<table>
<tr><th>ACTIVIDAD NO LÍCITA</th><th>SANCIÓN</th></tr>
<tr><td>Acceso a las salas de cómputo con una identificación falsa.</td><td>Suspensión del servicio un semestre.

Reincidencia.

Cancelación de los servicios por el resto de la carrera en todas las áreas de la Facultad de Ingeniería</td></tr>
<tr><td>Imprimir en hojas de rehusó, membretadas.</td><td>Suspensión por una semana.
Reincidencia.

Suspensión por un semestre.</td></tr>
<tr><td>Imprimir sin autorización de los encargados</td><td>Suspensión del servicio por un mes.

Reincidencia.

Suspensión del servicio por un semestre.</td></tr>
<tr><td>Faltarle al respeto al personal.</td><td>Suspensión del servicio por un mes.

Reincidencia.

Cancelación de los servicios por el resto del semestre.</td></tr>
</table>
</td></tr>
</table>

	PROPUESTA DE MEDIDAS DE SEGURIDAD	IMPLEMENTACIÓN
NIVEL LÓGICO	- Se recomienda proteger al servidor con sus propias herramientas, además de auditarlo de manera interna.	- Se protege al servidor con las propias herramientas del Windows NT. Desde su instalación, se le desactivaron algunos servicios que no se utilizan.
	- Se aconseja instalar un programa para auditar al servidor y a la red, desde un cliente. (Máquina del administrador).	- Se instalo el siguiente programa para monitorear y auditar al servidor es Microsoft Baseline Security Analize, GFI Languard Network Security Scanner.
	- Se recomienda instalar un Firewall, un programa antiespias. Además se recomienda la instalación de un Firewall externo.	- Se instalo un Firewall que es el Zone Alarm. - Se le instalo un programa antiespias que es el SpySweeper. - El Ing. Rafael Sandoval instalo un Firewall externo, que no solo analiza las salas de UNICA, si no también el Anexo de la Facultad de Ingeniería.
	- Se les aconseja la instalación de un antivirus en el Servidor y en los clientes (maquinas)	- El servidor tiene instalado dos antivirus Norton Symantec y el AVG Antivirus como refuerzo. - En los clientes se encuentran instalados dos antivirus el Panda Antivirus y el AVG Antivirus.
	- Se recomienda también proteger a los clientes con programas para limpiar anti-spams, temporales, además de contar con sus antivirus.	-Se les instalo a los clientes un limpiador de temporales que es el Tempclean y un programa anti-spams que es Ad-ware.
	- Se aconseja instalar en los clientes un programa que administre las directivas de configuración de las máquinas para un mejor control.	- Se refuerza la administración de los clientes con las directivas de configuración con los programas Windows Configurator para los clientes en Windows 98 y Tweak para los clientes con Windows XP.

Tabla 6.5 Propuesta de medidas de seguridad e implementación a nivel físico, administrativo y lógico.

CONCLUSIONES

CONCLUSIONES

Después de realizado el análisis de los requerimientos de seguridad informática en la red de salas de UNICA, determinamos la necesidad de un ambiente estable que garantice el buen funcionamiento de la misma, así como, la disponibilidad permanente de los servicios, que se brindan a los usuarios, lo que conlleva a tener un correcto funcionamiento de servidores, para ello fue necesario estandarizar la plataforma de servicios para poder implementar herramientas de seguridad y mejorar el uso de los sistemas de administración de red, los cuales permiten optimizar las tareas de administración, soporte a los usuarios y servicios que conforman UNICA.

Se cumplió el objetivo general ya que se lograron establecer estrategias, se pudieron implementar medidas de seguridad que ayudan a fortalecer la seguridad que se tiene en la sala No. 2 de UNICA, de la División de Ciencias Básicas de la Facultad de Ingeniería.

Las medidas de seguridad que tomamos tomadas fueron enfocadas a resolver las oportunidades de mejora bajo el análisis del método OCTAVE-S, dicho análisis nos permitió detectar las debilidades que enfrentan las salas, como son: el que no se contaba con plan de contingencia o procedimiento a seguir ante un incidente de seguridad, el cual ya se hace referencia en el capítulo 6, así como la falta de políticas que no se aplican y que ponen en riesgo la seguridad , ya que no sólo es responsabilidad de lo usuarios, sino también de los administradores de las salas, además detectamos que no se contaba con las herramientas suficientes para disminuir las vulnerabilidades en los sistemas, así como la restricción de acceso a los servicios prestados, por otra parte este método de seguridad nos oriento en como mantener la disponibilidad, integridad y confidencialidad de la información que contienen los servidores.

Establecimos políticas de seguridad en las salas se dejo claro lo que se puede y no se debe realizar con los recursos de las salas.

Con la propuesta de las políticas de seguridad para UNICA específicamente en la División de Ciencias Básicas de la Facultad de Ingeniería, establecimos que los responsables de mantener la seguridad, tengan un respaldo ante las eventualidades que ponen en riesgo la integridad de los sistemas, así mismo, entre más herramientas utilicemos y se sepan explotar adecuadamente se tendrán controlados los riesgos y tendremos pruebas de que nuestra red tiene un nivel de seguridad, sin embargo se recomienda hacer una revisión periódica de las mismas, para que éstas sean capaces de seguir cubriendo las necesidades de UNICA. No olvidando que para que dichas políticas sean eficientes se deben publicar y divulgar de manera adecuada es decir, asegurarnos que todos los involucrados las entiendan, principalmente los usuarios, además de que las políticas reciban el apoyo de los directivos.

Se implementaron herramientas como el Zone Alarm, SpySweeper, Languard, Msbaseline, antivirus como el AVG, Panda Antivirus y Norton System (para servidor). Con lo que permitirá disminuir los riesgos a los que estamos expuestos.

Además no sólo se le dio importancia a la Seguridad Lógica, sino también a la Física, ya que como se pudo observar, el robo de equipo o de información a través de una intrusión física al sistema con estas medidas de seguridad se pretende no se lleve a cabo, además de que contribuirán a mejorar no solo la infraestructura, si no también a conservar en mejor estado los equipos y red en general.

La seguridad puede verse como un producto en constante cambio que no se debe analizar una sola vez, sino que debe ser un proceso de supervisión, revisión, actualización y capacitación continua, ya que de ello dependerá la mejor solución para evitar que ocurra un incidente, además al conocer nuestros recursos críticos los riesgos que enfrentan se podrá buscar las medidas y acciones con que podamos protegernos.

La red de UNICA opera confiable y eficientemente al cumplir con las políticas de seguridad fijadas y con la flexibilidad suficiente para soportar nuevas aplicaciones que contribuyan a mejorar la seguridad.

De esta manera UNICA cuenta con una serie de herramientas que fortalecen el ejercicio de brindar el servicio a los alumnos de la Facultad de Ingeniería.

Se concluye el análisis de las diferentes herramientas de seguridad cumpliéndose con los objetivos generales y particulares satisfactoriamente.

A continuación detallaremos los puntos de mejora que se realizaron de acuerdo con los objetivos particulares.

A NIVEL FÍSICO

Implementamos las medidas para proteger los equipos y las instalaciones de la sala No. 2 de UNICA. Llevamos a cabo la capacitación al personal para saber cómo actuar en caso de un siniestro y el cómo utilizar adecuadamente un extinguidor.

Con estas medidas físicas se pretende reducir los robos y extravíos de equipo y material, cuidar el equipo y poder obtener un mejor provecho de él.

A NIVEL ADMINISTRATIVO

Establecimos las medidas para una mejor administración, se realizaron aportaciones para las políticas de seguridad de las cuales se están estudiando para su aprobación, así como también se puso en práctica la utilización de dos formatos para control interno de préstamo de equipos y llevar una bitácora de incidencias.

Se cuenta con un plan de contingencia el cual nos ayudará a mantener en operación los servidores e infraestructura de red para poder seguir brindando el servicio.

A NIVEL LÓGICO

Protegimos al servidor con sus propias herramientas de Windows NT desde su instalación, deshabilitando servicios que no son necesarios para que el servidor funcione.

Además se protegió al servidor con antivirus, programas para limpiar temporales, para eliminar troyanos, anti-spams, un firewall, programa anti-espias, un software para auditarlo y para monitorearlo, así como también a los clientes.

En colaboración con el Jefe del Departamento de Seguridad se pudo instalar un firewall físico no sólo para UNICA, sino también para la División de Ciencias Básicas de la Facultad de Ingeniería. Para protección de la red de UNICA.

Todas estas medidas de seguridad fueron avaladas y aprobadas por el jefe de la sala No. 2 de UNICA de la División de Ciencias Básicas de la Facultad de Ingeniería y otras están bajo análisis para su aprobación aprobarse por el jefe de UNICA.

APÉNDICES

APÉNDICE I

FIGURAS

APÉNDICE II

TABLAS

FORMATO PRÉSTAMO

FORMATO DE PRÉSTAMO DE EQUIPO

FORMATO DE PRÉSTAMO DE EQUIPO MÉXICO, D.F. A _____ DE _____.

PRÉSTAMO DE LA: SALA 1 ☐ SALA 2 ☐ SALA 3 ☐ FECHA DE DEVOLUCIÓN: _____

PRÉSTAMO A LA: SALA 1 ☐ SALA 2 ☐ SALA 3 ☐ Ó DEPENDENCIA: _____

ENCARGADO DEL EQUIPO: _____

PERSONA QUE SE HACE RESPONSABLE DEL EQUIPO: _____

EQUIPO	MARCA	MODELO	No. INVENTARIO	No. SERIE
CPU				
MONITOR				
TECLADO				
RATÓN				
IMPRESORA				

DISCO DURO _____ TARJETA DE RED _____ DRIVE 3.5" _____
CD-ROM _____ QUEMADOR _____ MEMORIAS _____
DIADEMAS _____ SOFTWARE _____ TONER _____

ESTADO EN EL QUE SALE EL EQUIPO: _____
_____
_____

_____ _____
NOMBRE Y FIRMA DEL ENCARGADO NOMBRE Y FIRMA DEL QUE SE HACE RESPONSABLE

FORMATO DE INCIDENCIAS

FACULTAD DE INGENIERÍA

UNIDAD DE SERVICIOS DE CÓMPUTO ACADÉMICO

FORMATO PARA CONTROL DE INCIDENCIAS

LABORATORIO No_____ REPORTE No. _____ FOLIO_____

FECHA: _____ HORARIO: _____ SEMESTRE: _____

EQUIPO O SOFTWARE DAÑADO

NÚM. DE INVENTARIO _____ **NÚM. SERIE**_____

EQUIPO O SOFTWARE _____

DESCRIPCIÓN DE LA CONTINGENCIA

_____

_____

_____

NOTA IMPORTANTE: En la descripción se debe poner como se detecto el incidente o daño, y las consecuencias que genera este.

MEDIDAS A TOMAR CONTRA LA CONTINGENCIA

_____

_____

_____

_____

NOTA IMPORTANTE: En las medidas a tomar se debe poner si se detecto al causante del incidente, así como lo que se daño (software o hardware) y decir a que departamento se reportan los hechos.

Nombre y firma de quien reporta: _____

Nombre y firma de enterado del encargado del laboratorio: _____

REFERENCIAS

URL´S

- ftp://ftp.andrew.cmu.edu/pub/argus
- ftp://ftp.stanford.edu/general/security-tools/swatch/
- http://www.lawebdelprogramador.com
- ftp://cpast.cspurdue.edu/pub/tools/unix/crack
- ftp://ftp.porcupine.org/pub/security
- ftp://coast.cspurdue.edu/pub/tools/unix/cops
- ftp://coast.cspurdue.edu/pub/tools/unix/Tripwire
- http://www.microsoft.com/ntserver/nts/downloads/recommended/
- http://www.microsoft.com/technet/security/notify.asp
- http://www.microsoft.com/latam/seguridad/glosario/glossary_a_z.asp
- http://www.vsantivirus.com/especial-seguridad2004.htm
- http://www.rediris.es/cert/doc/unixsec/unixsec.pdf
- http://www.abcdatos.com/tutoriales/tutorial/o149.html
- http://www.seguridad.unam.mx/
- http://www.qualita.com.mx/site/Soluciones/Seguridad.html
- www.seguridad2003.unam.mx/
- http://www.cem.itesm.mx/dacs/publicaciones/logos/actual/oislas.html
- www.isocmex.org.mx/seg_info.html
- http://www.cert.org.mx/
- http://www.cert.org/other_sources\viruses.html

- http://www.unam-cert.unam.mx
- http://www.seguridad.unam.mx
- http://www.microsoft.com/latam/seguridad/glosario/glossary_a_z.asp
- http://www.cintel.org.co/ONLINE/rct_online_agosto/seguridad1c.htm
- http://www.pandasoftware.com/home/default.asp
- http://www.hispasec.com/
- http://www.microsoft.com/technet/treeview/defaults.asp?url=/technet/security/virus/virus.asp
- http://www.antivirus.com/
- ftp://ftp.seguridad.unam.mx
- http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- http://www.ntl-uk.com/products/lan_explorer.htm
- http://www.snort.org/
- http://www.sygate.com/
- http://www.insecute.com/tools.html
- http://www.el-hacker.com/txt/026.php
- http://www.isoftland.com/info/nav/Navcorp/navcorp.htm
- http://www.simtel.net/product.download.mirrors.php?id=55702
- http://www.rediris.es/cert/doc/unixsec/
- http://cozumel.fi-a.unam.mx/~cacfi/politicas_seguridad.html

BIBLIOGRAFÍAS

- Garfinkel, Simson and Spafford, Gene.
  Practical UNIX Security.
  Ed. O'Reilly & Associates. Inc.
  USA 1994

- Tanenbaum Andrew S.
  Redes de Ordenadores
  Ed. Prentice Hall
  México, 1991

- N, Derek Arnold.
  UNIX Security a practical Tutorial.
  Ed. McGrawHill
  USA 1993

- Pressman, Roger.
  Ingeniería del Software
  Ed. McGraw Hill
  Mexico 1993

- Madron, Thomas W.
  Network Security in the 90's.
  Issues and Soluctions form Managers.
  Ed. Wiley Professional Computing.
  USA 1992

- Stevens, W. Richard
  TCP/IP Ilustrated
  Ed. Addison-Wesley
  USA 1992.

- Lynch, Daniel C. And Marshall T.
  Internet System Handbook.
  Addison Wesley Publishing Company Inc.
  USA 1993.

- Tanenbaum, Andrew S.
  Redes de Computadoras
  Ed. Prentice Hall
  México, 1987

- Fairley, Richard
  Ingeniería de Software
  Ed. McGraw Hill
  Mexico 1993

- Departament of defense
  Trusted Computer System Evaluation Criteria,
  DOD 5200.28.STD
  USA 1985.

- Cooper, James Arlin,
  Computer & Communications Security Strategies for the 1990's.
  Ed. McGraw Hill Communications, Series,
  New York, 1989.

GLOSARIO

Glosario

- Administrador.

Persona que se encarga de la instalación, configuración y mantener en buen estado un equipo de cómputo.

- Agujero.

Una vulnerabilidad en el diseño del software y/o hardware que permite el software diseñado específicamente para la detección, prevención y engañar a las medidas de seguridad.

- Amenaza.

Persona, circunstancia, evento, fenómeno o una idea maliciosa que planta algún daño a un recurso.

- Análisis de riesgos.

Es el proceso de eliminar los posibles riesgos y clasificarlos por nivel de severidad, esto involucra tomar decisiones costo-beneficio. No debe de llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

- Antivirus.

Es un programa que se ejecuta en la computadora para buscar indicios de virus. Si encuentra alguno, guía al usuario en los pasos a seguir para la remoción del mismo. El programa antivirus debe ser actualizado periódicamente con las nuevas definiciones de virus.

- Aplicación.

También llamada Programa de computadora. Es un conjunto de instrucciones escritas en lenguaje de máquina que le permiten a la computadora realizar una tarea específica, normalmente con la interacción del usuario.

- Archivo

Conjunto de datos con un nombre asociado.

- Ataque.

Es la realización de una amenaza.

- Ataque pasivo.

Es aquel que no causa modificación o cambio en la información o recurso; es decir únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida.

- Ataque activo.

Es aquel que implica algún tipo de modificación de flujo de datos transmitido o la creación de un falso flujo de datos.

- Auditoría.

Es el registro, análisis y revisión de las actividades relacionadas con la seguridad de un sistema confiable. Consiste en revisar los eventos que pueden ser importantes para detectar un posible ataque al sistema.

- Base de datos (DataBase).

Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más

extendidos. Entre las más conocidas pueden citarse dBase, Paradox, Access y Aproach, para entornos PC, y Oracle, ADABAS, DB/2, Informix o Ingres, para sistemas medios y grandes.

- Bit.

Es la unidad más chica utilizada para medir un dato de computadora. Un bit puede tener dos valores: 1 o 0.

- BitNet

Red académica de ordenadores que sólo hace correo electrónico y FTP, basada en un protocolo diferente a Internet. Actualmente está interconectada a Internet por medio de gateways.

- Bomba de e-mail (Mailbomb).

Son mensajes de correo electrónico excesivamente largos enviados a la cuenta de correo de un usuario con el propósito de provocar la caída del sistema o evitar que los mensajes verdaderos sean recibidos.

Bomba lógica

Es un programa informático que se instala en una computadora que permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción.

- Boot.

Término utilizado para indicar el encendido de su computadora.

- Bps.

Bits por segundo. Es la unidad de medida de la velocidad de un modem. Generalmente expresada en kbps (kilobits por segundo)

- Bridge.

Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar

- Búfer.

Es una región de la memoria reservada para servir como receptáculo intermediario en el cual la información es temporalmente retenida antes de su transferencia entre dos ubicaciones o dispositivos.

- Bug.

Error en un programa de computadora que causa su mal funcionamiento.

- Byte.

Es un grupo de 8 bits.

- Caballo de Troya.

Es un programa computacional que aparentemente es útil pero que en realidad causa daño, contiene códigos escondidos que permiten la modificación no autorizada y la explotación o destrucción de la información. Los programas caballo de Troya se distribuyen por lo general por Internet. Los juegos, freeware y protectores de pantalla son los medios comunes que utilizan los caballos de Troya.

- Cableado.

Columna vertebral de una red.

- Chat.

Es un servicio de comunicación vía Internet, en la que pueden participar a la vez un alto número de usuarios.

- Cliente.

Es una computadora que utiliza los servicios de otra computadora denominada servidor. Cuando se esta utilizando Internet para descargar un archivo de información en su computadora, su maquina está actuando como cliente.

- Codificación.

Para que algunos mensajes de correo electrónico puedan ser enviados por la Internet, necesitan ser alterados. A este proceso se lo denomina Codificación. Algunos tipos de codificación son: uuencode y MIME.

- Confidencialidad.

Calidad de secreto, que no puede ser revelado a terceros o personas no autorizadas.

- Contraseña (password).

Es una cadena de caracteres que el usuario escribe para verificar su identidad en una red o en una PC local.

- Control de Accesos (Access Control).

Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web, etc... El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de dominio, nombre de usuario y password, certificados del clientes, protocolos de seguridad de redes, etc...

- Cookie.

Rastro que el servidor de un sitio web deja en nuestro PC cuando lo visitamos por primera vez; cada vez que volvemos a dicho sitio, la señal se actualiza, dando información al servidor de nuestro paso por la página. Con estas señales, los servidores pueden saber por dónde navegamos, cuáles son nuestros intereses, etc...

- Copia de Seguridad (Backup).

Es una copia de todos los datos originales contenidos en redes y PC's que puede ser utilizada en caso de que éstos se destruyan por diversas causas.

- Cortafuegos (Firewall).

Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, antivirus, autenticación, etc...

- Cracker.

Persona que elimina las protecciones lógicas y físicas de los sistemas para acceder a los mismos sin autorización y generalmente con malas intenciones.

- Cuenta.

Es el registro de un usuario dentro de un sistema, lo cual implica que este usuario podrá acceder a los servicios que este proporcione.

- Dato.

Es la unidad mínima con la que se compone cierta información.

- Debug.

Encontrar o corregir errores o bugs.

- DEC (Digital Equipment Corporation).

Empresa americana más conocida como Digital. Es una multinacional fabricante de computadoras, propietaria de la arquitectura de red DNA y creadora del procesador Alpha.

- Delito Informático.

Delito cometido utilizando un PC; también se entiende por delito informático cualquier ataque contra un sistema de PC's.

- Desastre.

Surge de las fuerzas naturales tales como las inundaciones, los terremotos, el fuego, el viento

- Descarga (download).

Es la transferencia de la copia de un archivo desde una PC remota a otra que lo pide por medio de un módem o por red.

- Dirección IP (estática y DHCP).

Identifica una computadora determinada dentro de una red para las otras computadoras. Una dirección IP es similar a la dirección de una casa. En un barrio, cada casa tiene una dirección única; en una red cada computadora debe tener una dirección única. Hay dos tipos de direcciones IP: estáticas y DHCP. Una dirección estática es donde alguien se conecta físicamente a una computadora y define la dirección IP para esa computadora. Una dirección estática no cambia a menos que alguien físicamente la cambie. Las direcciones DHCP (protocolo de configuración dinámica de host) son asignadas dinámicamente desde un servidor que contiene un grupo de direcciones. El servidor presta a la computadora una de las direcciones disponibles por una cantidad específica de tiempo. Una vez agotado este tiempo específico, la computadora renueva el préstamo o solicita una dirección IP nueva.

- Disco Duro (Hard Disk).

Es un componente de la computadora que almacena los programas y los archivos de datos. Es diferente a la memoria RAM debido a que la información se mantiene almacenada aún cuando se apaga la computadora.

- DNS (Domain Name System).

Servidor de nombres de dominio, cuya función principal es la de identificar la dirección IP a partir del nombre del dispositivo que se requiere accesar.

- E-Mail (Correo Electrónico).

Abreviación de Electronic Mail, que es un servicio de correo pero en la Red que nos permite comunicarnos con rapidez y de una forma muy sencilla con otro usuario.

- Encriptación.

Es un proceso de cifrado de las comunicaciones que tiene como finalidad que no puedan ser interceptadas. Las personas pueden desencriptar y leer el mensaje solo si poseen la clave adecuada.

- Escáner (Scanner).

Programa que busca virus en la memoria del PC o en los archivos.

- Explotar (Exploit).

Método de utilizar un bug o fallo para penetrar en un sistema.

- Fallo (Bug).

Cuando un programa tiene errores, se dice que tiene bugs. Como los virus son programas, también pueden contener bugs. Esto implicaría que, si el virus debe realizar determinadas acciones, podría no realizarlas, o no hacerlo bajo las condiciones que su programador ha establecido inicialmente.

- Filtrado.

Proceso mediante el cual un puente o conmutador Ethernet lee el contenido del paquete y descubre que éste no necesita volver a ser enviado, por lo que lo desprecia. La velocidad de filtrado es la velocidad a la que un dispositivo puede recibir paquetes y desecharlos sin ninguna pérdida de paquetes entrantes o demoras en su procesado.

- Filtro.

Patrón o máscara a través de la cual la información es pasada para separar elementos específicos. Por ejemplo, un filtro utilizado en correo electrónico o al recobrar mensajes de un grupo de noticias puede permitir a los usuarios el descartar automáticamente mensajes que vienen de usuarios específicos.

- Filtros Anti-Spam.

Son herramientas para filtrar el Spam o correo basura no solicitado en los programas de correo.

- Freeware.

Es un software que se provee sin cargo. Uno, no necesita adquirir ningún tipo de licencia para el uso de este software.

- FTP (File Transfer Protocol).

Protocolo de Transferencia de Archivos Software que permite la transferencia de archivos entre máquinas conectadas a una red.

- Gateway (Puerta).

Dispositivo que funciona como puerta de enlace entre Internet y redes inalámbricas.

- Gigabyte.

Son 1,000,000,000 bytes de datos. Esto parece ser una gran cantidad de datos pero instalar el software actual consume una buena parte de un disco de 1Gb.

- Gusano (worm).

Un programa destructivo que se copia a sí mismo a lo largo del disco y la memoria, consumiendo los recursos de la computadora y eventualmente inhabilitando el sistema.

- HEPNet (High Energy Physics Network)

Red de la alta física de energía

- Herramienta de búsqueda.

Es un servicio gratuito en Internet. Las herramientas de búsqueda se encargan de buscar e indexar enlaces en Internet que apuntan a la información que uno requiere. Cuando uno ingresa una frase o palabra clave, la herramienta revisa sus índices buscando páginas que contengan coincidencias con su requerimiento.

- Herramienta de seguridad.

Programas que permiten incrementar la fiabilidad de un sistema de cómputo. Existe una gran variedad de ellas.

- HTTP (Hypertext transfer protocol).

Es el método utilizado para transferir documentos desde la computadora server hacia los navegadores. Comúnmente se ven estas siglas al comienzo de las URLs o direcciones de Internet.

- Host.

Computadora central o principal en un entorno de procesamiento distribuido. Por lo general se refiere a una gran computadora de tiempo compartido o un computadora central que controla una red.

- Hub (Concentrador).

Es un dispositivo en una red que conectada múltiples computadoras para conformar una red LAN. Hay dos tipos de concentradores: estándar y conmutador. Un concentrador estándar comparte ancho en banda entre todos los puertos.

- Incidente.

Suceso que se interpone inesperadamente en el transcurso normal de una acción.

- Infección.

Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo.

- Internet.

Es una red de redes de computadoras conectadas a nivel mundial y se emplea para el intercambio de información y el acceso a las bases de datos.

- Intranet.

Es como la red Internet pero a nivel de una organización o empresa. Usando el popular software para Internet, la intranet le permite a los usuarios intercambiar datos dentro de la organización como si lo hicieran con el resto del mundo a través de Internet.

- Intruso

Persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

- IRC (Internet Relay Chat).

Charla Interactiva Internet. Protocolo mundial para conversaciones simultáneas que permite comunicarse por escrito entre si a través de ordenador a varias personas en tiempo real. El servicio IRC esta estructurado mediante una red de servidores, cada uno de los cuales acepta conexiones de programas cliente, uno por cada usuario.

- IP (Internet protocol).

Secuencia de números que se utiliza para asignar una ubicación a nivel electrónico y cuya administración a nivel mundial le corresponde a comisiones especializadas.

- IPsec (IP Security).

Conjunto de protocolos desarrollado por el IETF para soportar intercambio seguros de paquetes a nivel IP donde el emisor y receptor deben compartir una llave pública. Ampliamente extendido para la implementación de Redes Privadas Virtuales (VPNs), soporta dos modos de encriptación: Transporte y Túnel. El primero sólo encripta la parte relativa a los de datos (payload) de cada paquete, pero deja la cabecera intacta. Por su parte, el modo Túnel, más seguro, encripta todo.

- ISO 17999.

Estándar para la gestión de la seguridad de la información.

- Kernel.

Es la parte central y más importante del sistema operativo.

- Login.

Significa nombre de usuario.

- Modem (Modulator Demodulator).

Es un componente de hardware de su computadora que permite la transmisión de datos digitales sobre un enlace de transmisión analógico, es decir Convierte las señales digitales en analógicas y viceversa.

- Navegador.

Software que le permite a Ud. acceder a la información en Internet, mediante una computadora. EL Netscape Navigator y el Internet Explorer son ejemplos de navegadores que utilizan una interfase gráfica para buscar, ver y manejar información.

- NT

Es la forma común de abreviar Windows NT.

- Navegar.

Es la utilización de un navegador para buscar material interesante en Internet, mediante herramientas de búsqueda e hipervínculos.

- Netware

Nombre de un sistema de red desarrollado y comercializado por Novell Incorporated.

- Norma.

Regla que se debe seguir o que se debe ajustar a las conductas, actividades o tareas.

- Parche.

Es el archivo que realiza correcciones en un archivo ejecutable o en sus datos para eliminar errores.

- Plan de contingencia.

Conjunto de procedimientos que permiten recuperar y reestablecer el correcto funcionamiento del sistema en un tiempo mínimo después de que se haya producido el problema; considerando las acciones que se llevarán a cabo antes, durante y después del desastre, para tener el mínimo de pérdidas posibles.

- Pirata

La práctica habitual de la copia ilegal de software, tanto en el terreno doméstico como en el ámbito empresarial, ha relegado este término a ciertos personajes con alguna aureola capaces de penetrar en bases de datos de centros clave. Sin embargo, el término alude precisamente a esta práctica no por extendida menos reprobable, que ocasiona cuantiosísimas pérdidas a la industria informática.

- Política.

Definiciones establecidas por la dirección que determina criterios generales a adoptar distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

- Política de seguridad.

Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para poder llevar a cabo los objetivos de seguridad informática dentro de la misma.

- Protocolo de Comunicación.

Se refiere a la manera como los datos pasan de una estación de trabajo a otra.

- Protocolo de transferencia de archivos.

Es el que permite a los usuarios de gestores de correo la captura de documentos, archivos, programas y otros datos contenidos en carpetas existentes en cualquier lugar de Internet sin tener que proporcionar nombre de usuario y contraseña. Solamente se puede acceder a los archivos públicos situados en el sistema remoto al que se accede.

- Protocolo.

Es el lenguaje de comunicación utilizado entre las computadoras.

- Red.

Conjunto de computadoras y elementos que permite una comunicación entre sí y forman parte de un mismo ambiente.

- Sanción.

Acto solemne mediante el cual se confirma una ley.

- Seguridad.

Confianza tranquilidad de una persona procedente de la idea de que no hay ningún peligro. Es una cualidad o estado seguro.

- Servidor.

Es una computadora que provee servicios a otras computadoras denominadas clientes. Está compuesto por uno o más ordenadores.

- Servidor Proxy.

Componente de un firewall que maneja el tráfico de Internet hacia y desde una red de área local (LAN) y puede desempeñar otras funciones, como el almacenaje de un documento y control de acceso.

- Sniffer.

Equipo que efectúa análisis y medición en el tráfico de una red.

- Spam.

Identifica la acción de enviar correo electrónico con fines comerciales a una gran cantidad de personas. También usado para referirse a otros tipos de mensajes de correo no solicitados y molestos.

- Spyware.

Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se de cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

- Suplantación.

Ocupar el lugar de otro valiéndose de medios ilícitos.

- TCP (Transmission Control Protocol).

Es el encargado de garantizar que la comunicación entre dos ordenadores sea fiable y que llegue sin ningún problema a su destino.

- TCP/IP (Transfer Control Protocol/ Internet Protocol).

Son los protocolos de Internet más conocidos que garantizan la transmisión confiable de la información.

- Troyano.

Programa informático cuya ejecución tiene unos efectos imprevistos y, generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

- UNIX.

Es una familia de sistemas operativos tanto para ordenadores personales como para mainframes. Soporta gran número de usuarios y posibilita la ejecución de distintas tareas de forma simultánea (multiusuario y multitarea). Su facilidad de adaptación a distintas plataformas y la portabilidad de las aplicaciones (está escrito en lenguaje C) que ofrece hacen que se extienda rápidamente.

- URL (Uniform Resource Locator).

Es la dirección de un sitio en Internet con el nombre del servidor, el directorio donde esta el material y el nombre del archivo que lo contiene.

- Violación.

La violación es el incumplimiento de una ley que ya esta establecida.

- Virus.

Programa que trata de esparcirse de una PC a otra, usualmente a través de correo electrónico, adjuntándose a si mismo a un programa huésped. Puede dañar el hardware, software o datos.

- Web.

Por éste término se suele conocer a WWW (World Wide Web), creado por el Centro Europeo de Investigación Nuclear como un sistema de intercambio de información y que Internet ha estandarizado. Supone un medio cómodo y elegante, basado en multimedia e hipertexto, para publicar información en la red. Inicial y básicamente se compone del protocolo http y del lenguaje html.

- Worm (gusano).

Un programa destructivo que se copia a sí mismo a lo largo del disco y la memoria, consumiendo los recursos de la computadora y eventualmente inhabilitando el sistema.

- WWW (World Wide Web).

La WWW provee una manera de enlazar las computadoras en Internet a través del código html y usando hipervínculos que le permiten avanzar de un sitio a otro en la web.