UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Facultad de Ingeniería

ESQUEMA INTEGRAL DE SEGURIDAD EN CENTROS DE COMPUTO DE LA SECRETARIA DE HACIENDA Y CREDITO PUBLICO

T E S I S

Que para obtener el título de

INGENIERO MECANICO ELECTRICO
AREA: ELECTRICA Y ELECTRONICA

p r e s e n t a n:

DAVID SOTO JUAREZ

Director de Tesis:
M.I. Lauro Santiago Cruz

Ciudad Universitaria, México D. F. 1998

A NUESTRA UNIVERSIDAD...

Por darnos la oportunidad de ser parte de ella e integrarnos a su fraternidad.

A NUESTRA FACULTAD...

A la que debemos nuestra formación profesional.

INDICE

INTRODUCCIÓN

Hoy en día los procesos informáticos son vitales para las empresas que confían en las computadoras para manejar desde su información de inventarios hasta su sistema de pagos, pasando por la nómina, sus registros de clientes y proveedores, control de cuentas, etc. Esto hace que la información procesada y almacenada en los equipos de cómputo sea un activo aun invaluable dentro de los estados financieros de la empresa, ya que el concepto de "valor de la información" no es medible más que de forma indirecta, es decir, nos podemos dar una idea del daño provocado por la pérdida o alteración de los datos sólo a través del impacto que produce, no contar con ellos en el momento oportuno o bien recibirlos con errores por fallas en el procesamiento.

Lo anterior pone de manifiesto que debe existir una preocupación para lograr que la información almacenada y procesada mantenga intactas sus propiedades de integridad, confidencialidad y disponibilidad; y que se definan cuales son los riesgos latentes y/o amenazas del entorno para estar en condiciones de establecer los controles que permitan minimizar el impacto que algún evento dañino, fortuito o intencional, pudiera causar sobre los recursos informáticos resguardados en el centro de cómputo.

Definición del problema

Durante los años en que hemos proporcionado servicios de procesamiento de información para la Secretaría de Hacienda y Crédito Publico (SHCP) nos hemos enfrentado con que los responsables de desarrollar proyectos de construcción y modernización de centros de cómputo no cuentan con la documentación técnica de referencia que contenga los estándares de seguridad que se recomiendan para este tipo de inmuebles. Esto origina un deterioro de los niveles de servicio que se ofrecen a la SHCP, debido a que el proyectista pierde una gran cantidad de tiempo recopilando los requerimientos de seguridad de las áreas de infraestructura, desarrollo de sistemas, bases de datos, sistemas operativos, etc...; para contar con los elementos necesarios para la evaluación de su proyecto y posterior presentación para aprobación del cliente.

Este problema es aún más grave si tomamos en cuenta que con estos proyectos se tratan de solucionar problemas de seguridad en una entidad gubernamental, como lo es la SHCP, que procesa en sus centros de cómputo toda la información correspondiente a la recaudación de los impuestos de todas la empresas y personas productivas en la república mexicana.

En este trabajo se analiza este problema para proponer una solución práctica que optimice el tiempo de planeación proporcionando de manera general todas la previsiones para que la entidad informática llamada centro de cómputo sea, además de funcional, lo suficientemente segura como para evitar que cualquier evento dañino externo o interno ponga en riesgo la operación del mismo.

Propuesta de solución y método a utilizar

El propósito primero de este documento es señalar que en el ambiente operativo de cualquier sistema se presentan una gran cantidad de parámetros que no están bajo el control del operador o diseñador, y que es importante describir y entender estas

variables (aquí los llamaremos riesgos o amenazas), para posteriormente establecer los controles a través de los cuales se estarán protegiendo los recursos para permitir la continuidad en la prestación del servicio que otorga una sala informática.

También, mediante una pequeña retrospectiva histórica, analizaremos la evolución de los controles que hoy en día se aplican para la protección de los recursos de un centro de cómputo; y veremos que se establece una clara relación entre la detección de algún riesgo y la reacción inmediata para establecer la manera de evitar su presencia en el futuro; teniendo en cuenta que muchas de estas medidas reactivas tienen que ver con el establecimiento de estándares y normas para la fabricación de equipo, para el desarrollo de sistemas operativos y aplicaciones y para la fabricación misma de los cuartos de proceso, por lo que aquí se dejará bien clara la importancia de contar con un marco normativo que rija todas las partes involucradas en el diseño, construcción y operación.

Una vez bosquejado el escenario histórico y normativo del problema planteado, nos daremos a la tarea de describir las herramientas y recursos que se tienen actualmente para solventarlo, así que dividiremos el ámbito de la protección de centros de cómputo en dos partes: seguridad lógica y seguridad física, con lo que pretendemos abarcar la mayor parte de los riesgos que comúnmente se presentan. En la parte de la seguridad lógica se describirán las herramientas para impedir que personas ajenas tengan acceso al entorno de la programación, configuración y sistemas en general instalados en los equipos, siempre con el fin de proteger la veracidad de la información procesada y almacenada, a través de la implementación de barreras (lógicas) para evitar la observación, extracción o interceptación de la misma.

Por lo que se refiere a la parte de seguridad física describiremos la infraestructura que se requiere para contar con un local que ofrezca un máximo de protección a los equipos que ahí se alojan, es decir, un local que no permita el acceso a personas no autorizadas, que proteja contra inclemencias del clima (filtraciones de humedad, polvo, interferencias electromagnéticas, etc...), que minimice daños provocados por eventos fortuitos (sismos, inundaciones, incendios, etc...) y que tenga capacidad de autonomía

para el suministro del servicios (eléctrico principalmente) y no depender de la calidad del servicio proporcionado por proveedores externos (CFE, por ejemplo).

Finalmente, no debemos olvidar que es prácticamente imposible estar prevenidos al 100 % contra cualquier tipo de amenaza o riesgo, por lo que la posibilidad de un desastre que afecte significativamente partes vitales de los centros de cómputo siempre está latente, por lo que debemos de contemplar la manera de recuperar lo más rápido posible la operación de los servicios incluyendo, naturalmente, los servicios informáticos.

Recomiendan los especialistas que la mejor manera de regresar a la operación normal después de un desastre es planeando la recuperación aún cuando se piense que jamas sucederá una situación semejante, así que en esta última parte se establece la metodología y los requerimientos para la elaboración de un buen plan de recuperación ante contingencias; desde el levantamiento de información necesaria hasta los procedimientos indispensables que se deben incluir y las pruebas que se requieren para contar con un plan confiable.

Objetivo

Definir los parámetros necesarios para establecer un esquema integral de seguridad, que permita que la operación de un centro de cómputo no se vea comprometida ante la presencia de amenazas externas, preservando la integridad de los equipos, del personal y, principalmente, de la información que se procesa.

Resultados esperados

Al concluir el presente trabajo se espera que se reduzca de manera sustancial el tiempo que transcurra entre el planteamiento de un problema por parte de nuestro cliente y la propuesta con la solución del mismo.

Así que, a medida que los lideres de proyecto lo tomen en cuenta como un documento de consulta y exploten de manera adecuada la información aquí contenida se estará optimizando el proceso de planeación; teniendo como resultado que las expectativas del cliente, tanto en tiempo de respuesta como en calidad de la propuesta, se vean satisfechas; ya que esperamos que a corto plazo se convierta en una herramienta básica para evitar pérdidas en tiempo y esfuerzo al esbozar la solución conceptual y redondearla inmediatamente en una propuesta formal.

Por otro lado y de la misma manera en que se cuente con una guía de referencia confiable y de la cual se tomen consideraciones básicas de seguridad, se tendrá también un esquema general con los parámetros y principales características que deben conformar la estructura de un centro de computo seguro, teniendo documentados los estándares establecidos para que la información que es procesada en dichos centros se mantenga integra y confiable.

1

ANTECEDENTES

La seguridad en la computación es hoy en día un tema candente, pero que se ha ido calentando a fuego lento al paso de los años. El desarrollo de normas y estándares por parte de gobierno y otras organizaciones involucradas, las investigaciones relacionadas con los mecanismos de seguridad, los debates sobre las amenazas a la información y los costos de la protección contra esas amenazas son actividades que se han desarrollado sólo en las últimas tres décadas; lo que nos hace pensar que el tema de la seguridad en la computación es, por sí mismo, un tema nuevo y que ha tenido que evolucionar a marchas forzadas, desde un enfoque estrecho en el que lo importante era mantener a los intrusos fuera del área de procesamiento y el gobierno como única entidad reguladora, hasta los conceptos modernos de seguridad integral y la participación de empresas y otros organismos que junto con el gobierno van forjando la cultura de la protección a la información automatizada.

En este capítulo se ofrece un panorama que permite ubicar la importancia del tema a través de la historia, describiendo a grandes rasgos los eventos que marcaron el desarrollo de herramientas para superar las debilidades en la seguridad de los centros de cómputo. Se identifican, también, las amenazas y vulnerabilidad que pueden afectar a cada instalación a través de un método que deja bien claro contra que se deben proteger, los costos y las ventajas que tienen los controles que deben aplicarse. Y, finalmente, se resalta la importancia que tiene un adecuado marco normativo dando una reseña de los temas que se deben abarcar al redactar las políticas, normas y procedimientos que deben seguirse dentro de las empresas, particularmente en las áreas informáticas.

1.1 Evolución de la seguridad en centros de cómputo

En los primeros días de la computación, los sistemas de cómputo eran grandes, raros y muy caros. Naturalmente aquellas compañías que tenían la suerte de tener una computadora intentaban protegerla lo mejor posible. En ese entonces la seguridad de la computadora era una aspecto más del plan de seguridad de la planta, si es que lo había; y se limitaba a que las instalaciones en general y un poco más particular el cuarto de proceso estuvieran protegidos contra el posible acceso de personas ajenas que pudiera causar daños. La preocupación por la seguridad se enfocaba en evitar daños físicos, robo de equipo y/o robo o destrucción de discos, cintas, tarjetas perforadas u otros medios de almacenamiento. La razón era que poca gente conocía el uso de las computadoras y sólo aquellos que conocían los secretos de la máquina eran los privilegiados que permanecían en presencia de la misma.

Pero los tiempos cambian y en los últimos años de la década de los 60's e inicios de los 70's, la tecnología de las computadoras se transformó radicalmente y con ello los caminos a través de los cuales se relacionaban los usuarios con las computadoras y los datos. La multi-programación, el tiempo compartido y las redes de trabajo cambiaron dramáticamente las reglas del juego. Los usuarios podían ahora interactuar directamente con un sistema de cómputo, vía una terminal, dándole mayor poder y

flexibilidad pero llevando consigo, también, apertura a nuevas y diferentes posibilidades de abuso.

Las telecomunicaciones (como una facilidad para accesar computadoras desde ubicaciones remotas y compartir programas y datos) cambiaron radicalmente el uso de las computadoras. Grandes empresas iniciaron el almacenamiento automatizado en línea de la información de sus clientes, proveedores y transacciones comerciales. Las redes de trabajo permitieron la comunicación entre minicomputadoras y con servidores principales que contienen grandes bases de datos en línea.

Inevitablemente, el incremento de la disponibilidad de sistemas e información en línea conducen a los abusos, y la seguridad en la computación amplía su campo de acción, ahora en lugar de preocuparse sólo por el acceso de personas ajenas dentro de las salas de cómputo y equipo auxiliar, las empresas se preocupan por computadoras que son vulnerables a ataques furtivos a través de las líneas telefónicas, por la información que podría ser robada o cambiada sin que quede una sola pista. Incidentes de crímenes computacionales empiezan a ser reportados. Individuos y agencias de gobierno expresan su preocupación por la invasión a la privacidad debido a la disponibilidad de registros financieros, legales y médicos existentes en bases de datos compartidas.

Hacia la década de los 80's se habló del amanecer de una nueva edad de la computación con la introducción de las computadoras personales, individuos de todas las edades y ocupaciones son ahora usuarios de computadoras apareciendo éstas en escritorios de la casa y la oficina. Como el precio de los sistemas baja a la par que los paquetes de contabilidad se hacen disponibles a un bajo costo, entonces más y más pequeñas empresas automatizan sus operaciones. Sin embargo, la tecnología de las PC's introduce un nuevo riesgo: preciados e irremplazables datos corporativos se almacenan en disquetes, los cuales se pueden perder o ser robados más fácilmente.

Tan pronto entramos a los 90's, nos enfrentamos al reto de los sistemas abiertos, principalmente porque se incrementa la dependencia en las redes de trabajo y la

necesidad de compartir datos, aplicaciones y recursos de hardware/software más allá de la frontera de los vendedores, llevándose consigo incrementos en los riesgos para la seguridad. En esta década, la seguridad en las empresas viene por etapas con más y más vendedores desarrollando sistemas confiables, manojos de funciones de seguridad, dispositivos biométricos y productos para seguridad en redes de trabajo. Todavía, los sistemas de seguridad vienen detrás de la tecnología que buscan controlar. Y los esfuerzos individuales y de empresas están todavía más atrás en su preocupación por hacer de la seguridad una parte integral de sus productos y sus trabajos.

El reto de la próxima década será consolidar lo que se ha aprendido forjando la seguridad en las computadoras, reflejándolo en productos y en la rutina diaria para proteger los datos sin que necesariamente se impida la disponibilidad para accesar a ellos; y asegurarse de que tanto los productos de seguridad como el gobierno y los estándares industriales crecerán hasta estar al parejo de los retos de la tecnología.

1.1.1. Eventos relevantes

La seguridad de la información es casi tan antigua como la información misma, siempre que la gente descubre nuevos métodos para grabar, almacenar o transmitir información; estas innovaciones van siempre e inevitablemente seguidas por nuevas tecnologías para la protección de la información y sus procesos. Y aun más, van también seguidas por controles e investigaciones gubernamentales. Por ejemplo:

- Con la introducción del telégrafo de Samuel F. B. Morse, vino la preocupación por proteger la confidencialidad de los mensajes transmitidos. En 1845, sólo un año después de la invención, fue desarrollado un código de encripción comercial para mantener en secreto los mensajes transmitidos.

- Dentro de los cinco años posteriores a la introducción del teléfono en 1881, fue archivada la patente de una aplicación para disfrazar la voz.

- En los años 20's, la intervención de líneas telefónicas por parte del gobierno y el crimen organizado dio como resultado que el público se quejara, propiciando debates en el congreso y finalmente una legislación prohibiendo la intervención de teléfonos.

- En la década de los 40's, la preocupación en relación al control de la proliferación de información relacionada con la energía atómica condujo al Acta de la Energía Atómica en 1946. Esta acta creó una categoría de **Datos Restringidos** de información que requería de protección especial y penalización por su distribución. Controles similares han sido impuestos en relación a nuevos avances en otros campos científicos.

- En los 80's, el Acta de Autorización de la Defensa especifica controles en la información técnica relacionada con emergencias militares y tecnología espacial.

Las primeras actividades relacionadas con seguridad en computadoras iniciaron en los años 50's con el desarrollo del primer estándar de seguridad llamado *TEMPEST*, la consideración de temas de seguridad en algunos diseños de sistemas de cómputo y el establecimiento de la primera organización gubernamental de seguridad en los Estados Unidos, *el* ***U.S. Communications Security Board***. Este comité está formado por representantes de muchas y diferentes ramas del gobierno y supervisa la protección de información clasificada.

Aunque este evento configura el escenario para los posteriores avances de la seguridad en computadoras, la década de los 60's marca el verdadero inicio de la época de la seguridad, con iniciativas del Departamento de Defensa, la Agencia de Seguridad Nacional y el Buró Nacional de Estándares para lograr una conciencia pública de seguridad.

El interés público en la seguridad de las computadoras emerge hacia finales de la década. El ciclo de conferencias de computación en la primavera de 1967 es generalmente reconocido como el escenario de la primera presentación global de seguridad en computadoras para una audiencia técnica. En ella se identificaron la

amplia variedad de vulnerabilidades que se presentan en los recursos compartidos y el acceso remoto a los sistemas de cómputo; también se identificaron las amenazas que van desde radiación electromagnética hasta virus en la programación, intervención de las líneas de comunicación, acceso de usuarios a sistemas y datos, etc.

1.1.2. Fraudes famosos

El crimen computacional se ha convertido una gran amenaza para los negocios. De acuerdo con el Buró Federal de Investigaciones (FBI por sus siglas en inglés), este tipo de eventos es la más cara forma de delito comercial con un costo promedio de 450,000.00 USD por robo (se estima que esta cantidad representa también el costo de los daños que se tendrían en el remoto caso de un incendio o algún otro tipo de desastre). Por lo que se calcula que el total de dólares al año que son defraudados a través de delitos computacionales es de cinco billones.

Esta estimación está basada en reportes que indican que el 90 % de las penetraciones a los sistemas de cómputo no son denunciadas por las víctimas por el simple hecho de que la divulgación podría traerles mayores problemas debido a publicidad adversa, o bien, la pérdida de la confianza de sus clientes por la falta de confidencialidad en el manejo de la información. De hecho se tienen reportes de empresas que establecen acuerdos con los delincuentes ofreciéndoles amnistía y un pago a cambio de tres cosas principalmente: la devolución de una parte de lo robado, evitar posteriores intentos de penetración a los sistemas y, lo más importante, no divulgar los huecos en la seguridad de los sistemas de la empresa que la hacen vulnerable a este tipo de estafas. Algunos casos documentados de este tipo de delitos son los siguientes:

- En 1988, en su libro "El Huevo de Cuckoo", el astrónomo convertido a detective Cliff Stoll relata como gastó un año rastreando y eventualmente atrapando a un 'cracker' Alemán que intentó penetrar en 450 computadoras (lo logró en 30 de ellas) de redes de todo el mundo, incluyendo el laboratorio Lawrence Berkeley donde Cliff Stoll trabajaba. El intruso revisó archivos militares que contenían información relacionada con armamento nuclear, químico y biológico; y casi interrumpe un experimento

médico (posiblemente con resultados fatales). Con el señuelo de falsos archivos relevantes relacionados con el Departamento de Defensa, y con ayuda de micrófonos en los teléfonos, Stoll engaño al intruso rastreándolo hasta su escondite. Cuando las autoridades alemanas descubrieron que el intruso y sus compatriotas habían estado vendiendo información a la KGB, fueron consignados por espionaje.

- En 1988, una importante agencia de viajes descubrió que alguien había penetrado en su sistema de expedición de boletos y reservaciones para imprimir ilegalmente boletos de aerolíneas. La penetración había levantado interrogantes acerca de la posibilidad de que organizaciones terroristas podían accesar a los sistemas de las aerolíneas para obtener información de sus pasajeros y planear atentados. Ha habido especulaciones de que el atentado terrorista en el cual miembros de la familia real de Kuwait fueron tomados como rehenes a bordo de un avión pudo resultar de tal robo de información.

- En 1989, un joven de 14 años, usando una computadora personal *Apple* accesó a un sistema de localización satelital de la fuerza aérea. Como adepto al uso de computadoras desde los 8 años, el muchacho marcó a códigos de acceso de larga distancia restringidos y también revisó archivos confidenciales de más de 200 empresas. Cuando fue aprehendido, él dijo que esperaba persuadir a alguna compañía para que lo contrataran como consultor de seguridad.

En México, el caso más comentado de fallas en la seguridad de un sistema de cómputo fue aquella famosa caída del sistema de conteo de votos en las elecciones presidenciales de 1988, del cual se tienen varias versiones que van desde la presencia de virus hasta fallas en los sistemas auxiliares de soporte eléctrico y ambiental, sin que hasta la fecha se conozca si el caso tiene origen en la seguridad de los sistemas o se debió a negligencia por parte del personal operativo.

1.2. Vulnerabilidad y amenazas

En la sección anterior repasamos eventos aislados que ponen de manifiesto la existencia de muchas maneras de alterar la "operación normal" de un centro de proceso informático; sin embargo, es muy arriesgado pretender una delimitación de la problemática general a partir de hechos que, aunque representativos, no dejan de ser una simple muestra que permite establecer un escenario de referencia para justificar los esfuerzos que en diferentes áreas profesionales se hacen para prevenir, detectar y corregir elementos de falla y hacer de los centros de cómputo entidades cada vez menos susceptibles a daños por factores externos.

Existen varias técnicas para determinar el grado de vulnerabilidad con base a un reconocimiento de las amenazas que acechan. Aquí se hará referencia, de manera descriptiva, a una técnica que de manera sencilla permitirá evaluar los riesgos existentes, tipificar amenazas, identificar los controles y establecer un plan de acción para mejorar la seguridad.

El primer paso para una evaluación es recolectar la información que describa como se supone que la seguridad debe ser tratada y compararla con lo que realmente sucede. Cuestionar sobre:

- ¿Quién determina lo que es confidencial?
- ¿Hay procedimientos que guarden información confidencial?
- ¿Quién especifica la necesidad de conocer los requerimientos para cada función?
- ¿Quién suministra la seguridad y con qué bases?

Otra manera efectiva y más directa es preguntando a los usuarios como utilizan los sistemas y que tipo de información. De estas entrevistas dependerá la información considerada sensible por la gente propietaria de la misma y la manera en que la información viaja en la red. Este paso le proveerá de un conocimiento sólido de las políticas que existen, si las políticas son aplicadas en operación normal y si los procedimientos se ejecuten normalmente. Se debe estar consciente de que la información es poder y dentro de una compañía la información puede dar el poder a extraños para penetrar en los sistemas de cómputo.

En este paso deberán preguntar cosas tales como:

- ¿Cuánto saben los extraños acerca de su compañía?
- ¿Saben qué sistemas se usan?
- ¿Conocen qué partes han sido instaladas?
- ¿Conocen la clave de acceso o la dirección IP y los nombres del servidor?

Esta información típicamente identifica el tipo de tecnología usada por una compañía con sistemas críticos y por lo tanto prevé asaltos potenciales a la información de la computadora.

La evaluación deberá analizar el esquema de seguridad de las implementaciones del sistema principal. Esto deberá determinar como las aplicaciones de software, la capacidad de sistemas de operación y los procesos de seguridad trabajan juntos.

Se puede obtener esta información conduciendo en tres partes la entrevista y preguntando lo mismo para cada grupo de:

- Especialistas en sistemas operativos
- Programadores de aplicación
- Administradores de seguridad

Si los tres grupos son consistentes y las respuestas tienen sentido, probablemente se tiene un razonable nivel de seguridad. Todo lo que tiene que hacer es determinar si la seguridad es suficiente. Si las respuestas son inconsistentes entonces se debe asumir que hay huecos en la seguridad.

Los sistemas cliente-servidor son por definición, accesibles, dispersos en la población usuaria. Mientras su seguridad es inmadura su exposición es alta. Están frecuentemente disponibles a través de cableado y conexiones remotas. Su conectividad frecuentemente se extiende dentro de viejos sistemas principales. La evaluación necesita identificar que protecciones son necesarias para el servidor a través de la recolección de datos y el análisis.

Lo anteriormente descrito sería un proceso manual tedioso; sin embargo, hay muchas herramientas de análisis disponibles. Un producto de estas herramientas rápidamente revelará el porcentaje de usuarios que tienen derechos de acceso o son miembros de muchos grupos. Por lo que para fines prácticos se deben llevar a cabo de manera que haya una distribución en subconjuntos de servidores y usar el resultado para identificar los problemas por áreas. Se pueden hacer algunas generalizaciones sin incurrir en errores y por medio de análisis subsecuentes se puede también validar si la seguridad ha sido mejorada.

Por otra parte, hay muchos productos que protegen la conexión a Internet de una compañía. Como parte de la evaluación, es necesario el análisis de la conducta y la prueba en contra de la penetración de un asalto en la base del Internet, existe una variedad de herramientas disponibles para llevar a cabo estos análisis. Cada una tiene sus ventajas y desventajas, lo importante es asegurarse del uso de herramientas apropiadas, analizar los resultados y examinar la empresa tanto como sea posible para garantizar niveles adecuados de seguridad.

Durante la década pasada los modems revolucionaron la capacidad de comunicación. En el caso de la seguridad, para las organizaciones los modems instalados en redes y los modems de autorrespuesta son los de mayor vulnerabilidad. La guerra del marcado es el acto de llamar a todos los números en un rango de números telefónicos buscando tonos de módem. Cuando un tono es encontrado, un registro es creado. Si el tono no es encontrado, el número es descartado. Programas automatizados pueden correr a través de rangos masivos de números telefónicos toda la noche y por la mañana se pueden ver a través de un simple archivo de texto todos los números telefónicos donde fueron encontrados modems de autorrespuesta e iniciar la cacería de información.

A través de un riguroso proceso de análisis se puede garantizar que se cuenta con la información necesaria para mejorar la seguridad de la compañía y probablemente se tendrá información de otros esfuerzos hechos en este sentido. También se debe saber que se necesita para apuntalar la seguridad además de haber levantado conciencia de seguridad en la demás gente de la organización.

Todo lo anterior nos permite dar paso a toda una metodología de análisis de riesgos, que arroja como resultado un informe de la vulnerabilidad de un centro de cómputo en particular, pero antes es necesario dejar muy claras algunas definiciones que serán de utilidad al repasar la citada metodología.

1.2.1. Definiciones

Las propiedades de la información son las características de este activo que pueden verse afectadas por factores externos en situaciones anormales. Se definen a continuación:

- *Disponibilidad:* Esta propiedad permite contar con la información y/o sistemas que son considerados parte inherente de la empresa, sin que las operaciones pudieran verse disminuidas o en otro caso severamente impactadas, es decir que la disponibilidad de la información se ve afectada cuando el acceso a la aplicación, sistema o información es negado por causas fuera de control (por ejemplo: negar, prolongar o demorar el uso o acceso; desastres mayores, etc...).

- *Integridad:* Propiedad que permite identificar la autenticidad en la información o en el sistema exacta y completamente, es decir, que la información que se esta recibiendo es la verdadera. Se puede decir que la integridad de la información se ve afectada cuando es atentada con una corrupción o modificación no autorizada o no deseada (por ejemplo: introducir, usar o reproducir reportes falsos; modificar, remplazar o re-secuenciar la información, etc.).

- *Confidencialidad:* De manera general, se refiere a la propiedad de la información utilizada por la organización y que es el resultado de algún esfuerzo, gasto o inversión que proporcionan a la organización una ventaja competitiva por lo que la empresa quiere o debe proteger del descubrimiento de un tercer partido. Se ve afectada esta propiedad cuando la información ha sufrido una revelación no autorizada o no deseada (por ejemplo: acceso sin autorización, revelar sin autorización, observar o monitorear transacciones, copiar sin autorización, etc.).

Dentro de lo que se conoce como análisis del valor de los recursos, la regla general para poner un valor a un recurso es la que está definida por el propietario del recurso, esto debe ser lo primero que se haga. Y es por esto que se definen las siguientes jerarquías para el manejo de los recursos:

- *Propietario:* Es el mayor nivel asignado para ejercitar los derechos de propiedad de la organización y las responsabilidades fiduciarias para los recursos que se manejan.
- *Custodio:* Es quien tiene la responsabilidad para proteger los recursos de acuerdo con las direcciones específicas del propietario.
- *Usuario:* Es la persona u organización que ha sido autorizada para tener acceso a los recursos.

Por último se definirá qué es una **amenaza** y se dará una relación de las que se consideran más comúnmente. Este término puede significar un sinnúmero de cosas, típicamente ninguna de ellas buena. Una amenaza normalmente es vista como un intento de hacer algo malo a alguien, a alguna empresa o específicamente, en este caso, a los recursos informáticos.

Existen tres elementos que son asociados con las amenazas:

- *El agente:* Es el catalizador que ejecuta la amenaza, el agente puede ser una persona, una máquina o un fenómeno natural.
- *El motivo:* Ocasionado por el agente, es la razón por la cual la amenaza deja de ser potencial para convertirse en un acto. El único que puede hacerlo de manera accidental o intencional es el factor humano.
- *Los resultados:* Para la comunidad de sistemas de información esto llevaría a perder el acceso o contar con un acceso no autorizado, modificaciones y descubrimiento o destrucción de datos.

Amenazas naturales

Son aquellas que se generan por la presencia de un fenómeno natural y las que normalmente nos toman desprevenidos, aunque en el ambiente de la construcción de

centros de cómputo es común tomar precauciones que van más allá de los estándares de edificaciones para uso de oficinas, por ejemplo.

- *Terremoto:* Un movimiento violento del suelo que resulta de fuerzas y movimientos de la superficie terrestre.
- *Inundación:* Una acumulación de agua originada por causas naturales como lluvia excesiva, movimientos raros de la marea, nieve derretida o acción volcánica.
- *Huracán:* Un ciclón del océano tropical. En general, cualquier ciclón con velocidad superior a 64 km/h se debe considerar (aunque técnicamente un huracán tiene velocidades del viento mayores que 119 km/h). Se considera que tormentas tropicales y tifones también deben estar en esta categoría de amenazas.
- *Derrumbe:* Un movimiento súbito o violento de tierra o rocas sueltas debido a erosión, sismo o defecto de ingeniería.
- *Relámpago:* Una descarga eléctrica en el aire causa un rayo que de manera directa puede golpear las líneas de transmisión de energía eléctrica, los transformadores, etc.
- *Tormenta de nieve/hielo:* Fuerte y prolongada precipitación en forma de nieve, hielo, granizo o aguanieve.
- *Tornado:* Columna de aire de gran diámetro que gira violentamente, en cuyo eje central existe una fuerte corriente vertical ascendente, capaz de elevar en el aire objetos pesados. Cualquier columna de aire que gire con velocidad mayor a 64 km/h puede ser considerado.
- *Tsunami:* Ola de agua inusualmente grande y destructiva (p.e., maremoto) causada por un terremoto o actividad volcánica submarina.
- *Erupción volcánica:* Cualquier eyección de lava, lodo, nubes del polvo o flujo magnético.
- *Tormenta de viento:* Clima con ráfagas frecuentes de viento a más de 64 km/h no incluido arriba en otra categoría de riesgo.

Amenazas accidentales

Entran en esta categoría todas aquellas que tienen su origen en el descuido del factor humano y que no tienen la intención de causar un daño a los recursos, o bien son fallas en la infraestructura que soporta el centro de cómputo. Definiremos los más comunes:

- *Revelación:* La liberación prematura, accidental o no autorizada de información sensible; ya sea clasificada, personal, confidencial o de patente.
- *Perturbación eléctrica:* Una fluctuación momentánea en la fuente del poder eléctrica, puede ser un pico de voltaje, caída de voltaje o interrupciones de menos de media hora.
- *Interrupción eléctrica:* Una interrupción de largo plazo de la fuente de energía eléctrica, usualmente más de media hora.
- *Emanación:* La emanación inadvertida o transmisión de señales de datos de componentes de computadoras, periféricos y procesadores de palabras, que pueden ser grabados por equipos de monitoreo.
- *Falla del ambiente controlado:* Una interrupción en el suministro de servicios de ambiente controlado en el centro de cómputo. El medio ambiente controlado incluye la calidad del aire: temperatura, humedad y limpieza.
- *Fuego:* Una conflagración que afecta los sistemas de información por calor, humo o residuos del agente extintor. Se puede descomponer esta amenaza por categorías: menor, mayor y catastrófico.
- *Fallas en el hardware:* Una falla en una unidad o componente basta para causar retrasos en los procesos o pérdida monetaria a la empresa.
- *Derrame de líquidos:* Presencia excesiva de líquidos provenientes de fuentes distintas a la lluvia. Ejemplos de esto incluyen cañerías reventadas o con goteras y la descarga accidental de rociadores.
- *Error del software:* Cualesquiera datos extraños o erróneos en el sistema operativo o programas de aplicaciones que dan por resultado errores de proceso, errores en los datos de salida o retrasos de proceso.
- *Interrupción de las telecomunicaciones:* Cualquier falla en componentes o unidades de comunicación es suficiente causar interrupciones en la transferencia de datos vía

telecomunicaciones entre terminales de computadora, procesadores remotos o distribuidos y el servidor central.

Actos intencionales

Finalmente, la amenazas por actos voluntarios destinados a alterar o dañar los recursos informáticos. Generalmente son los más difíciles de prever y controlar porque son perpetrados desde el interior de las instalaciones.

- *Alteración de datos:* Una modificación intencional, inserción o borrado de datos; hecha por usuarios autorizados o no autorizados, que comprometen la auditabilidad, recuperabilidad, disponibilidad, confidencialidad o integridad del información producida, procesada, controlada o almacenada por los equipos de proceso.
- *Alteración de software:* Una modificación intencional, inserción o borrado del sistema operativo o programas de aplicación del sistema, por usuarios autorizados o no, que comprometen la auditabilidad, eficacia, recuperabilidad, disponibilidad, confidencialidad o integridad de la información, programas, el sistema o recursos controlados por el sistema de cómputo.
- *Amenaza de bomba:* Una notificación de la existencia de un aparato explosivo en algún lugar del centro de cómputo, sea esta amenaza verdadera o no.
- *Descubrimiento:* La liberación no autorizada o prematura intencional de información clasificada, confidencial, personal, de propiedad o sensitiva para la empresa.
- *Sabotaje por parte de algún empleado:* Una acción deliberada hecha por un empleado, grupo de empleados o no-empleado(s) coludido(s) con empleado(s) para dañar el funcionamiento de la empresa.
- *Fraude:* Una manipulación deliberada no autorizada de hardware, software o información con la intención de obtener ganancias financieras por parte del perpetrador.
- *Alboroto/desorden civil:* Un disturbio de grupo (organizado o no) que causa generalizada e incontrolable suspensión de la ley y el orden social.

- *Huelga:* Una acción organizada por empleado (sindicalizados o no, legal o no) diseñada para detener o romper el funcionamiento normal de la empresa.
- *Robo:* La apropiación no autorizada de hardware, software, medios de comunicación, suministros para computadora o datos clasificados.
- *Uso no autorizado:* Un uso no autorizado del equipo de cómputo y/ o programas. Ejemplos de esto incluyen el uso de programas personales tales como juegos, Internet y otros archivos.
- *Vandalismo:* El daño a la propiedad de la empresa sin ningún motivo.

1.2.2. Metodología de análisis de riesgo

Contar con una metodología concreta para el análisis de las amenazas latentes a los recursos de un centro de cómputo, debe tener como objetivo la identificación los posibles eventos no deseados o no autorizados, llamados "riesgos", que podrían tener un impacto negativo en la integridad, confidencialidad o disponibilidad de la información procesada o que fluye a través de una aplicación o en un sistema. Al mismo tiempo debe identificar los posibles "controles" para reducir o eliminar el impacto de determinados riesgos, siendo éste el principal interés. Y por último debe establecer un "plan de acción" para la implementación de controles elegidos.

Así pues, los recursos informáticos son el objetivo central del análisis de riesgo. La definición de los recursos está generalmente descrita en el siguiente modelo:

- Hardware
- Software
- Datos
- Documentación

Aunque la mayoría de las veces esta lista se extiende a:

- Personal
- Procedimientos
- Equipo de comunicación

- Datos lógicos en lugar de archivos físicos
- Servicios intangibles

Los siguientes son los pasos que, a grandes rasgos, describen la metodología que permitirá hacer una evaluación de la situación actual de los centros de cómputo; identificando las amenazas del medio ambiente para emitir como producto un plan de acción para la corrección de las debilidades encontradas.

1.- Comenzar el proceso con una entrevista diseñada para identificar y cuantificar todos los tipos de recursos informáticos elaborando un inventario que debe incluir: equipo de cómputo, periféricos, equipos auxiliares, equipo de comunicación, aplicaciones, manuales técnicos y de usuario, etc. Algunas recomendaciones para facilitar la entrevista son:

   a) Permanecer neutro todo el tiempo.
   b) Estar preparado (elaborar cuestionario, previamente).
   c) Ayudar a los entrevistados a visualizar la situación.
   d) Mantener la entrevista a paso firme (evitar distracciones).

2.- Hacer una clasificación de los riesgos latentes con base a las definiciones de la sección anterior, ordenándolos de la manera siguiente:

   Actos accidentales:

   - Eventos indeseables (incluir aquí las amenazas naturales)
   - Omisiones y errores

   Actos deliberados:

   - Eventos no autorizados
   - Fraude y mal uso de información

3.- Elaborar una matriz de análisis de riesgo con el fin de revisar los objetivos de la seguridad bajo las siguientes tres categorías: integridad de los datos, sensibilidad de los datos y disponibilidad de los datos. En la figura 1.1, se muestra el arreglo que debe tener esta matriz agrupando en cada celda las amenazas encontradas para

cada una de las propiedades del que debe ser uno de los activos más preciados: la información.

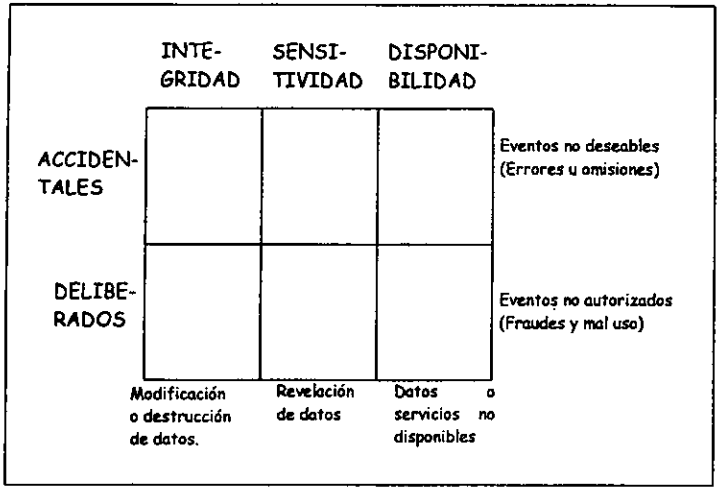


Figura 1.1 Matriz de análisis de riesgo.

4.- Preparar un documento para revisión y aplicar una valoración de los recursos en los que se detectaron riesgos. Aquí se debe recordar que según la definición del análisis del valor de los recursos, ésta es una actividad que debe ser ejecutada por el propietario y que se debe basar precisamente en el documento que se preparó a partir de la matriz del análisis del punto anterior.

5.- Ordenar los riesgos identificados, iniciando con el más urgente y sugerir controles o salvaguardas y restricciones para la protección de cada riesgo. Resaltar que la salvaguarda o control es la protección o medida que se adopta para cubrir los huecos expuestos en puntos vulnerables. Así, desde que las amenazas, impactos y puntos vulnerables son implicados en un nivel de riesgo, las protecciones pueden reducirlo a un nivel aceptable.

Las salvaguardas son generalmente divididas en tres categorías como: preventivas, de detección y correctivas. Y es posible que las salvaguardas transfieran el riesgo a

algún otro lugar (por ejemplo: un seguro). Así que las salvaguardas generalmente tienen costos de mantenimiento y adquisición, como los recursos.

6.- Presentación de resultados a la dirección escribiendo un reporte final que incluya las recomendaciones hechas.

No importa que tan científicamente fue conducido el análisis de riesgos o que tan sorprendentes sean los resultados, el análisis es un fracaso a menos que los resultados puedan ser presentados a la dirección en forma entendible y justificable. Generalmente las gráficas son la mejor manera de mostrar los resultados del análisis de riesgo.

1.3. Marco Normativo

Con la proliferación de los sistemas de cómputo, es esencial la estandarización de las funciones de seguridad que abarquen tanto a las computadoras como a las redes de trabajo. En el pasado, los esfuerzos de una estandarización y normatividad adecuada ha sido manejado principalmente por entidades gubernamentales, aunque la apreciación generalizada es que esta estandarización y aplicación de sanciones por parte del gobierno no está muy acorde con el desarrollo tecnológico y el avance de los ilícitos computacionales.

En años recientes los esfuerzos por normar adecuadamente para la seguridad informática se han incrementado y existen iniciativas principalmente por parte de organizaciones de usuarios de computadoras. Ambos, usuarios y vendedores, están llegando juntos a un acuerdo para determinar que funciones de seguridad son apropiados para prevenir y sancionar los actos delictivos en los sistemas de cómputo modernos.

A continuación se muestra la tabla 1.1, en la cual se hace un resumen de las actividades relevantes que en materia de normatividad y estándares para la seguridad

en computación están llevando a cabo algunas organizaciones tanto gubernamentales como descentralizadas, principalmente en los E.E.U.U.

Organización	Descripción
ABA	La *American Bankers Association* desarrolla estándares para las áreas financiera y bancaria. Los estándares desarrollados por este comité se enfocan en encripción y autenticación de mensajes para instituciones financieras. El ABA también desarrolla normas para números de identificación personal (PIN's) y llaves de administración.
ANSI	El *American National Standars Institute* es la organización designada oficialmente para estándares nacionales en los Estados Unidos y es su representante formal ante ISO. ANSI no desarrolla sus propios estándares pero marca la pauta para estándares de los E.U. e internacionales (por ejemplo: código ASCII, lenguajes y protocolos de comunicación).
CBEMA	La *Computer and Business Equipment Manufacturers Association* desarrolla estándares en una gran variedad de áreas, incluyendo lenguajes, gráficas y tecnologías de bases de datos. Se envían estos estándares para su aprobación a ANSI y se distribuyen como estándares ANSI.
CCITT	El *Comité Consultatif Internationale Telegraphique et Telephonique* fue establecido por las Naciones Unidas y es el responsable de los estándares X.25 (intercambio de paquetes en redes de trabajo) y X.400 (correo electrónico) y de otros estándares internacionales de comunicaciones. CCITT trabaja con ISO en la elaboración de estándares internacionales para seguridad.

Tabla 1.1 Estándares desarrollados en relación con la seguridad (continúa...).

Organización	Descripción
ECMA	El *European Computer Manufacturers Association* es una asociación de aproximadamente 50 manufactureras europeas de computadoras. Es un grupo de seguridad que está involucrado en el desarrollo de estándares para seguridad en áreas tales como: proceso interactivo de distribución, distribución de aplicaciones de oficina y sistemas abiertos.
EIA	La *Electronic Industries Association* es una organización de comercio que ha desarrollado estándares como el RS-232 para conexión de terminales y computadoras.
IEEE	El *Institute of Electrical and Electronic Engineers* es una organización profesional que desarrolla estándares y los envía a ANSI para su aprobación. El estándar IEEE 1003.1, anunciado en 1988, es el estándar oficial POSIX (*Portable Operating System Interface for Computer Environments*) para la portabilidad de aplicaciones en sistemas abiertos.
IFIP	La *International Federation of Information Processing* es una federación multinacional de profesionales y organizaciones técnicas involucradas con el proceso de información y las computadoras. Originalmente se estableció bajo el auspicio de la UNESCO. El comité técnico 11 (TC-11) en seguridad y protección de sistemas de información trabaja en la divulgación internacional de información de seguridad y en el desarrollo de estándares.

Tabla 1.1 Estándares desarrollados en relación con la seguridad (continúa...).

Organización	Descripción
ISO	La *International Standars Organization* fundada en 1946, es una organización internacional por varias organizaciones de estándares nacionales. ISO y otras organizaciones están trabajando en la extensión del modelo OSI (*Open Systems Interconection*) para definir la seguridad relacionada con la arquitectura de los elementos. Varios grupos dentro de ISO están desarrollando estándares utilizando la criptografía como un mecanismo de seguridad en redes de trabajo. Estos estándares proveerán confidencialidad e integridad a los datos y para cada usuario la autenticación, control de acceso, distribución de llaves y firmas digitales.
MAP/TOP	El *Manufacturing Automation Protocol/Technical Office Protocol* es un consorcio de usuarios de fábricas automatizadas patrocinado por General Motors (MAP) y *Boeing* (TOP) que trabaja en partes de los estándares ISO.
NCSC	El *National Computer Security Center* publica la serie arcoiris de estándares de seguridad en computadoras para sistemas confiables sobresaliendo el Orange Book. El NCSC patrocina el Trusted UNIX Organization, que consiste de un grupo de vendedores, incluyendo a AT&T, involucrados en el desarrollo de sistemas UNIX confiables.
NIST	El *National Institute of Standars and Technology* (formalmente llamado *National Bureau of Standars*) especifica estándares para productos y procedimientos relacionados con el gobierno de los Estados Unidos.

Tabla 1.1 Estándares desarrollados en relación con la seguridad (continúa...).

Organización	Descripción
X/Open	La organización *X/Open* se fundó en 1984 como un consorcio de cinco manufactureras americanas y europeas de computadoras. Están involucrados dentro de un grupo internacional que se dedica al desarrollo de estándares en la portabilidad de aplicaciones en sistemas abiertos, comúnmente llamados "el medio ambiente de las aplicaciones comunes".

Tabla 1.1 Estándares desarrollados en relación con la seguridad.

Adicionalmente a estas organizaciones, existen un gran número de grupos de usuarios orientados a la comercialización de la seguridad que juegan un papel activo en la distribución de información de seguridad y, en algunos casos, tienen la iniciativa de desarrollar estándares de seguridad. Aquí se incluyen el *Computer Security Institute* (CSI), la *American Society for Industrial Security* (ASIS) y la *Information Systems Security Association* (ISSA).

En México existen instituciones como la ANIPCO que aunque no son generadoras de estándares se formaron para dar seguimiento a violaciones de la normatividad establecida, por ejemplo: apoyan a entidades de gobierno para la ejecución de auditorías en sistemas de cómputo principalmente para la detección de software pirata que atenta contra los derechos de autor. También tienen labor de difusión de las leyes que existen en esta materia y son precursores del desarrollo de una conciencia de seguridad en los usuarios.

1.3.1. Seguridad Corporativa (Políticas)

Un programa de protección a las computadoras y/o a la información de la empresa, debe formar parte del programa de protección de los recursos de una organización. Debiendo marcar especialmente los rubros relacionados con la entrada de los empleados de nuevo ingreso asignados a la responsabilidad de proteger la información;

sin que esto sea un sustituto de la supervisión constante de las actividades de estos empleados o motivo de evitar un cambio imprevisto de planes para la protección de la información.

Con el uso de las computadoras aumentó, alrededor del mundo, la necesidad de contar con políticas cuyo objetivo debe ser el establecimiento de un mensaje universal que todos los empleados puedan entender y adoptar, desde los de nuevo ingreso hasta los de nivel administrativo más alto.

El desarrollo de políticas de protección a la información es parte de un programa de protección a los recursos de una organización que sin la comprensión de la dirección para el soporte de los objetivos del programa tiene una probabilidad de éxito muy bajo.

El objetivo de las políticas es poner la primera piedra para el desarrollo de un programa de seguridad completo. Las políticas sustentarán la infraestructura de los estatutos, normas, procedimientos y reglas de la organización por lo que deben tener las siguientes características:

- *Ser fácil de entender.* La lectura y el nivel de comprensión debe estar al nivel de todo el personal de la empresa.
- *Ser aplicable.* Se debe estar seguro de que cualquier política escrita describe a la organización.
- *Ser realizable.* Preguntarse, por ejemplo, si los empleados ¿pueden todavía cumplir con los objetivos de la empresa si la política está implementada?
- *Ser imponente.* No se debe indicar a los empleados que una causa específica y un efecto ocurrirá, sólo se debe escribir la política.
- *Ser hecha en etapas.* Permite a la organización leer, resumir y responder a la política.
- *Ser activa.* Se deben usar frases que definan acciones evitando aquellas frases que limiten la actividad.
- *Evitar lo absoluto.* Nunca decir nunca. Ser diplomático y entender el camino lícito para decir las cosas.

- *Conocer los objetivos de la empresa.* Permite a la organización identificar un nivel aceptable de riesgo.
- *Cubrir todas las formas de información.* La computadora cubre solamente del 10 al 15 % de la información de toda la organización.
- *Obtener un soporte apropiado de la dirección.* Una política que no tiene eco en los niveles superiores difícilmente se puede implementar en la empresa.

Contenido de las Políticas

Las políticas son generalmente cortas (en comparación con los procedimientos), generalmente no más de una o dos páginas deben describir la manera de actuar dentro de la empresa. Y se debe estar consciente de que aquello que está escrito debe aclarar confusiones y no generar nuevos problemas. Cuando se escriben las políticas se debe recordar lo siguiente:

- ¿Qué debe ser protegido?
- ¿Quién es el responsable?
- ¿Cuándo la política toma efecto?
- ¿Dónde dentro de la organización la política se extiende?
- ¿Porqué la política fue desarrollada?
- ¿Cómo será supervisada la obediencia?

Permitiéndose incluir algunos artículos adicionales como los siguientes:

- ¿Qué área autoriza la política (desarrollo y prueba)?
- ¿Quién tiene la actual responsabilidad?
- ¿Con qué frecuencia será la política revisada y actualizada si es necesario?
- ¿Cuáles son los procedimientos de corrección de desviaciones?
- ¿Cuál es la fecha de la última revisión?

Una vez que se cuenta con las políticas adecuadas dentro de la empresa se está en posibilidad de redactar las normas y los procedimientos necesarios para que cada una

de las áreas en específico tenga los elementos que le permitan desarrollar su trabajo sin salirse de la ruta que marcan las mencionadas políticas.

Con este repaso a las bases de las seguridad corporativa y desarrollo de políticas internas se concluye el primer capítulo. Y ahora ya se tiene la referencia histórica y los hechos relevantes que marcan la evolución de la seguridad en las empresas y en particular en los centros de proceso de información, además de algunos conceptos que ayudarán a la mejor comprensión de los temas restantes.

En el siguiente capítulo se establecerán las bases de las seguridad física a partir de la descripción de toda la infraestructura necesaria para que los equipos de proceso de datos no se vean afectados por las amenazas inherentes al medio ambiente. Es decir, se describirán los equipos auxiliares e instalaciones físicas que permitirán una mayor confiabilidad en la operación de cualquier centro de cómputo.

2

SEGURIDAD FÍSICA

En el entorno de operación de cualquier sistema de cómputo, cualquiera que sea el tamaño de éste, existen elementos que amenazan o ponen en riesgo la operación de los mismos sin que hasta la fecha se tenga un esquema que permita garantizar la eliminación de eventos perjudiciales que puedan dar como resultado la pérdida de alguna cualidad (integridad, confiabilidad, disponibilidad) de la información que se procesa.

En este capítulo se hará un repaso del equipamiento e instalaciones que funcionan como mecanismos de control para mejorar la seguridad física y reducir los riesgos que afecten a los centros de cómputo.

La seguridad física se refiere a las medidas tomadas para proteger sistemas, edificios y lo relacionado con la infraestructura de apoyo, contra amenazas asociadas con el ambiente físico. Dichas medidas deberán tomar en cuenta los factores definidos a continuación:

- *Ubicación física:* Es normalmente el edificio, estructura o vehículo que alberga los componentes del sistema y de la red, estos últimos se pueden clasificar en: estáticos, móviles o portátiles.

- *Ubicación geográfica del inmueble:* Se refiere la región en donde se localiza el inmueble y que permite clasificar los riesgos inherentes (p.e.: sismos, inundaciones, robos, manifestaciones, explosiones, interferencia electromagnética, etc.).

- *Servicios de apoyo*: Son aquellos recursos que soportan el funcionamiento de los sistemas (p.e.: suministro eléctrico normal y de emergencia, UPS's, aire acondicionado, etc.).

La seguridad física dimensiona sus resultados por medio de los beneficios en aspectos tan importantes como la protección de los recursos (humanos, materiales, etc.).

Dentro de la seguridad física se considera la protección de los sistemas de cómputo contra los siguientes riesgos:

- Interrupción de los servicios de cómputo proporcionados.
- Daño físico.
- Acceso no autorizado a las áreas de proceso.

Por esta razón se considera el reforzamiento de varios aspectos que mejoran la seguridad física y reducen los riesgos a un nivel controlable, los aspectos que se consideran a continuación son:

- Parámetros constructivos.
- Controles de acceso.
- Instalaciones eléctricas.
- Servicios de apoyo (equipos auxiliares).

2.1. Parámetros constructivos

La inmensa mayoría de los edificios administrativos no están proyectados para la función informática; en la actualidad, los técnicos van tomando conciencia de este tipo de instalaciones y poco a poco se encaminan hacia una nueva tecnología informática. Arquitectura e Ingeniería Industrial, así como otras áreas relacionadas, no han llegado a un entendimiento pleno en este nuevo concepto de instalaciones que sin lugar a dudas es una "mezcla especial" de todas ellas. A la hora de proyectar un edificio que revista la categoría de informático, se deben presentar dos casos perfectamente diferenciados:

1) Que el edificio esté ya construido (readaptación).
2) Que el edificio se deba construir (construcción).

La experiencia dicta que en la mayoría de los casos el edificio se encuentra ya construido (por lo menos es el caso más probable); por tanto, habrá que darle forma, proyectar su interior y exigir que cumpla unas condiciones mínimas de trabajo, en cuanto a la instalación de equipos informáticos se refiere. Para lo cual será necesario fijar los parámetros de construcción que tengan en consideración los criterios que serán discutidos a continuación:

- Ubicación geográfica
- Requerimientos estructurales
- Distribución interna
- Ubicación de equipos auxiliares

2.1.1. Criterios para ubicación geográfica

Si el edificio debe construirse se tomará como norma general, antes incluso de tomar en cuenta la arquitectura, unos criterios muy sencillos de elección, que también pueden ser útiles si se trata de readaptación de uno ya construido. En primer lugar, y por motivos de seguridad externa, una construcción de estas características estará exenta de edificios colindantes o anexos. Se puede proyectar de forma que el bloque quede rodeado perimetralmente de un terreno lo suficientemente extenso para su protección.

En segundo lugar, no estará situado en un área industrial que por su actividad desprenda gran cantidad de polvo al exterior, ya que esto podría afectar considerablemente y de forma perjudicial a las computadoras. También se tendrá en cuenta la presencia de determinadas industrias que puedan crear campos magnéticos o eléctricos de alta frecuencia, que producirían saltos y/o rayas en las pantallas. Los campos magnéticos pueden provocar el borrado total o parcial de los soportes magnéticos, cintas, cartuchos magnéticos, discos flexibles, etc.

Tampoco es aconsejable proyectar el edificio en altura aunque de todas formas se deberán observar en todo momento las indicaciones dadas para las estructuras sismoresistentes, en previsión de posibles movimientos. La seguridad, en este tipo de edificios, para la evacuación de personas es otro de los factores a tener en cuenta a la hora de su diseño; la relación en planta con una vía central de evacuación deberá ser inmediata y transparente debido a que cada día que pasa las regulaciones son más estrictas en cuanto a medidas de seguridad, nos referimos, sin duda, a minimizar los recorridos desde cualquier punto del edificio para su rápido desalojo en caso de inminente peligro.

Si se dispone de suficiente terreno, lo aconsejable es hacer la edificación lo más extensa que sea posible horizontalmente, en planta. Con este sistema se conseguirán resultados más eficaces en cuanto sismoresistencia, posible evacuación, seguridad y luminosidad. Se deberá de cuidar que la relación con los patios y el sentido de salida sean muy simples y sencillos desde cualquier puesto de trabajo.

Un factor adicional es la elección de una zona que no represente riesgos de disturbios civiles o vandalismo. La ubicación del inmueble en zonas populares o en las cercanías de algún edificio público en el que sean recurrentes las manifestaciones violentas o no violentas, puede significar la presencia de problemas que pueden ir desde daños a los bienes hasta peligro para el personal que ahí labora, por lo que es un riesgo que de ser posible debe evitarse.

Por último, los servicios indispensables para la operación de las instalaciones informáticas deben ser de la mejor calidad posible; por lo que debe elegirse una zona que se distinga por la calidad de sus servicios de distribución de agua, energía eléctrica y principalmente servicios modernos de comunicación; siendo este último el servicio que cobra mayor importancia debido a que por ser el más caro en su aprovisionamiento es poco probable que se tenga la infraestructura para contar con una red de intercomunicación propia. Los servicios de agua y energía eléctrica se pueden mejorar para su consumo con una inversión pequeña comparada con la inversión en infraestructura que se requeriría para soportar la caída de los servicios de comunicación, por ejemplo.

Además, el estudio para la elección del edificio debe comprender todo lo que compete a la arquitectura tradicional y muy especialmente:

- Estructuras y sus resistencias.
- Suministros de energía eléctrica.
- Instalaciones.
- Seguridad.

2.1.2. Requerimientos estructurales

Una vez definida la ubicación geográfica del edificio atendiendo a los criterios discutidos en la sección anterior, se deberá atender el problema específico del cuarto en el que se alojarán los equipos de proceso central, es decir, el centro de cómputo que como tal deberá cumplir con ciertas características constructivas para brindar un alto nivel de seguridad para que los riesgos se queden fuera. Se debe recordar que la principal preocupación de la seguridad física es evitar daños a la infraestructura que soporta el centro de cómputo y a los equipos mismos, por lo que el cuarto o cuartos destinados a éste uso serán construidos con estándares superiores a los considerados en el resto del inmueble.

El primer paso es definir en que planta se debe ubicar el centro de cómputo, lo cual sería una decisión fácil en el caso de que se tratara de una construcción nueva porque se estaría en condiciones de diseñar una estructura lo suficientemente resistente en el área elegida. Sin embargo, en el caso de una readaptación se hace necesaria la evaluación especializada para comprobar la resistencia y características constructivas del lugar seleccionado y, en su caso, reforzar esta sección del inmueble.

Antes de ejecutar cualquier obra civil se deben considerar las siguientes condiciones:

- Que el acceso para equipo sea amplio.
- Que no crucen esta área tuberías de agua horizontales ni verticales, exceptuando las específicas para el aire acondicionado.
- Previsiones para el suministro de energía eléctrica.
- Evitar la cercanía de fuentes de interferencia electromagnética (p.e.: motores).
- Garantizar la resistencia de la estructura.
- Según el equipo a instalar es aconsejable observar lo siguiente:
    - Situación de columnas
    - Situación de puertas
    - Pasillos de seguridad
    - Previsión de espacios para futuras ampliaciones.

Un parámetro fundamental para la elección del lugar que ha de ser utilizado como cuarto de cómputo es la resistencia del suelo, que debe ser superior los 600 kg/cm^2 ([1]) (normalmente entre 600 y 1200 kg/cm^2) dependiendo de la cantidad y tipo de equipos a instalar. Aunque se sabe que poco a poco los equipos de cómputo van reduciendo su volumen y tamaño y quizá en un futuro sea necesario proyectar de nuevo esta cifra de resistencia; hoy por hoy sigue siendo perfectamente válida.

Por lo que se refiere a los muros perimetrales del área dedicada a equipos de proceso y periféricos, es necesaria su construcción en base a concreto armado con malla electrosoldada para una resistencia mínima de 100 kg/cm^2, suficiente para cumplir con

[1] Soriano Calvo, Carlos A..- Instalaciones de salas informáticas.- edit. Parainfo

un nivel de seguridad clasificado como nivel 3 (a prueba de impactos equivalentes a 30 gramos de explosivos plásticos)[1]. Ninguno de estos muros deberá tener ventanas y la puerta de acceso debe ser de tipo tambor metálico que proporcione también un blindaje de nivel 3 con tratamiento aislante especial para no permitir el paso del fuego. En los muros se deben prever únicamente los ductos para paso de cableado de comunicaciones, acometida eléctrica y conexiones del aire acondicionado.

Por último el techo debe ser tratado especialmente para garantizar que no existan filtraciones de humedad con un nivel de resistencia suficiente para soportar algún equipo auxiliar, debido a que es generalmente en el techo donde se instalan las condensadoras de los equipos para aire acondicionado en el caso de equipos de tipo dividido. La altura de piso real a techo real debe estar prevista en al menos 3.2 metros si es que se planea instalar falso plafón y piso falso (las ventajas y características de ambos las analizaremos en una sección posterior).

2.1.3. Distribución interna

Una vez seleccionada la mejor ubicación geográfica del centro de cómputo, así como características de resistencia de la construcción, ajustados a los criterios anteriormente expuestos, se deben tomar en cuenta las áreas funcionales internas en las que debe ser dividido el local. Deben existir los siguientes espacios perfectamente delimitados:

- Espacio para el equipo central de proceso (área estática).
- Espacio para terminales y estaciones de trabajo (área dinámica).
- Espacio para equipos de comunicaciones.
- Espacio para impresoras.
- Espacio para archivo de medios magnéticos (área de cintoteca).

Como norma general, es conveniente que todas estas áreas se encuentren dentro del centro de cómputo pues, de esta forma, harán uso de las instalaciones auxiliares (aire acondicionado, UPS, etc.), propias del centro y no será necesario duplicar gastos. En algunos casos es necesario situar alguna de estas áreas en locales separados,

generalmente por falta de espacios en edificios readaptados; las áreas que pueden ser proyectadas en locales anexos son las de cintoteca, la de impresoras y la de terminales; sin embargo, esta separación implicaría la instalación de condiciones ambientales similares al local de proceso.

En la figura 2.1 se presenta un diagrama esquemático de la distribución idónea de una sala informática, la cual permite optimizar la operación e integrar adecuadamente las funciones operativas de un centro de proceso de información.

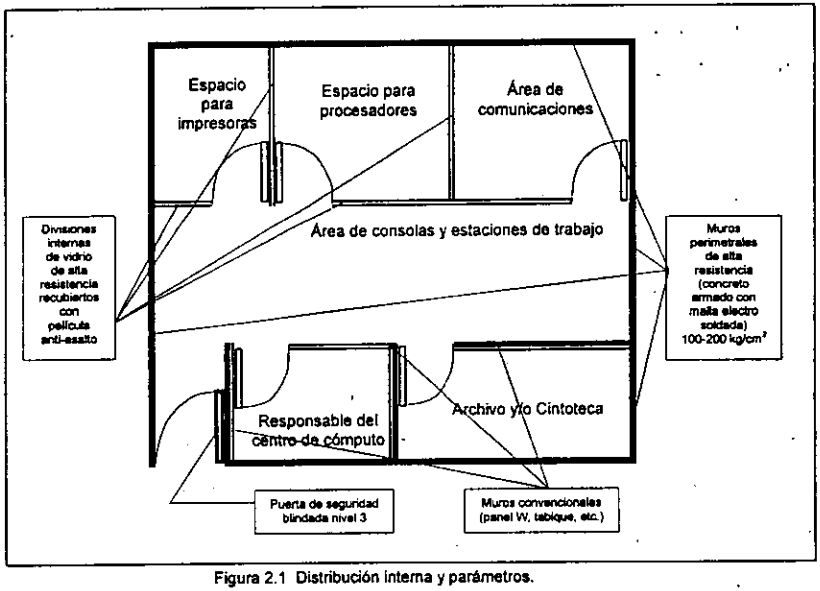


Figura 2.1 Distribución interna y parámetros.

En este esquema se señalan las características constructivas de los muros perimetrales, el tipo de puerta de acceso y los materiales que pueden usarse para las divisiones internas; asimismo se señala una distribución de áreas que puede variar en función de las disponibilidad de espacio, ya que en la figura se representa un área rectangular y en base a ésta se hace la distribución sin perder de vista que los espacios pueden tener muchas y variadas formas. Por lo que, en caso de contar con un espacio

de forma y/o tamaño diferente es conveniente considerar los siguientes puntos para la planeación de espacios:

- El área de telecomunicaciones debe ubicarse en un espació contiguo al área del procesador, de esta manera se facilita el monitoreo de la operación de los equipos más importante en cualquier red informática. Además, algunos servidores de comunicaciones requiere conexión a través de puerto SCSI con el procesador y la longitud del cable de conexión esta restringida a alrededor de un par de metros.

- Las divisiones entre el espacio para impresoras y el espacio del procesador no deben tener interconexión ni por debajo de piso falso ni por arriba del plafón, esto debido a que en el proceso de impresión se liberan demasiadas partículas de polvo que "tienen la costumbre" de alojarse en los mecanismos críticos de los equipos de proceso aumentando el riesgo de fallas. La conexión las impresoras en puerto paralelo del procesador no permite mucha distancia entre estas áreas, por lo que es poco probable alejar el área de impresión de los procesadores.

- El espacio para terminales y estaciones de trabajo debe preverse frente al área de procesadores porque es desde este punto que se hará el monitoreo visual de los equipos de proceso, comunicaciones y respaldo. Además, también en este caso la distancia permitida del cable de conexión de las consolas se vuelve una limitante para la instalación de las mismas.

El espacio para archivo o cintoteca puede estar ubicado en un local anexo, entre otras cosas porque es un local autónomo en el que no existen equipos que se interconecten; sin embargo, como ya se mencionó es necesario que, para la adecuada conservación y durabilidad de los dispositivos de respaldo, se tenga la precaución de dotar a este local con la adecuada hermeticidad para evitar el acceso de partículas de polvo y los equipos para aire acondicionada para el adecuado control del ambiente (temperatura y humedad). Es también un espacio de poco acceso de personal por lo que se deberán instalar los dispositivos de detección de fuego y humedad necesarios para prevenir algún accidente con la información almacenada. En una sección posterior se estudiará

a detalle los requerimientos de instalaciones de protección necesarios para este local en particular y para el centro de cómputo en general.

2.1.4. Ubicación de equipos auxiliares

El avance tecnológico ha hecho que los equipos de cómputo sean cada vez más pequeños y eficientes, es decir, que el consumo de energía eléctrica es cada vez menor y la disipación de calor en condiciones normales de operación ya es mínima. Por esta razón, esos cuartos de máquinas que resguardaban aquellos equipos de acondicionamiento ambiental con grandes compresores y manejadoras de aire, aquellos sistemas de energía ininterrumpida (UPS por sus siglas en inglés) que requerían grandes bancos de baterías y aquellas plantas de energía eléctrica tan grandes en tamaño y tan molestas por el nivel de ruido generado, son cosa del pasado.

Es común, hoy en día, ver salas de proceso informático en las que un UPS de hasta 20 kVA's es parte de mobiliario habitual; integrando en un solo gabinete de dimensiones aceptables que incluye el propio equipo electrónico y su correspondiente banco de baterías que le permite autonomía de operación hasta de dos horas en ausencia de energía eléctrica comercial. La característica de ser un equipo electrónico y muy caro hace necesario que se tengan cuidados similares a los del equipo de cómputo en lo que se refiere a humedad y temperatura ambiental, por lo que es conveniente que se encuentre instalado dentro de la sala de proceso.

Los equipos para aire acondicionado, dependiendo de su capacidad, pueden ya ser instalados sin la necesidad de un cuarto especial para guardar los compresores y manejadoras de aire; y podemos ver dentro del local equipos de tipo dividido en los que sólo se requiere instalar en el exterior la unidad condensadora que se conecta a la unidad principal a través de un tubo de cobre, evitando así aquellos ductos que tradicionalmente ofrecían una alternativa para penetrar en el cuarto de proceso de manera furtiva y tal vez poner en riesgo la integridad de las computadoras. Sin embargo, la necesidad de un mayor volumen de aire acondicionado hará necesaria la instalación de otro tipo de equipo, que si requerirá de un local que ofrezca seguridad y

que esté lo suficientemente cerca del cuarto de proceso para evitar pérdidas y gastos innecesarios del aire tratado.

El único equipo auxiliar que puede, y debe estar alejado del cuarto de computadoras es la planta generadora de energía eléctrica de emergencia, debido al nivel de ruido que produce y la presencia de fuertes campos electromagnéticos que se presentan durante su operación. En caso de que exista un cuarto especial para la acometida eléctrica en el que se tenga instalada una subestación, es recomendable que ahí mismo se instale la planta generadora para tener en un solo cuarto, y lejos de las computadoras, las dos posibles fuentes de interferencia electromagnética que comúnmente existen.

2.2. Control de Acceso

Una de las preocupaciones más grandes en lo que a seguridad se refiere, es el hecho de mantener los riesgos fuera y alejados del centro de cómputo. Como vimos en la sección anterior, una adecuada elección de la ubicación del local y una construcción robusta permiten que la mayoría de las amenazas naturales o gran parte aquellas cuya ocurrencia puede clasificarse como accidental reduzcan sustancialmente su probabilidad de causar daños a los recursos protegidos. En consecuencia, el siguiente paso lógico es el establecimiento de medidas de control en los puntos de acceso a las instalaciones para asegurar que las personas que cruzan estos controles están autorizados para permanecer dentro de las áreas protegidas; aunque de ninguna manera se puede, ni se debe, confiar en que con esto es suficiente para tener evitar todos los riesgos ya que se tienen reportes estadísticos que indican que muchas y las mas costosas violaciones a la seguridad se ejecutan desde el interior de las instalaciones. Aunque esto es un asunto que no sólo tiene que ver con la instalación de barreras físicas, sino que involucra hasta una adecuada selección de los recursos humanos entre otras cosas que van más allá del alcance de este trabajo.

Los controles de acceso físico permiten establecer criterios para conceder selectivamente la entrada y salida de personal (y a menudo de equipo y/o medios de almacenamiento) de un área. Los controles pueden ser manuales, semi-automáticos o

automáticos; con niveles de sofisticación tecnológica que depende del tipo de recursos a proteger. Algo muy importante es que deben instalarse no sólo en el área que contiene el hardware del sistema, sino también:

- En los locales de cableado donde se interconectan los elementos del sistema.
- En los servicios de suministro eléctrico.
- En el local donde se encuentran el sistema para aire acondicionado y la planta de emergencia.
- En los locales de acometida telefónica, líneas de datos y respaldo de los medios de comunicación.
- En archivos de documentos fuente.

En esta sección se estudiarán los equipos electrónicos que permiten controlar el acceso a un área a través de la activación o no activación de una cerradura electromagnética instalada en la puerta de entrada. Y, aunque la selección del tipo de cerradura es importante ya que debe cumplir con parámetros de resistencia similares a los de la puerta donde se instala, generalmente se le concede el nivel de seguridad al dispositivo electrónico seleccionado para la activación de la chapa, razón por la cual aquí se analizan varias opciones.

2.2.1. Clasificación

La primera defensa contra intrusos es mantenerlos fuera del edificio o del cuarto de computadoras, por lo que para obtener acceso a un área asegurada, un usuario debe pasar por una prueba de identificación y autenticación que en general debe cumplir las siguientes fases:

1.- Algo que se tiene: una tarjeta, una llave, un gáfete o una tarjeta inteligente.
2.- Algo que se sabe: generalmente una contraseña, y/o
3.- Algo que se es: por ejemplo una huella digital.

Un sistema de control de acceso para seguridad mínima utilizará solamente alguna de las dos primeras fases, es decir, la cerradura se verá activada al reconocer una tarjeta

válida en un lector de tarjetas simple, o al reconocer una secuencia de dígitos en un teclado; sin importar que el portador de la tarjeta o la persona que teclea el código sea o no una persona autorizada para entrar al área protegida. Definitivamente un sistema de este tipo no ofrece confiabilidad alguna, por lo que su uso no debe ir mas allá del control de áreas de uso común o para aquellas en la que no es posible causar daño a equipo o instalaciones críticas para la operación, es decir, que para poder accesar a éstas es necesario superar algún otro sistema de control de acceso de nivel superior al básico.

Para obtener un nivel de seguridad aceptable y sobre todo auditable en un control de acceso es necesario combinar al menos dos fases de las descritas arriba; es decir, una en la que se esté usando un dispositivo en el que se registra información que permite la identificación del portador, misma que quedará registrada en el equipo de lectura; y otra en la que se utiliza un código de acceso personal solamente conocido por el dueño del dispositivo de identificación. Existen muchos sistemas que combinan características de identificación y autenticación, generalmente por medio de distintos tipos de tarjetas y algún código de validación del usuario.

Hasta este nivel se puede asegurar que la persona que logra entrar a un área asegurada es porque cuenta con una tarjeta o dispositivo de acceso válido y que además conoce la contraseña asociada al dispositivo, en este caso ya es posible fincar responsabilidades acerca de los posibles daños causados a equipos o instalaciones durante su permanencia en el interior; sin embargo, no es posible asegurar que a quien se le emitió la tarjeta y contraseña y quien está entrando en ese momento al área restringida son la misma persona, por lo tanto es muy posible que en caso de algún problema o daño a la instalación, la persona responsable o supuesto dueño de la "llave" puede no ser el causante debido, entre otras causas, al extravío o préstamo del recurso.

Un sistema de control de acceso altamente confiable, en el que se puede estar seguro de que sólo las personas autorizadas estarán dentro del área protegida, es aquel que utiliza como medio de identificación alguna característica física, imposible de duplicar,

de la persona a la que se le permitirá el acceso. El uso de estos dispositivos de identificación puede ser suficiente para garantizar que los recursos de cómputo serán utilizados por las personas autorizadas; sin embargo, es posible utilizar alguna otra fase de identificación o autenticación, o aun más, la combinación de varias de ellas para obtener la máxima seguridad, sobre todo si los recursos (llámese equipo, información y/o personas) que serán protegidos son la parte vital de la operación de una empresa aun si su actividad principal no es la de proporcionar los servicios informáticos.

2.2.2. Descripción de equipos

Existen en el mercado una gran variedad de dispositivos de identificación con la correspondiente unidad de lectura que son utilizados por los equipos de control de acceso automatizado, en este apartado se dará una breve descripción de la manera en que opera cada uno de ellos para conseguir que el sistema conceda el acceso.

Tokens

Una *Token* es un objeto que se usa para autenticar la identidad de usuario. Es un aparato electrónico que usualmente contiene información codificada acerca del usuario que está autorizado para portarla. Típicamente se utiliza en combinación con otro tipo de autenticación en sistemas de autenticación de dos factores.

Sistemas Desafío-Respuesta

De manera general, estos sistemas utilizan dispositivos "*hand-held*" que contienen un programa de encripción y una llave; cuando alguien intenta accesar, el sistema emite un desafío con un número aleatorio; la persona teclea este número en su dispositivo "*hand-held*" que encripta y despliega un resultado en forma de número. Este nuevo número se accesará al sistema que comparará la respuesta tecleada con el resultado de su propia encripción del número aleatorio, si ambos números concuerdan se activa la cerradura que permite el paso a la persona en cuestión.

Tarjetas (inteligentes y tontas)

Por muchos años los gafetes de identificación con fotografía han servido como credenciales. Es necesario mostrar el gáfete de empleado para tener acceso al lugar donde trabaja. En estos casos la autenticación es visual por comparación de la fotografía con la cara del portador; sin embargo existen otros tipos de tarjetas como las usadas en los cajeros automáticos (incluidas las tarjetas de crédito) que usan un tipo de verificación más fiable, por identificación de la información codificada magnéticamente en la tarjeta. Así que, este tipo de tarjetas se usa para controlar el acceso a edificios, cuartos de computadoras y a las computadoras mismas.

Las tarjetas inteligentes contienen microchips que constan de un procesador, memoria usada para almacenar programas, datos y algunos tipos de interfaces de usuario. La información sensible se mantiene en una zona secreta de la memoria de sólo lectura, esta zona es codificada durante la fabricación, usando técnicas cripotográficas, y es inaccesible para el dueño de la tarjeta. Existen muchas tarjetas inteligentes que se construyen para trabajar con lectores de tarjeta, en las que la persona inserta la tarjeta en la lectora, el sistema despliega un mensaje y se teclea un identificador personal en respuesta; si el identificador asociado a la tarjeta es válido, entonces se permite el acceso.

Tipos de tarjetas de acceso

- *Tarjetas de identificación con fotografía.*- Contiene una fotografía del rostro que se verifica visualmente por una persona.
- *Tarjeta óptica codificada.*- Contiene un arreglo geométrico de puntos diminutos grabados fotográficamente o por láser que representan unos y ceros binarios que típicamente representan el número de identificación del usuario.
- *Tarjeta con circuito electrónico.*- Contiene un patrón de circuito impreso, cuando se inserta en una lectora, la tarjeta cierra selectivamente los interruptores del circuito electrónico.

- *Tarjeta magnética.*- Contiene particulas magnéticas que codifican el número de identificación permanente de la tarjeta. También se pueden codificar datos, pero la estructura de identificación de la cinta por si misma no se puede alterar o copiar.
- *Tarjeta de metal rayado.*- Contiene renglones de cobre rayado, la presencia o ausencia de rayas determina un patrón de codificación.
- *Tarjeta de capacitancia.*- Contiene un arreglo de pequeños platos conductores, la capacitancia de los platos determina cuales están aislados y cuales están conectados.

Dispositivos biométricos

Cada persona tiene una única configuración fisiológica, conductual y características morfológicas que se pueden examinar y cuantificar, la biometría es el uso de estas características para permitir la identificación positiva de una persona. Se han usado huellas digitales y firmas por años para probar la identificación de un individuo, pero se pueden identificar de muchas otras maneras. Los sistemas de identificación biométricos computarizados examinan un rasgo particular y usan la información para decidir si tienen el derecho de entrar a un edificio, a usar una computadora o accesar a un sistema de información. A continuación se describen los dispositivos más comunes, incluyendo algunos parámetros que evalúan la confiabilidad de cada uno.

- *Lector de huella digital.*- El usuario coloca un dedo en un lector especial, el aparato examina el dedo, digitaliza la huella digital y compara contra un código de huella digital almacenado. Se puede utilizar este método para un individuo específico (comprobación), o para comparar un grupo de individuos contra una base de datos (reconocimiento).

  Indice de falso rechazo = 9.4 % (3 intentos)
  Aceptación falsa = 0 (3 intentos)
  Tiempo medio de proceso = 7 segundos

- *Lector de retina.*- Aquí el usuario ve al interior de un dispositivo óptico especial y el patrón de los vasos sanguíneos se examina por medio de rayo láser.

Indice de falso rechazo = 0.4 % (3 intentos) ó 1.5 % (1 intento)
Aceptación falsa = 0 (3 intentos) ó 1.5 % (1 intento)
Tiempo medio de proceso = 7 segundos

- *Comprobación de voz.*- El usuario dice una frase específica en un micrófono, se analiza el patrón de la voz y se compara contra uno guardado en una base de datos.

  Indice de falso rechazo = 4.3 % (3 intentos) ó 8.2 % (1 intento)
  Aceptación falsa = 0.7 % (3 intentos) ó 0.4 % (1 intento)
  Tiempo medio de proceso = 7 segundos

- *Firma dinámica.*- El usuario firma en una superficie especial que mide rapidez, aceleración y otros factores que relatan la manera en que se escribe la firma mas que como se ve. Su enfoque de diseño permite rechazar personas que intentan efectuar trazos similares falsos.

  Indice de falso rechazo = 2.1 % (3 intentos) ó 9.1 % (1 intento)
  Aceptación falsa = 0.7 % (3 intentos) ó 0.4 % (1 intento)
  Tiempo medio de proceso = 15 segundos

- *Geometría de las manos.*- El usuario pone su mano contra una plantilla con postes que se ajustan para medir acertadamente la relación de dimensiones entre los dedos y la palma.

  Indice de falso rechazo = debajo del 0.1 %
  Aceptación falsa = 0 (3 intentos)
  Tiempo medio de proceso = 5 segundos

- *Reconocimiento facial.*- Una imagen de vídeo de la cara del usuario es digitalizada, la relación entre rasgos faciales, más que la imagen de vídeo misma, se analiza y se compara contra una base de datos de más de 5000 individuos. La tolerancia del sistema se puede configurar para rechazar la misma cara con una expresión diferente, o para aceptar una variedad de expresiones.

  Indice de falso rechazo = 2.5 % (3 intentos)
  Aceptación falsa = 0 (3 intentos)

Tiempo medio de proceso = 18 segundos

- *Escritura dinámica.*- Los usuarios entran su clave y contraseña con signos normales a proceso. Sin embargo, se monitorea la entrada de la contraseña cronometrando sutilmente el patrón de escritura del usuario el cual es casi imposible reproducir.

  Indice de falso rechazo = 11.2 % (3 intentos)
  Aceptación falsa = 0.3 % (3 intentos)
  Tiempo medio de proceso = 4 segundos

2.2.3. Selección de dispositivos adecuados

Un análisis de riesgo bien conducido revelará las amenazas potenciales en cada centro de cómputo y, generalmente, es este estudio el que indica un criterio de selección en base al valor de los recursos resguardados, a los riesgos detectados y al tipo de información procesada.

Sin embargo, una limitante poderosa para la instalación de uno u otro dispositivo puede ser el costo de los mismos o, aun más, las disponibilidad de la tecnología seleccionada en el mercado nacional. Se debe recordar que la mayoría de los productos, al menos los más sofisticados, son fabricados en el extranjero y en algunos casos, aunque sea factible la importación, es probable que no se tenga acceso a la infraestructura de servicio posterior a la instalación, lo cual tendría como consecuencia un deficiente programa de mantenimiento preventivo y en caso de fallas es probable que deba ser desconectado el equipo dejando desprotegidas las instalaciones.

De cualquier modo, el cuarto de computadoras se considera una zona crítica por lo que el sistema de control de acceso que sea seleccionado debe cumplir al menos con la clasificación de nivel de seguridad aceptable; es decir, que debe contar con la combinación de dispositivos para cubrir las fases de identificación y autenticación y que tenga la característica de ser auditable, lo cual implica que las claves de acceso y llaves que porte el usuario deben ser personalizadas, debiéndose generar las políticas de responsabilidad de los usuarios.

Es importante recalcar que la selección del dispositivo de identificación (tarjeta, *token* o biometría), debe ir acompañada de una verificación de que el tipo de cerradura utilizado tenga al menos las características de resistencia similares a las definidas para los muros y la puerta del cuarto de computadoras; porque sería muy lamentable que alguien al encontrarse con que no puede violar el dispositivo de identificación del control de acceso, pudiera con un impacto violento (patada, empellón, explosión) romper la cerradura elegida.

Algunas observaciones finales con respecto a los controles de acceso, que a manera de sugerencias permiten evaluar si están cumpliendo su cometido, son: por ejemplo, repasar la efectividad de los controles de acceso físico en cada área, tanto en horas de trabajo normal como en otros horarios, ya que la efectividad de un control depende tanto de las características de los dispositivos usados como de su implementación y operación. Por lo que las empresas deben determinar: si los intrusos pueden burlar fácilmente el control, que tan difícil es el acceso para los extraños, cual es la efectividad de otros procedimientos de control, la viabilidad de entrada subrepticia, si sería posible pasar por el espacio existente entre el techo y el falso plafón, etc...

Las acciones correctivas pueden dirigirse a cualquiera de los factores señalados recordando siempre que una barrera adicional reduce el riesgo para las áreas que están detrás de la barrera y que reforzar la selectividad en un punto de entrada puede reducir el número de penetraciones.

Con estas sugerencias, que permiten contar con una guía para la adecuada selección de los dispositivos de control de acceso, se concluye esta sección; dando paso al análisis de los servicios de apoyo para la operación del centro de cómputo, iniciando con la descripción de las instalaciones eléctricas.

2.3. Instalaciones Eléctricas

Una vez que se ha configurado el cerco de protección externo, es decir, todos los elementos que protegen al centro de cómputo de los ataques físicos perpetrados desde el exterior, se debe poner atención en proveer los servicios que utiliza el propio centro.

Para empezar, el suministro de energía eléctrica debe ser independiente y único para el cuarto de proceso; tomando en cuenta que la alimentación de los equipos para aire acondicionado deben ser proporcionada por una fuente independiente, aunque esto no siempre es posible; en tal caso, es necesario asegurarse de que la alimentación a los mismos sea proporcionada de manera independiente desde la acometida principal del edificio (subestación) y nunca de un tablero de distribución en el que también estén conectados circuitos que alimenten equipo de cómputo. Esta precaución permite evitar la ocurrencia de variaciones de voltaje atribuidos al arranque de motores involucrados en la operación de los sistemas de aire acondicionado.

En la figura 2.2 se muestra el diagrama típico de la acometida y subestación de un edificio catalogado como informático, en el que la acometida se proporciona en alto voltaje (generalmente 23,000 volts) teniendo dos transformadores para bajar la tensión, a 220 volts uno de ellos y a 440 volts el otro.

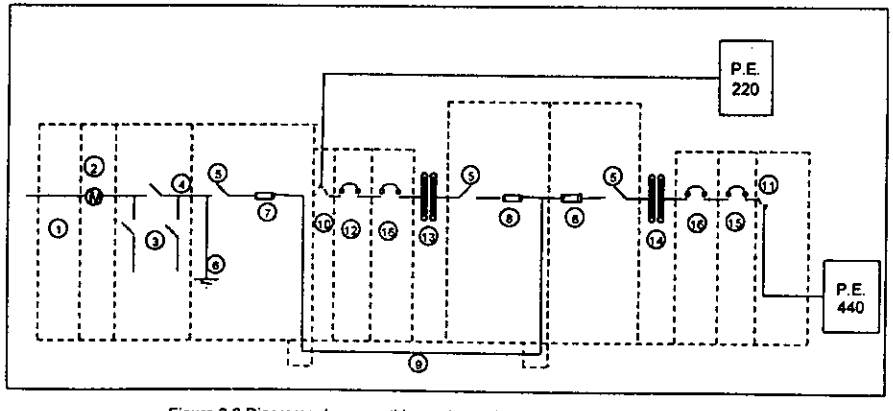


Figura 2.2 Diagrama de acometida y subestación para un edificio informático.

El voltaje de 220 volts trifásicos (127 volts monofásicos), se utiliza para los servicios normales de contactos e iluminación de todo el edificio; mientras que el de 440 volts trifásicos (220 volts monofásicos), es el que se utiliza para alimentar los equipos de aire acondicionado para todo el edificio incluyendo, por supuesto, el aire acondicionado del cuarto de proceso. En la tabla 2.2, asociada a la figura, se describe cada uno de los componentes de señalados en la ilustración.

Número	Descripción
1	Acometida de la compañía suministradora.
2	Equipos de medición de la compañía suministradora.
3	Cuchillas tripolares para operación en grupo por medio de volante.
4	Buses de alta tensión formados con solera de cobre electrolítico con baño de plata.
5	Seccionador de carga tripolar de un tiro para operación en grupo.
6	Apartarrayos autovalvulares servicio interior con sistema neutro-tierra.
7	Fusible de alta tensión y alta capacidad interruptiva.
8	Idem al anterior pero de menor capacidad de corriente nominal.
9	Cable de alta tensión tipo poliphel (xlp).
10	Equipo de transferencia para voltaje de 220 volts.
11	Equipo de transferencia para voltaje de 440 volts.
12	Tablero general con servicio de emergencia a 220 volts.
13	Transformador trifásico conexión delta-estrella con voltaje nominal de 220 volts en el secundario.
14	Idem al anterior pero con 440 volts en el secundario.
15	Tablero general con servicio de emergencia de 440 volts.
16	Tableros de baja tensión.

Tabla 2.2 Descripción de componentes de acometida.

En el caso de estudio, la alimentación para el centro de cómputo se toma del tablero de baja tensión con servicio de emergencia (número 12) y se deriva en dos circuitos: uno para alimentar el equipo de energía ininterrupible (UPS por sus siglas en inglés), donde se conectarán todos los equipos de cómputo; y otro para alimentar contactos de servicio y los circuitos destinados a controlar la iluminación del centro de cómputo. Cabe señalar que, en el caso de edificios ya construidos, no siempre existe este modelo de acometida y que es necesario adaptarse a los recursos que se tienen en cada lugar. Por lo general es posible instalar un tablero independiente en la subestación o acometida principal que permita independizar las instalaciones eléctricas para el cuarto de proceso. Y es muy

probable que no exista una acometida de servicio adicional para los equipos electromecánicos del sistema de aire acondicionado, por lo que también será necesario instalar un tablero diferente para aislar desde este punto la alimentación a estos equipos, cuidando siempre que se cumpla con los estándares que mencionan en el siguiente apartado.

2.3.1. Referencia normativa

Los equipos de cómputo requieren de un suministro de energía eléctrica de calidad, que cumpla con las siguientes propiedades: confiabilidad, regulación y continuidad. Donde las propiedades de regulación y continuidad son proporcionadas por el UPS y la planta de emergencia (de los cuales se hablará específicamente en secciones posteriores); y la confiabilidad que se garantiza a partir del cumplimiento de estándares en el diseño y construcción de las instalaciones en el interior del edificio a partir de la acometida que, salvo por el adecuado dimensionamiento, generalmente queda fuera de la responsabilidad del proyectista.

Una instalación eléctrica confiable cumple con las especificaciones que dictan las Normas Técnicas para Instalaciones Eléctricas (NTIE) y, además, debe tener instalados elementos confiables que cumplan con las características técnicas y acabados que garanticen que fueron fabricados bajo normas de aceptación internacional; por lo que todos los componentes utilizados (cables, contactos, interruptores, etc...) deben contar con aprobación de la Norma Oficial Mexicana (NOM), además de exhibir especificaciones de comportamiento ante fuego y humedad. Las NTIE abarcan prácticamente todos los requerimientos que debe cumplir una instalación eléctrica para que se considere confiable y los técnicos están obligados a cumplir con estas normas; sin embargo, es poco probable que un proyectista pueda verificar que realmente se cumplió con todas ellas, por lo que aquí se señalan algunas características que pueden ser verificadas a simple vista:

- Tableros e interruptores identificados, indicando que equipos están alimentando.
- La tubería de instalaciones eléctricas debe tener sólo cables de energía eléctrica.

- Las tuberías y/o canaletas que contienen cableado de comunicaciones deberán estar separados al menos 15 cm. de las de cableado eléctrico.
- Los contactos con servicio de corriente regulada deben ser de color rojo.
- Cada circuito que alimenta contactos debe contar con tres cables (fase, neutro y tierra) desde el tablero de distribución.
- La calidad de los acabados debe dar confianza al usuario, por lo que tableros, tuberías y contactos deben estar bien sujetos (de preferencia empotrados).

Adicionalmente se debe contar con la documentación certificada por el responsable técnico, en donde se relacionen todos los parámetros de diseño que serán útiles para posteriores referencias y/o adecuaciones. La información a detalle de lo que debe contener esta memoria técnica se describe a continuación.

2.3.2. Memoria técnica

Las NTIE establecen que la memoria técnica de un proyecto eléctrico deberá incluir lo siguiente:

- Diagrama unifilar incluyendo la acometida, subestación, alimentadores hasta los centros de carga indicando su longitud en cada caso y caída de tensión, circuitos derivados indicando tipo, capacidad interruptiva y rango de ajuste de cada una de las protecciones de los alimentadores principales y derivados; calibre, tipo de material y aislamiento de los conductores activos y neutros de los alimentadores principales y derivados; tipo y dimensiones de la canalización empleada en todos los segmentos.
- Los datos que sirvieron de base para establecer el criterio de diseño y que fijará la manera de operar la instalación, tales como factor de demanda de cada alimentador principal y derivado, régimen de trabajo y tipo de servicio de los equipos instalados.
- Los cálculos para la adecuada selección de la capacidad interruptiva de las protecciones principales de la instalación.

- Los cálculos correspondientes al sistema de tierras, considerando las tensiones de paso, contacto y red, así como la selección del calibre y longitud del conductor de la malla.
- Cuadro de distribución de cargas de alumbrado y fuerza, incluyendo lo siguiente: número de circuito, número de lámparas, contactos o dispositivos eléctricos por cada circuito, fase a que va conectado el circuito, carga en watts y corriente en amperes de cada circuito, calibre de los conductores, diámetro de tubería y protección contra sobre corriente por cada circuito, desbalanceo entre fases expresado en porcentaje.
- Localización de centros de control de equipo, tableros de fuerza, de alumbrado y contactos y de concentraciones de interruptores.
- Localización del punto de acometida, del interruptor general y del equipo principal incluyendo el tablero o tableros generales de distribución.
- Trayectoria horizontal y vertical (proyecto isométrico) de alimentadores y circuitos derivados, tanto de fuerza como de alumbrado, identificando cada circuito, e indicando su calibre y canalización, localización de contactos y unidades de alumbrado con sus controladores, identificando cargas con su circuito y tablero correspondiente.
- Listas de materiales y equipos que se utilizarán especificando su marca y número de registro en la Secretaría de Comercio y Fomento Industrial (SECOFI).

También deben incluirse planos detallados de la instalación en los que se especifique lo siguiente:

- *Conductores*: Indicar calibre, tipo de material, clase de aislamiento y tensión en volts, mencionar si es cable o es alambre, así como el tipo y material de sus cubiertas y si cuenta con pantallas semiconductoras.
- *Canalizaciones:* Si es tubo conduit indicar el tipo de material, espesor de la pared, recubrimiento, diámetro nominal y si es flexible o rígido. Si es ducto metálico con tapa indicar el área o sección transversal del ducto. En el caso de charolas anotar el

tipo de material y ancho de la charola además de dibujar detalle del acomodo de los cables en cada tramo.

- *Alumbrado y contactos*: Indicar el tipo de lámparas y portalámparas, tensión nominal; capacidad en watts, pérdidas en watts del balastro o reactor y si éste es parte integral del portalámparas o no, asimismo, especificar el tipo de cubierta del portalámpara. Indicar también, la capacidad en watts de los contactos, número de fases, especificar si está o no aterrizado, tensión nominal y tipo de cubierta.
- *Sistema de tierras*: La instalación referente al aterrizado del sistema eléctrico y la puesta a tierra de las partes metálicas no conductoras de corriente de los equipos, pueden presentarse en planos o memorias descriptivas, pero en cualquier caso contendrá las características de los electrodos, dimensiones, tipo de material y longitud enterrada; especificará las características del puente de unión que conecta el electrodo de entrada del servicio con los conductores de tierra, tanto del sistema como del equipo; se indicarán las características del conductor de tierra del sistema, señalando las características de los conectores empleados, incluyendo si son de tipo soldable o atornillable; se anotarán los criterios y cálculos, en su caso, que dieron base a la selección del sistema de tierra.

Para la instalación de los equipos de cómputo se requieren algunas características particulares del sistema de tierras, mismas que serán abordadas en la siguiente sección.

2.3.3. Sistema de tierras

El objeto de conectar a tierra un circuito eléctrico es limitar las sobretensiones debidas a descargas atmosféricas, a fenómenos transitorios en el propio circuito o a contactos accidentales con líneas de mayor tensión; así como limitar la tensión a tierra del circuito durante su operación normal. Una conexión sólida a tierra facilita también la operación de los dispositivos de protección contra sobrecorriente, en caso de fallas a tierra.

Las canalizaciones y cubiertas metálicas de conductores o equipos (ajenos al circuito eléctrico) son puestas a tierra con el objeto de evitar que éstas tengan un potencial mayor que el de tierra en un momento dado y representen riesgos para las personas.

La puesta a tierra de sistemas, circuitos, equipos, canalizaciones y cubiertas metálicas de cables, debe ser permanente y continua; los elementos que la constituyen deben tener una capacidad suficiente para conducir cualquiera de las corrientes que puedan ser impuestas y ser de impedancia suficientemente baja, tanto para limitar el potencial sobre tierra, como para facilitar el funcionamiento de los dispositivos de protección contra sobrecorriente del circuito.

Las partes que constituyen a un sistema de tierra son:

- *Electrodo*: Es el elemento que propiamente hace contacto con la tierra y puede ser un tubo, una barra o una placa enterrados debiendo llenar los requisitos siguientes:
- Los electrodos de placa deben tener por lo menos 2000 cm^2 de superficie en contacto con la tierra, sin que el espesor sea menor a 6 milímetros.
- Los electrodos de tubo deben tener por lo menos 19 milímetros de diámetro exterior y, si son de fierro o acero, deben estar galvanizados.
- Los electrodos de barra deben tener por lo menos 1.6 centímetros de diámetro (2.0 cm^2 de sección transversal).
- Los *electrodos* de tubo o barra mencionados deben tener una longitud de al menos 2.40 metros y no deben tener revestimientos de baja conductividad como pintura, barniz, etc... Además, siempre que las condiciones del caso lo permitan, los electrodos deben enterrarse hasta sobrepasar el nivel de la humedad permanente. Cuando se encuentren lechos de roca, pueden enterrarse horizontalmente a la mayor profundidad que permita el mismo lecho de roca.
- *Conductor del electrodo de tierra:* Es el conductor que se utiliza para la conexión del electrodo de tierra con los demás elementos del sistema y los equipos que van a ser puestos a tierra, esta conexión debe hacerse con un solo conductor. En el caso general, este conductor se instala entre el mencionado electrodo y el puente de unión (que se definirá enseguida). El calibre de éste se determinará en base a los

requerimientos del sistema; sin embargo, las NTIE limitan a que no sea usado un conductor de calibre menor a 8 AWG, debiendo usar cable forrado con cubierta plástica anticorrosiva en instalarse en la canalización adecuada.

- *Puente de unión principal:* Es una barra o alambre grueso de cobre u otro material conductor similar que se utiliza para interconectar el conductor del electrodo de tierra con los conductores de puesta a tierra de los equipos instalados y, puede localizarse sobre o dentro de los gabinetes donde se ubican los tableros generales de distribución, debiendo fijarse a estos usando los accesorios adecuados.

Un elemento adicional de un buen sistema de tierra para equipo de cómputo, aunque no necesariamente indispensable, es la fabricación de lo que se llama un pozo de tierra y que no es otra cosa más que un preparado de elementos químicos que, por la acción de la humedad del suelo, se adhieren al electrodo incrementando considerablemente el área de contacto del electrodo con el terreno donde se encuentra instalado, lo cual permite la rápida disipación de voltaje inducido en caso de corto circuito.

En la figura 2.3 se muestran las proporciones de los elementos químicos utilizados y el esquema de fabricación del pozo.

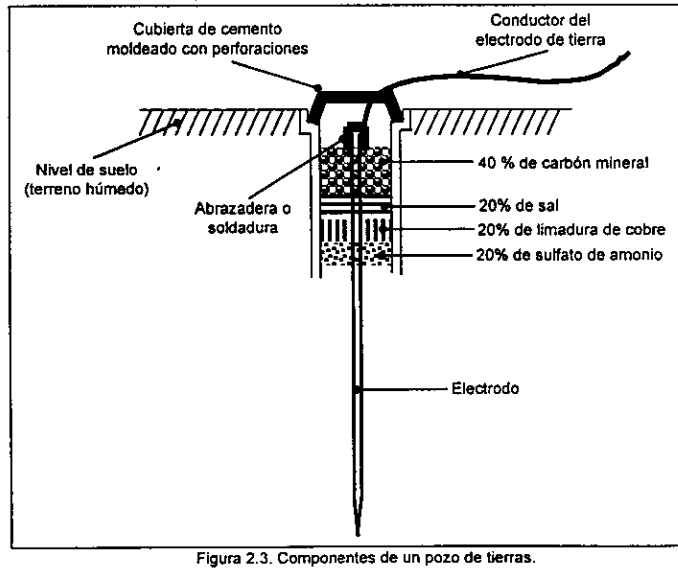


Figura 2.3. Componentes de un pozo de tierras.

Con esta figura se concluye la sección destinada a sistemas de tierra, que para fines de seguridad de las personas es una de las partes más importantes. Se abordará a continuación un apartado complementario dedicado a la iluminación de los centros de cómputo.

2.3.4. Iluminación en áreas de proceso

Las últimas tecnologías en la proyección y aprovechamiento de las fuentes de luz están consiguiendo unos rendimientos lumínicos sorprendentes, no sólo en la reflexión y control de todos los haces de luz, sino incluso en el reducido consumo y en el dominio del espectro luminoso para usos y fines concretos, siendo muy importante utilizar los artefactos necesarios para cada función específica.

Desde el punto de vista fisiológico, la legibilidad de un documento con un nivel de iluminación de 500 luxes no difiere mucho de la conseguida con otro de 1000 luxes. Estudios recientes han demostrado que la reducción en la frecuencia de fusión crítica, uno de los índices de fatiga visual, es mucho mayor en ambientes con niveles de iluminación de 1000 luxes, que en otros de 500 lux. Por estas razones, se estima que valores medios de 300 a 500 luxes, son los más adecuado como niveles de iluminación general en recintos donde se trabaje con pantallas de computadora.

De cualquier forma, es fundamental decidir el tipo de temperatura/color adecuado en cada caso. Una buena estrategia es combinar alumbrado fluorescente de iluminación general con puntos de alumbrado incandescente o halógeno para resaltar detalles informativos o de tráfico con lo que se valoran mejor los diferentes ámbitos y, sobre todo, se personalizan y resultan más atractivos visualmente. La iluminación para trabajar con terminales de computadora estará determinada por lo siguiente:

- Será principalmente natural con las pantallas dispuestas perpendicularmente a las ventanas, no apareciendo ninguna de éstas en el campo visual del operador. De ningún modo se colocarán pantallas a contra luz.

- La luz natural se tamizará con persianas, preferentemente de hojas verticales. Su color será distinto al de las paredes, pero no muy opuesto.
- La iluminación del local debe ser menos intensa que la de la pantalla y la de ésta, del mismo orden que la de la documentación que se utilice.
- Los valores de iluminación recomendados son de 300 a 500 luxes en la mesa del puesto de trabajo y entre 150 y 300 luxes en la pantalla. Esto no influye para que en algunos casos sean cómodos valores mayores de iluminación.

Para cumplir con todas las condiciones mencionadas, se ha comprobado que el tipo de iluminación que debe instalarse es el que está basado en luminarias fluorescentes en gabinetes estándares que alojan cuatro unidades de 40 watts cada uno. Estos gabinetes deben instalarse entre 1.5 y 2 metros de distancia entre ellos, con lo que se logran los requerimientos de luminosidad de entre 300 y 500 luxes a una altura de un metro. La alimentación debe tomarse del tablero general que cuenta con servicio de emergencia para que en caso de que se corte el suministra de energía eléctrica, el área de proceso no quede sin iluminación.

Como todas las instalaciones eléctricas, el sistema de alumbrado también requiere de un régimen de mantenimiento preventivo para detectar la posibilidad de ocurrencia de fallas. En el siguiente apartado se verán las recomendaciones que deben seguirse para el adecuado mantenimiento.

2.3.5. Mantenimiento a instalaciones eléctricas

En una sección anterior se mencionó que los componentes instalados deben proveer la confiabilidad en el suministro de energía eléctrica para los equipos de cómputo. Sin embargo, sin un adecuado programa de mantenimiento es muy probable que esta propiedad se deteriore causando problemas a la operación del centro de proceso.

Un buen programa debe incluir todas las partes analizadas de la instalación eléctrica; es decir, desde la acometida en la subestación hasta los circuitos derivados a los que se

conectan contactos, equipo o iluminación. Aquí se hacen las recomendaciones que deben seguirse para mantener en buen estado las instalaciones.

Acometida y subestación eléctrica

Generalmente esta parte se encuentra a cargo de una compañía externa especializada, que debe llevar a cabo una rutina anual de revisión y análisis que permita determinar el estado físico y operativo de los equipos de medición, barras de conexión, dispositivos de protección e interrupción, transformadores y tableros de baja tensión. A detalle, las partes que se revisan y el reporte que se emite incluye lo siguiente:

- Limpieza integral de gabinetes de alta y baja tensión, exterior de transformadores, trincheras, equipo de medición y en general el área de seguridad.
- Se verifica la existencia de elementos de seguridad, tales como: guantes para alta tensión, gafas antidestello, cascos de protección, cable de descarga, etc..
- Medición de valores de resistencia ohmica de puesta a tierra de todos los elementos no sometidos a tensiones eléctricas (gabinetes, canalizaciones, tanque de transformador, etc..)
- Ajuste de conexiones tanto en alta como en baja tensión.
- Revisión ocular del exterior de apartarrayos y medición de resistencia interna de los elementos.
- Limpieza y lubricación de interruptores y seccionadores de alta tensión.
- Medición de valores de resistencia de aislamiento de embobinados de los transformadores.
- Pruebas de rigidez dieléctrica y número de neutralización en muestras del aceite aislante del interior de los transformadores.
- Revisión de empaques de transformadores para localizar posibles fugas de aceite.

Tableros, canalizaciones y cableado

Debe hacerse una revisión semestral en la que se efectúen las siguientes actividades:

- Limpieza de gabinetes, charolas y/o trincheras.
- Reacomodo de cables, sustitución de interruptores dañados, apretar conexiones, etc...
- Revisar soportes de charolas y otras canalizaciones, sustituyendo o reparando posibles daños.
- Verificar fijación de contactos y sus correspondientes tapas.
- Cambiar secciones de conductor que presenten daños en aislante o indicios de haber estado sometidos calentamiento por corrientes de corto circuito.
- Verificar que no existan filtraciones de humedad en tableros y tuberías.
- Verificar valores de tierra física en tableros y contactos. Revisando también los electrodos y conductor del sistema de tierra.

Se debe estar plenamente consciente de que ni siquiera un excelente programa de mantenimiento garantiza que no ocurran problemas en una instalación eléctrica; sin embargo, se reduce la probabilidad de una falla hasta limites muy bajos en los que se puede convivir con éste y otros riesgos que también se verán reducidos por la vía de la implementación de otros dispositivos que mejoran la calidad de los recursos utilizados en el centro de cómputo. En la última parte de este capítulo se estudiarán los equipos que ayudan a que el centro de proceso opere con menor margen de incertidumbre.

2.4. Equipos auxiliares

Se define como equipo auxiliar aquel que sin ser equipo de cómputo, sirve de apoyo para el adecuado funcionamiento y protección de los recursos informáticos; es decir, son el último eslabón de la cadena de medidas de seguridad en el entorno de las amenazas físicas, ya que proporcionan un ambiente operativo perfectamente controlado, aislándolo de impurezas ambientales, fallas en el suministro de servicios, etc...; y protegiéndolo de eventos dañinos que pueden generarse de manera accidental o intencional. Se analizarán aquí los equipos y sistemas auxiliares que deben existir como instalaciones básicas para la operación de los equipos de proceso, sin descartar algunas otras opciones que proporcionan niveles más altos de protección aunque no

son comúnmente utilizados tal vez por su grado de sofisticación; los sistemas y equipos auxiliares que se considerarán aquí son los siguientes:

- Fuente de energía ininterrumpida (UPS, por sus siglas en inglés).
- Sistema generador de energía eléctrica (planta de emergencia).
- Sistema para aire acondicionado.
- Sistema de detección y supresión de incendios.
- Piso falso.

2.4.1. Fuente de energía ininterrumpida (UPS)

El primer equipo que se analizará en esta sección es el que proporciona las propiedades de regulación y continuidad a la instalación eléctrica del centro de cómputo, recordando que la característica de confiabilidad es inherente a la calidad de los componentes utilizados al construir la instalación eléctrica y a la calidad del trabajo realizado por los técnicos asignados a esta tarea. A este equipo se lo conoce genéricamente como UPS, que son las siglas derivadas de su nombre en inglés *Uninterruptible Power Supply* – Fuente o Sistema de Energía Ininterrumpida -. También se le conoce popularmente como "no-break", seguramente haciendo alusión a su función dentro de una instalación eléctrica, es decir, que es un equipo que no permite la interrupción o caída del suministro de energía hacia los dispositivos conectados en él. Existen varios tipos de UPS's, de los cuales el tipo *ON-LINE* es el que se considera adecuado para la conexión de equipo de cómputo, debido a dos de sus características exclusivas, mencionadas a continuación:

- *Tiempo de transferencia*.- Es el tiempo que tarda en activarse el suministro a través de las baterías ante la ausencia de la línea comercial. En el caso de los equipos tipo *ON-LINE*, este tiempo es igual a cero para evitar cualquier interrupción de energía eléctrica a los equipos críticos de procesamiento, en los cuales hasta un parpadeo de fracciones de segundo puede provocar la caída del sistema o de alguna aplicación que se encuentre activa.

- *Regulación.*- Es la característica que tienen de proporcionar una salida de voltaje constante independientemente de la calidad que se tenga en la entrada; por lo que, debido a que cuentan con transformadores de aislamiento a la entrada y a la salida, es casi imposible que alguna variación de voltaje en la acometida tenga repercusión en los equipos de proceso.

Con la ayuda del diagrama de la figura 2.4, es más fácil visualizar a que se refieren las características que se mencionaron antes. En esta figura se ve que el banco de baterías está siempre conectado al inversor, por lo que ante cualquier interrupción o cambio significativo de voltaje a la entrada, el inversor toma energía del banco de baterías y mantiene a salvo la carga; proporcionando en todo momento una salida de voltaje regulado.

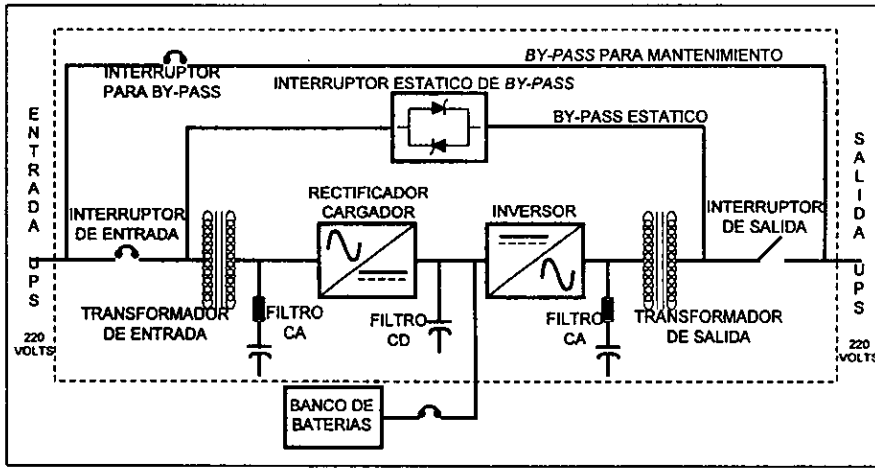


Figura 2.4. Diagrama de equipo UPS tipo ON-LINE.

Aunque el nombre de UPS indica que este equipo es una fuente de energía, en realidad es una fuente muy efímera, ya que toda la energía que puede proporcionar es la que se almacenó en el banco de baterías y no cuenta con un generador propiamente dicho, por lo que ante la ausencia de electricidad a la entrada del equipo, es limitado el tiempo que se puede mantener operando la carga conectada a él. Generalmente este tiempo depende del tamaño o capacidad del banco instalado y de la carga crítica conectada al

equipo, como se ve en la gráfica de la figura 2.5; donde parece atractiva la idea de adquirir un equipo de mucha capacidad para tener tiempos de respaldo muy altos, o instalar bancos de baterías muy grandes para lograr este mismo efecto. Sin embargo, tanto los equipos UPS como los bancos de baterías tienen un costo comercial muy alto, aunque siempre acorde con su uso e importancia de las cargas conectadas.

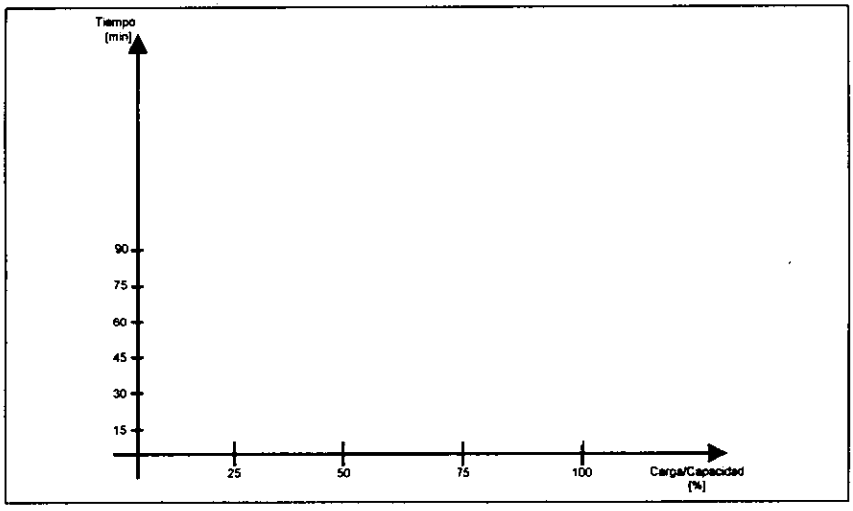


Figura 2.5. Gráfica Tiempo vs. Porcentaje de carga utilizado.

Con estas consideraciones es fácil entender que una UPS está diseñado para operar como fuente de energía en interrupciones de corta duración y para aislar perturbaciones comunes en las líneas comerciales, por lo que se recomienda calcular la capacidad del UPS considerando sólo el consumo de los equipos a conectar con un margen muy pequeño para crecimiento futuro y, para los períodos largos de interrupción de la acometida principal, utilizar otros dispositivos generadores de energía menos costosos (como las plantas generadoras con motor de combustión).

Los equipos UPS se fabrican en diferentes capacidades, adecuadas para distintas aplicaciones; y generalmente el diseño de un centro de cómputo debe adaptarse a las capacidades existentes en el mercado. El banco de baterías con el que cuentan de fábrica permite soportar la carga máxima durante un promedio de 10 a 15 minutos (ver

figura 2.5), que es tiempo suficiente para ejecutar rutinas de apagado en los equipos críticos, en el caso de considerar que el tiempo de interrupción de energía sea muy largo y no se tenga un equipo generador de energía alternativo.

Este equipo es, entonces, una inversión comparable con la inversión que se hace al adquirir equipo de proceso, por lo que es necesario protegerlo adecuadamente. Dependiendo de la capacidad requerida, los UPS de tecnología moderna tienen un tamaño tal que permite que sean instalados inclusive dentro del cuarto donde están los equipos de cómputo, con lo cual se encuentran ya protegidos contra daños físicos que pudieran ser causados por factores externos; el resto de la protección que requieren consiste principalmente en tomar alguna precauciones en su instalación y uso, con lo que prácticamente se asegura una operación con muy pocos riesgos.

Para la conexión de la UPS, en el centro de cómputo deben existir dos tableros de control de energía eléctrica perfectamente diferenciados, uno de ellos que se alimenta de la planta de emergencia y que es donde se conectan los circuitos de iluminación, contactos sin servicio de regulación y el UPS; y otro que se instala a la salida del UPS y alimenta contactos utilizados para conectar equipo de cómputo y periféricos que requieren de corriente regulada, tal como se muestra en la figura 2.6.

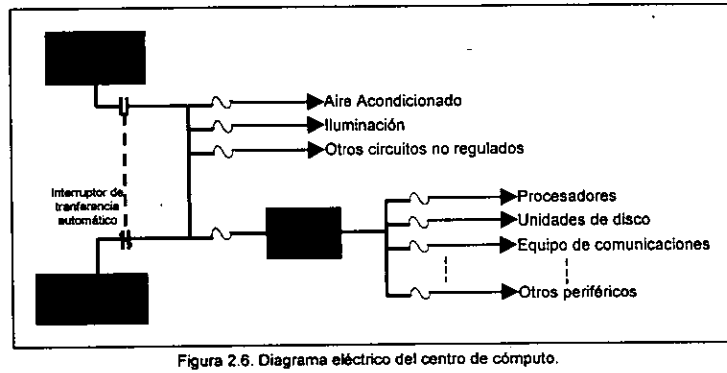


Figura 2.6. Diagrama eléctrico del centro de cómputo.

Como se puede apreciar deben habilitarse circuitos derivados independientes para cada equipo de proceso existente e instalar los contactos especiales necesarios, en caso de requerirse. Se debe cuidar, también, el balanceo de cargas, la selección de calibres

adecuados de cable, el tipo y dimensiones de tubería o canalizaciones adecuadas y , en general, deberá cumplir con los lineamientos de las NTIE; incluyendo, por supuesto, la elaboración de la memoria técnica correspondiente donde deberá anotarse, además de la información referida en la sección 2.3.2 de esta tesis, el porcentaje de utilización del equipo UPS y un plano con la ubicación de los contactos que cuentan con el servicio regulado.

Puede existir un tercer tablero de control en el que se conectará el equipo de aire acondicionado; sin embargo, éste deberá ser alimentado independientemente desde los tableros de baja tensión con servicio de emergencia ubicados en la subestación eléctrica del edificio.

Es importante mencionar que el UPS es un equipo electrónico y que la manera como genera su onda senoidal regulada a la salida es a partir de un método de integración digital llamado *Pulse Modulation Wide* (PMW –Modulación de Ancho de Pulso-), que permite lograr una excelente calidad en la forma de onda generada; sin embargo, no es una onda senoidal pura (como la que se obtiene en los generadores rotatorios), y por lo tanto es susceptible a sufrir alteraciones bajo ciertas condiciones que afortunadamente están bajo control del diseñador. Uno de los problemas que se pueden presentar es la presencia de distorsión armónica (alteraciones de la onda senoidal que provocan la presencia de armónicas menores en el espectro de frecuencias), provocados por la conexión de motores de inducción en los circuitos de salida del equipo; este tipo de problemas generalmente se presentas cuando el UPS está trabajando en el límite de su capacidad, es decir, muy cerca del 100 % y la corriente que se demanda en el arranque de los motores provoca pequeñas sobrecargas intermitentes que se reflejan en pequeña alteraciones de la señal de salida del UPS. Para prevenir este problema, generalmente se dimensiona la capacidad del UPS para que opere al 80 % de su capacidad como régimen de operación normal.

En un centro de cómputo se ha detectado que los equipos periféricos que llegan a causar este problema son algunos tipos de impresoras; por lo que se recomienda que, si por alguna razón se incrementa la carga al UPS, las impresoras sean conectadas en

contactos de servicio normal, ya que por lo general, la mayoría de las aplicaciones y sistemas detectan cuando se ha apagado la impresora y reinician sus procesos de impresión una vez que detectan nuevamente la presencia de este periférico.

Por último, en lo que se refiere a este tema, se listarán algunas recomendaciones de uso de los equipos UPS; algunas de estas recomendaciones se deben implementar como simples avisos de precaución en el centro de cómputo, pero algunas deben formalizarse incluyéndolas en la normatividad y/o políticas de la empresa para que sean observadas por todo el personal, estas recomendaciones son:

- Se deberán conectar al UPS todos los equipos de cómputo, de comunicaciones y periféricos existentes en el centro.
- No conectar aparatos electrodomésticos (cafeteras, enfriadores, ventiladores, etc.), en los contactos que cuentan con servicio de UPS.
- Los contactos que tienen servicio de UPS deben estar plenamente identificados, preferentemente deben ser de color rojo al igual que sus respectivas tapas, a diferencia de los contactos de uso normal que son de color ámbar.
- No instalar extensiones eléctricas ni conectar dispositivos multicontactos en los circuitos que cuentan con servicio de UPS. Cualquier requerimiento de contactos adicionales debe ser motivo de análisis especializado e instalación fija, cumpliendo con la normatividad existente (NTIE).
- El programa de mantenimiento preventivo debe ser similar al establecido para el resto de la instalación eléctrica.

2.4.2. Sistema generador de energía eléctrica (planta de emergencia)

El siguiente equipo que se analizará es el sistema generador de energía eléctrica que comúnmente se conoce como "planta de emergencia", debido a que la mayoría de las veces entra en operación de manera emergente cuando se presenta una falla en el suministro comercial. Es un equipo complementario que permite la continuidad en el servicio de energía eléctrica proporcionando autonomía por un tiempo mayor al que se puede tener con un UPS, de hecho puede llegar a operar continuamente durante largos

periodos de tiempo (meses, inclusive) permitiendo que la operación de un centro de cómputo no se detenga, aún en condiciones de desastre general en la zona geográfica en la que se localiza el inmueble.

Una planta de emergencia es un equipo electromecánico que se compone de tres parte fundamentales: un motor, un generador y una unidad de transferencia, que generalmente opera automáticamente. Además, casi siempre se requiere de un local especialmente diseñado para albergar estos equipos, debido a que aún hoy en día es un equipo que en conjunto genera mucho ruido y genera campos magnéticos de magnitud considerable; por lo que se debe instalar un tanto alejada del lugar en donde están instaladas las computadoras y los equipos de comunicaciones.

El tipo de motor que se usa generalmente, dependiendo de la capacidad de la planta en conjunto, es un motor de combustión interna que trabaja con combustible diesel. Este motor, que provee la energía mecánica que será convertida en energía eléctrica en el generador, está montado en una base de concreto o de metal provista de dispositivos especiales de anclaje que permiten absorber la vibración propia del motor. Debe estar instalado en un cuarto que permita, en una de sus paredes, montar una rejilla de ventilación para ubicar cerca de ésta el radiador por medio del cual se mantiene en su temperatura de operación al motor; además, se debe instalar el sistema de escape de los gases de combustión hacia un área perfectamente ventilada, preferentemente hacia el exterior en algún patio u otra zona abierta al medio ambiente por lo que el motor debe cumplir con las especificaciones de baja emisión de contaminantes para no transgredir las leyes ecológicas actuales.

El generador, que opera bajo el principio que dice que, "un conductor que se mueve dentro de un campo magnético genera en sus extremos una diferencia de potencial proporcional al campo magnético y a su posición relativa dentro del mismo"; será aquí tratado como una caja negra en la cual entra energía mecánica en forma de movimiento rotatorio a través de una flecha acoplada al motor y de la que sale energía eléctrica acondicionada para sustituir a la que se obtiene de la acometida comercial, es decir, trifásica y al voltaje nominal de operación. Por lo que no requiere mayores instalaciones

más que una ventilación adecuada para evitar calentamiento en sus componentes, y estar montado en la misma base que el motor, garantizando la alineación perfecta entre uno y otro para evitar esfuerzos mecánicos dañinos.

Por lo que respecta a la unidad de transferencia, es un dispositivo totalmente eléctrico que cumple también las funciones de control y monitoreo de los dos componentes mencionados antes, además de hacer el cambio entre la energía de la acometida comercial y la energía que proporciona el generador. Básicamente está formado por un par de interruptores con protección termomagnética que se alterna en su operación, es decir, cuando existe energía suministrada por la acometida comercial el interruptor que conecta ésta con la carga está cerrado y el otro está abierto. En el momento en que se presenta una interrupción en la acometida comercial y entra en funcionamiento la planta de emergencia se abre el interruptor que se encontraba cerrado y el interruptor que conecta la carga con la planta se cierra. Cuando se tiene una unidad de transferencia automática, entonces se verán en este gabinete, aparte de los mencionados interruptores, una gran cantidad de dispositivos electrónicos de control (temporizadores, relevadores, etc.) que se encargarán de sincronizar la operación de los interruptores.

Resulta natural que, siendo un sistema que basa su operación en la energía mecánica que proporciona un motor, éste deba estar listo para operar en cualquier momento; sin embargo, se requieren algunos segundos para que el sistema comience a generar energía útil; este tiempo es el que transcurre entre el arranque del motor (al detectar falla en el suministro comercial) y su estabilización a las revoluciones necesarias para la generación de la energía en sus condiciones nominales para, en ese momento, hacer el cambio en los interruptores de transferencia. A este tiempo se le llama "tiempo de transferencia de entrada", y generalmente es de entre 20 y 40 segundos, que de ninguna manera es tiempo suficiente para que el motor se caliente por lo que podría sufrir daños al ser revolucionado rápidamente, así que se prevé la instalación de precalentadores que hacen que el motor esté realmente listo en cualquier instante.

Existe otro parámetro de diseño que debe ser dimensionado cuidadosamente en un sistema generador de energía, es el "tiempo de transferencia de salida", es decir,

¿cuánto tiempo después de que se detecta el regreso de la acometida comercial, se hará la transferencia para trabajar con la energía normal?. Por el diseño del sistema, cuando la energía normal regresa se sincroniza de inmediato con las fases del generador y suministra energía a la carga; sin embargo, en previsión de que se presente otra caída en el suministro a los pocos minutos de haber regresado, la planta de emergencia se mantiene funcionando durante 5 minutos aproximadamente; en ese momento se desconecta de la carga y regresa a su estado de "espera". Este tiempo se ajusta a las necesidades del usuario y puede estar basado en datos estadísticos que reflejen el comportamiento del suministro comercial.

También es muy importante la selección de las cargas que serán conectadas al la planta de emergencia, ya que es poco probable que se cuente con un sistema que tenga capacidad suficiente para soportar a todo el edificio. Por lo que se recomienda que todos los circuitos correspondientes al centro de cómputo, los circuitos de operación básica del edificio, la totalidad del alumbrado del centro de cómputo y los circuitos de alumbrado que se requiere que se mantengan energizados, como mínimo, para la operación del edificio; así como los equipos para acondicionamiento de aire, tanto del centro de proceso, como los de todo el edificio, sean considerados como cargas críticas que deben conectarse a la planta de emergencia.

Este sistema es quizá el que requiere de mayor atención en lo que a mantenimiento preventivo se refiere, ya que por ser un equipo en su mayoría mecánico tiene muchas componentes susceptibles a desgaste físico que deben ser revisadas continuamente para prevenir cualquier falla que pueda impedir su funcionamiento en un momento crítico. Por esta razón, cuando se considera la adquisición de un sistema de suministro de energía de emergencia, es necesario considerar también la disponibilidad de recursos que permitan mantenerlo en buen estado. Una rutina de mantenimiento preventivo normal, incluye los siguientes puntos:

- Revisión de niveles de agua, aceite y combustible.
- Sujeción y limpieza de conectores de batería.
- Operación de precalentadores.

- Pruebas de arranque del motor.
- Pruebas de transferencia.
- Revisión de voltajes de salida del generador.
- Operación de instrumentos de medición.
- Limpieza general.
- Ajuste de inyectores (motores diesel).

Generalmente, estas rutinas se llevan a cabo mensualmente; sin embargo, algunas actividades dependen del régimen de operación que haya tenido el sistema, por lo que los períodos se ajustarán dependiendo de esto. Además, es muy útil instalar alguna herramienta de monitoreo de partes vitales del sistema para detectar oportunamente cualquier falla que requiera atención inmediata.

2.4.3. Sistema para aire acondicionado

En el concepto tradicional, un equipo para aire acondicionado permite mantener la temperatura de un espacio cerrado dentro de niveles preseleccionados para un fin definido. Sin embargo, dentro del ambiente de operación de un centro de cómputo, la temperatura no es el único factor que puede afectar la operación de los equipos de proceso cuando no se mantiene dentro de un rango aceptable para ellos. Los otros factores que se deben considerar para su control, además de la temperatura, son la humedad y la limpieza del aire; por lo que el sistema que se utilice para acondicionar el ambiente del centro de cómputo debe ser capaz de controlar estas variables. Así que, el equipo requerido para un centro de cómputo no es un equipo tradicional para aire acondicionado, sino un equipo especialmente diseñado para aplicaciones críticas que tenga estas tres funciones básicas: controlar la temperatura, compensar humedad y eliminar partículas de polvo.

Dependiendo de la capacidad requerida, existen en el mercado dos tipos de sistemas para el acondicionamiento ambiental de los centros de proceso: uno que es llamado tipo dividido (*split*) y que utiliza un solo ciclo a base de gas refrigerante (freón), y otro que

es llamado de dos ciclos, debido a que utiliza un ciclo a base de gas refrigerante (freón o amoniaco) en combinación con un ciclo de agua que es la que propiamente se usa para enfriar el aire que se inyecta al cuarto de computadoras.

El equipo de tipo dividido es el más utilizado, hoy en día, para aplicaciones de salas de proceso ya que prácticamente se elimina un riesgo muy conocido, los ductos para aire acondicionado que es por donde "tradicionalmente" se perpetran los accesos furtivos. Este tipo de equipos se llaman divididos porque el sistema completo consta de dos gabinetes en los que se instalan todos sus componentes: uno que es el módulo principal, que se instala dentro del centro de proceso, donde están incluidas la mayor parte de los componentes del sistema, desde el compresor hasta el panel de control; dejando el condensador para un módulo que se instala en el exterior (generalmente en el techo). La unión de estos dos módulos, para complementar el ciclo de refrigeración, se hace a través de dos tubos de cobre cuyo diámetro nunca es mayor a tres pulgadas; el otro orificio que se hace a la estructura del local es para un tubo que lleva la alimentación eléctrica del módulo exterior. En el módulo principal está instalado el difusor, que básicamente es un ventilador o turbina que toma el aire más caliente en la parte superior del módulo y lo hace circular a través del sistema de enfriamiento para después expulsarlo hacia la parte inferior del mismo equipo. En este mismo gabinete se encuentra el panel de control que permite preseleccionar los parámetros de operación requeridos, además de contener un procesador lógico que permite tomar lecturas de los sensores de temperatura y humedad para, en caso necesário, hacer operar el calentador o el deshumidificador o simplemente regular la cantidad de aire que será circulada dependiendo de la temperatura o humedad existentes en el local. En la figura 2.7 se muestra el esquema básico de operación de este sistema, destacándose la simplicidad de instalación y el hecho de que no se requiere un local adicional para instalar componentes del sistema, ya que el módulo exterior puede protegerse fácilmente instalando una rejilla metálica con soportes bien anclados a la estructura del inmueble.

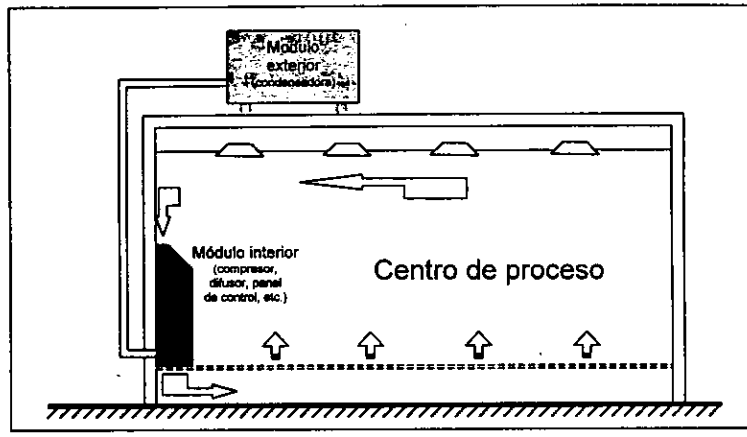


Figura 2.7. Diagrama de circulación de aire acondicionado con equipo tipo dividido.

La línea punteada en la figura indica el nivel de piso falso que, como se verá en una sección posterior, puede o no existir; aquí sólo se señala que uno de los usos del piso falso es el de distribuir el aire acondicionado en toda la sala y direccionarlo justo debajo de los equipos críticos y optimizar el aprovechamiento.

Es recomendable que en el diseño del local, el sistema para aire acondicionado sea sobredimensionado en un porcentaje adecuado y, además, se adquieran dos sistemas de la mitad de la capacidad requerida cada uno. Esto con el fin de prever la contingencia en que uno de los sistemas se dañe y tenga que quedar fuera de operación y el que otro sistema pueda soportar temporalmente la climatización de todo el local. En general, un equipo de tipo dividido se puede adquirir en el mercado en capacidades de 1 hasta 20 toneladas de refrigeración (T.R.), con las cuales se pueden cubrir las necesidades de centros de cómputo pequeños y medianos (espacios de hasta 800 m3, dimensiones aproximadas de 13x20x3 metros de ancho, largo y alto respectivamente), dejando como aplicación para los centros mayores los sistemas de doble ciclo; sin embargo, es más recomendable la instalación de varios equipos de tipo dividido para soportar una capacidad mayor, aunque esto depende de la disponibilidad de espacio dentro de la sala de proceso, por lo que la evaluación y la decisión debe ser tomada en particular para cada centro de proceso.

El otro tipo de sistema para aire acondicionado que se mencionó es el llamado de doble ciclo, debido a se utiliza un ciclo de agua para enfriar y, en caso necesario, humedecer el aire filtrado; y otro ciclo de gas refrigerante para enfriar el agua del ciclo anterior. Para instalar este tipo de sistemas se requiere un cuarto especial para ubicar los componentes electromecánicos y de control que son de gran tamaño, ya que se utilizan para capacidades superiores a las 50 T.R. Los componentes básicos de este tipo de sistemas son:

- Manejadora de aire: que inyecta aire frío y extrae, para reciclar, el aire caliente de la parte alta del cuarto de proceso.
- Bomba para agua fría: que hace circular el agua a través de un serpentín dentro de la manejadora de aire, para después depositarlo en una torre de enfriamiento.
- Bomba para agua helada: extrae agua de la torre de enfriamiento para hacerla circular dentro del sistema de enfriamiento por ciclo de gas refrigerante.
- Torre de enfriamiento: ventila el agua que circula en el sistema, además de hacer una fase de preenfriamiento antes de entrar al sistema de refrigeración. Aquí también se aplica tratamiento químico al agua para descontaminarla y evitar la corrosión de las tuberías.
- Sistema de refrigeración: es un equipo completo de refrigeración que baja la temperatura del agua que será utilizada en la manejadora para enfriar el aire.
- Tableros de alimentación y control: son los interruptores de energía para todos los equipos que componen el sistema; además, procesan las señales de los sensores de humedad y temperatura para aumentar y reducir la demanda de sistema en general.

En la figura 2.8 se ilustra un modo de operación de este tipo de sistemas, aunque no es la única manera de inyectar el aire hacia la sala de proceso, ya que para instalaciones mayores puede ser necesaria la distribución a través de ductos especiales para cada área. En cualquiera de los casos es necesario tomar precauciones para control de acceso al cuarto de máquinas, similares a los controles que se instalen para el acceso al centro de cómputo; ya que una vez dentro del cuarto de máquinas resulta un tanto

sencillo sabotear los ductos de inyección del aire acondicionado y penetrar a través de ellos.

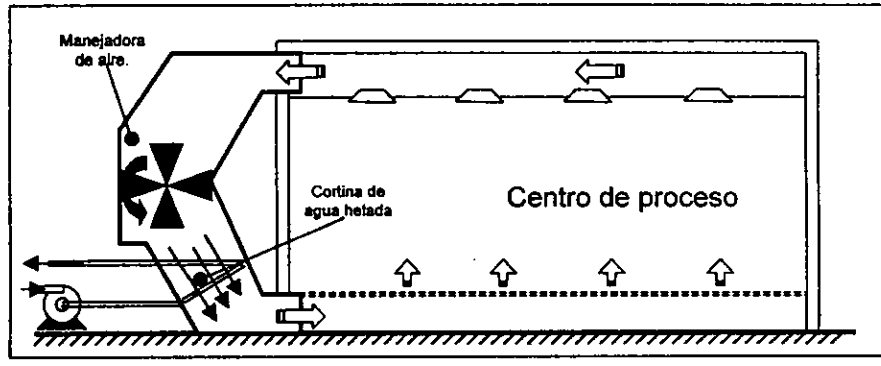


Figura 2.6. Diagrama básico de operación de un sistema de doble ciclo.

Por último, es necesario tomar algunas precauciones adicionales con respecto a la operación de los sistemas para aire acondicionado, ya sea de tipo dividido o de doble ciclo. La precaución más importante es la instalación de un mecanismo de interrupción de la operación del sistema ante la presencia de un incendio y la evidente operación del sistema de supresión del mismo, ya que en caso de que se detecte fuego y por consecuencia se active el sistema contra incendio, es posible que la acción del aire acondicionado sea contraproducente teniendo el efecto de avivar el fuego al filtrar el agente extintor y circular aire limpio hacia el interior del cuarto de proceso; por lo que un mecanismo de interrupción del sistema de aire acondicionado, que se dispare con las señales de alarma en el tablero del sistema contra incendio, es indispensable para la protección integral de los recursos informáticos. Otra elemento precautorio es la instalación de rejillas metálicas dentro de los ductos de inyección de aire para evitar la penetración por esta vía; además de la instalación de sensores de movimiento para detectar cualquier intento de acceso a través de los mencionados ductos.

2.4.4. Sistema de detección y supresión de incendios

El sistema de detección y supresión de incendios es llamado comúnmente "sistema contra incendios" y cumple con dos funciones básicas: detección y extinción de una de las amenazas más temibles debido a su capacidad destructiva, el fuego. Sus componentes mínimos se muestran en la figura 2.9.

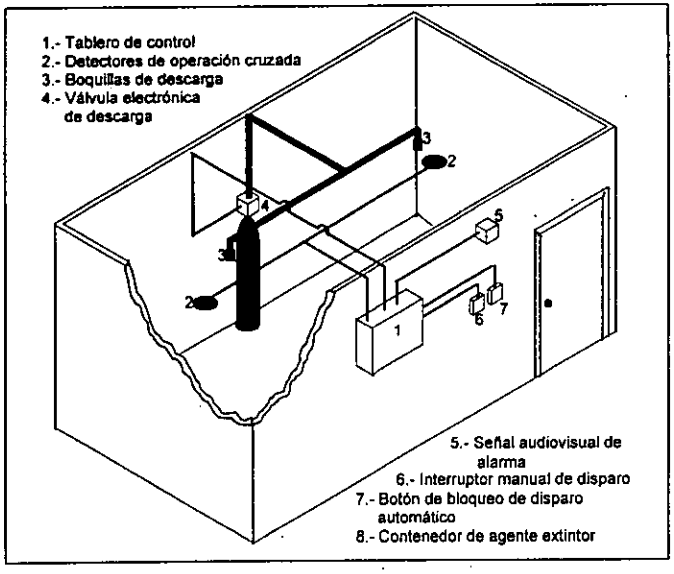


Figura 2.9. Componentes de un sistema de detección y supresión de incendios.

Aunque esta figura puede resultar bastante ilustrativa, resulta conveniente la descripción de cada uno de los componentes, así como su forma de operación típica.

- *Tablero de control*: Es un circuito electrónico diseñado para procesar señales provenientes de los detectores y, en caso de incendio, enviar aviso a través del dispositivo audiovisual de alarma; permitiendo cierto tiempo para que un operador verifique la existencia del fuego y que en caso de ser falsa alarma o ser un conato controlable con extintores manuales, se pueda abortar el disparo del agente extintor del sistema; en caso contrario el tablero debe continuar su secuencia y enviar la señal de descarga a la válvula del cilindro contenedor del agente extintor. Este

tablero también debe tener capacidad para enviar una señal electrónica al tablero de control del equipo para aire acondicionado e interrumpir su operación.

- *Detectores*: Son dispositivos electrónicos con sensores de calor y/o humo que indican al tablero de control la existencia de un incendio. Generalmente se instalan al menos dos detectores para permitir una operación cruzada, es decir, que si se activa un solo detector, el tablero de control emite una alarma sin iniciar la secuencia de disparo. Con esta forma de operar se eliminan un gran porcentaje de falsa activación por fallas de un detector.

- *Boquillas de descarga*: Es el medio a través del cual se descarga al ambiente el agente extintor y su diámetro, junto con el de la tubería de descarga, debe diseñarse para que el gas extintor se descargue casi instantáneamente (en menos de dos segundos).

- *Válvula de descarga*: Es un dispositivo electrónico que recibe una señal del tablero de control una vez que se ha completado la secuencia de disparo y/o se confirmó la existencia del incendio, accionando un mecanismo que rompe de un golpe el sello con el que cuenta el cilindro contenedor liberando rápidamente el contenido.

- *Señal audiovisual*: Es una combinación de luz estroboscópica con un sonido de alarma para dar aviso al personal acerca de la existencia del incendio. Se debe tener un procedimiento implementado para ser ejecutado al sonar la alarma, ya sea el desalojo inmediato o la verificación de la existencia del fuego.

- *Interruptor manual de disparo*: Es, normalmente, un botón que permite disparar el sistema sin que se complete el tiempo normal de secuencia; se usa cuando el incendio es evidente y no hay razón para continuar la secuencia normal, pudiendo evitar, tal vez, daños mayores.

- *Botón de bloqueo*: Es un interruptor que permite abortar la secuencia de disparo cuando se detecta que la alarma es falsa o que el incendio está en el nivel de conato y puede ser controlado con otros medios menos costosos.

- *Contenedor.* Es un cilindro metálico en el que se almacena el gas extintor. Debe ser capaz de soportar la presión de operación del gas y de almacenar la cantidad necesaria y suficiente para inundar todo el espacio del centro de cómputo.

Con esta descripción se tiene una idea bastante útil de la forma en que opera este sistema; sin embargo, falta conocer el elemento más importante, es decir, lo que hasta este momento se ha denominado "agente extintor". Existen en el mercado una gran cantidad de agentes extintores, que van desde agua hasta algunos gases inertes, pero solo unos cuantos pueden ser utilizados para su aplicación en centros de cómputo, debido a que deben cumplir con algunas características que lo hacen adecuados para este fin, estas características son:

- Su descarga no debe ser motivo de daños a los equipos de cómputo.
- Comprobada eficiencia en la extinción de fuego cualquiera que sea el origen de éste.
- No debe causar daños por exposición o inhalación a las personas.

Bajo estos requerimientos, el agente que parece estar hecho a la medida para su aplicación en centros de proceso es el Halón 1301; sin embargo, en años recientes las regulaciones ambientales han prohibido su uso y producción debido a que tiene un efecto dañino sobre la capa de ozono; debido a esto se hizo necesaria la búsqueda de un agente extintor que sustituyera al Halón, encontrándose en la familia de los CloruroFluorMetanos (HFC) un sustituto adecuado llamado comúnmente FM-200 y referido en las normas NFPA[2] como HFC-227ea, mencionándolo como el más efectivo sustituto del Halón, ya que aparte de cumplir con las características mencionadas arriba, no deteriora la capa de ozono.

Existen otras opciones que cumplen con los requerimientos para ser un agente extintor efectivo, pero la mayoría de ellos presentan algunos inconvenientes que de uno u otra manera impactan en el diseño del centro de cómputo. Por ejemplo, el uso de gases inertes tales como el "inergen" que tiene todo para ser una competencia considerable

[2] NFPA.- National Fire Protection Associates.- Asociación Nacional de Protección contra Fuego.

del FM-200; sin embargo, utiliza para su almacenamiento un espacio 9 veces mayor al que utiliza el FM-200 para lograr el mismo efecto extintor en el mismo espacio protegido. Otros agentes generan un ruido considerable al descargarse al ambiente, otros más requieren la instalación de boquillas de descarga especiales, lo cual hace que en las instalaciones en que ya existía un sistema de gas Halón se deba hacer una inversión mayor para cambiar la tubería ya instalada, cosa que no sucede al sustituirlo con el FM-200, ya que puede utilizarse la totalidad de las instalaciones existentes de gas Halón.

El principio de operación de cualquiera de los agentes aquí descritos se basa en la inundación total del espacio protegido en una concentración no mayor al 7% del volumen de aire existente (según normas NFPA); por lo que, a fin de no causar problemas a la salud del personal que labora en el cuarto de proceso, se debe hacer un cálculo particular para cada centro, tomando en consideración sus dimensiones particulares (incluyendo los espacios que están debajo del piso falso y sobre el falso plafón), la humedad relativa de operación, las divisiones internas (se debe incluir al menos una boquilla de descarga en cada espacio cerrado) y la altura sobre el nivel del mar. Naturalmente que en este análisis deben, también, considerarse la ubicación y cantidad de detectores y boquillas de descarga a utilizar en la instalación, para hacer eficiente la detección y supresión de incendios.

2.4.5. Piso falso

La utilización de piso falso en los centros de cómputo surge, históricamente, de la necesidad de formar una cámara plena que permita la inyección aire frío precisamente debajo de los equipos de proceso que, hasta hace algunos años, generaban mucho calor durante su operación normal y requerían que éste fuera disipado de una manera eficiente para evitar daños a los propios equipos y/o problemas operativos en general.

Una de las primeras ventajas que presenta la utilización del piso falso es la facilidad de instalación de cableado de alimentación eléctrica y de cableado de comunicaciones

entre equipos del mismo centro de cómputo, además de permitir la reubicación de equipos con adaptaciones mínimas a dichos cableados.

Sin embargo, también se presentan algunos problemas que se van reduciendo o eliminando por la vía de la normatividad y generación de estándares en la construcción e instalación de cada uno de los componentes físicos del piso falso. Estos problemas van desde la acumulación de polvo y basura debajo del piso hasta problemas más severos, como la formación de cargas estáticas en el piso debidas a la fricción de los zapatos, fricción de utensilios de limpieza, circulación del aire acondicionado, etc.

Por lo anterior, el piso falso que se instale en un centro de cómputo debe ser de tipo modular y cumplir con estrictos estándares de construcción en lo que a resistencia y propiedades de los materiales utilizados se refiere, además de contar con las siguientes características de instalación:

- Utilizar material 100% inoxidable, térmico, de baja resistencia eléctrica, anti-inflamable, que absorba el ruido y con cubierta resistente a la abrasión.
- Los módulos deben estar perfectamente ajustados y sellados.
- La estructura debe descansar en pedestales y estar aterrizada para evitar descargas estáticas.
- Debe existir un aislamiento entre las placas, amarres y ductos, para formar un plénum en el piso falso y techo.
- La altura mínima entre piso real y piso falso es de 0.20 metros si es de hasta de 400 m^2, y de 0.40 metros para instalaciones mayores.
- Debe estar topográficamente nivelado.
- Debe soportar el peso calculado de todos los equipos y sus aditamentos.

En la figura 2.10 se muestran las características principales de instalación del piso falso en un centro de cómputo; además, se muestra el detalle de construcción de un módulo de 60 x 60 cms., como los que se utilizan en la mayoría de las instalaciones y el detalle de armado de los soportes estructurales del piso falso.

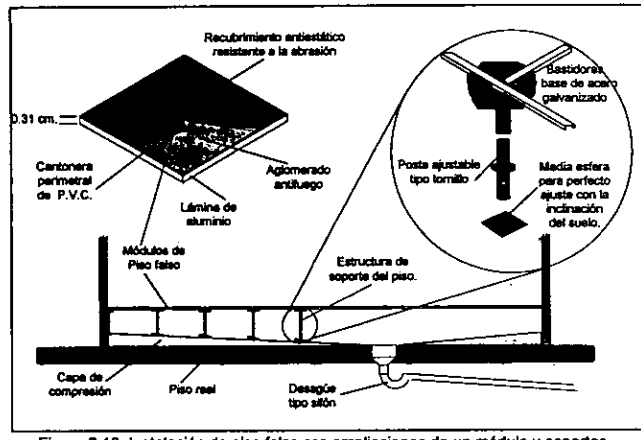


Figura 2.10. Instalación de piso falso con ampliaciones de un módulo y soportes.

Algunos inconvenientes que se presentan a menudo son: desnivel del piso, desprendimiento de losetas debido al uso, falsos contactos, cortos circuitos, formación de humedad, posibilidad de inundación sin detección oportuna, daños a cableados causados por roedores, etc. Por lo que se deberán implementar las siguientes precauciones:

- Se deben instalar detectores de humedad a nivel piso firme, además de detectores de fuego, de humo y, cuando el lugar así lo requiera, se deben instalar detectores de sismo.
- Se tendrán indicaciones visuales que permitan identificar dónde se encuentran los detectores de humo, de humedad, de sismos y de fuego en piso falso.
- Los detectores de humo deberán estar como mínimo a 1.5 m. y como máximo a 3 m. de la pared.
- Los detectores deberán instalarse en forma cruzada y como máximo a 5 m. entre sí.
- El plafón, paredes, tuberías y piso de los centros de cómputo, deberán estar pintados con pintura anti-polvo y anti-inflamable.
- El servicio de mantenimiento y limpieza a la cámara plena debe ser proporcionado por personal calificado y de manera periódica.

La mayoría de estos problemas y los riesgos que implican son eventos de tipo aleatorio y es probable que nunca se presenten, o no sean perceptibles a simple vista, por lo que es posible que se tenga conocimiento de ellos sólo a través de sus efectos (por ejemplo: se tienen reportes de errores en la comunicación de datos sin llegar a determinar exactamente cual es la causa, generalmente la causa es la presencia de electricidad estática en el recinto). Así que resulta de vital importancia la aplicación de los programas de mantenimiento preventivo y correctivo adecuados para mantener en optimas condiciones el piso falso y evitar riesgos tanto al personal como a los equipos de procesamiento, por lo que una rutina de supervisión periódica debe abarcar, al menos los siguientes puntos:

- Revisión y nivelación de soportes metálicos (cada 6 meses).
- Verificar continuidad eléctrica entre módulos y estructura de soporte (cada año).
- Revisar conductor y pozos de tierra física (bianual, incluir cambio de electrodos).
- Verificar estado físico de módulos y cambiar aquellos que presenten daños visibles.
- Aplicar pintura repelente al polvo en el piso real (cada 2 años).

Hoy en día, la mayoría de los equipos de proceso ya no requieren del direccionamiento del aire frío hacia su base para una eficiente disipación del calor producido; por lo que ya no es indispensable la instalación del piso falso, salvo por algún requerimiento específico de algún equipo en particular. Sin embargo, es necesario hacer énfasis en que la instalación del piso falso lleva consigo todas las actividades precautorias mencionadas arriba y, además, debe preverse en el diseño del sistema contra incendio, la instalación de boquillas de descarga tanto debajo del piso falso como por encima del falso plafón (en caso de existir), etc.

Con este análisis al piso falso que se instala en las salas informáticas se concluye el capítulo 2, en el que se dio un repaso a los principales aspectos relacionados con la seguridad física de un centro de cómputo. Desde los requerimientos constructivos del espacio que ha de destinarse al cuarto de proceso, hasta los elementos auxiliares que ayudan a prevenir los riesgos o amenazas que de manera tangible están presentes y pueden afectar los recursos dedicados a la operación del edificio informático.

En el siguiente capítulo se cambia un poco el panorama para entrar a otro aspecto importante de la seguridad integral de un centro de cómputo, ya se abordara un tema que se denomina "seguridad lógica"; en el cual se analizarán los riesgos que amenazan a los recursos intangibles, es decir, que si algún intruso logró penetrar las barreras físicas le sea todavía más difícil lograr el acceso a la información utilizable. Se estudiarán, también, la herramientas y controles que permitirán definir niveles de acceso y protección de la información para evitar que personas no autorizadas o con falta de conocimientos puedan destruirla, alterarla o simplemente extraerla para su provecho.

3

SEGURIDAD LÓGICA

En la seguridad de los sistemas de información, a un nivel de administración corporativo, se deben considerar los elementos que se ven afectados en este entorno; de esta manera, cada corporación tiene una responsabilidad consigo misma, con sus clientes y con la sociedad en general para tener un buen control de sus sistemas de información para que las operaciones internas cuenten con información exacta y oportuna, los datos personales acerca de empleados y clientes estén guardados en forma confidencial ya que gran parte de la posición competitiva de la corporación puede depender del adecuado control de la información que ésta tiene. En consecuencia, estos y otros factores implican que se deba contar con un plan de seguridad corporativo.

Es un hecho que hoy en día el crecimiento de las grandes corporaciones, empresas gubernamentales, secretarías de estado y, en general, cualquier entidad, pública o privada, requiere de la interacción de sus funcionarios con equipos computacionales, ya

sean estos monousuarios, multiusuarios e inclusive equipos personales que mediante periféricos de comunicación, como modems o bajo redes locales hacen acceso a diversos bancos de datos, aplicaciones de diversos tipos, etc.

Sin embargo, a medida que se automatizan estos ambientes, se corre un riesgo inminente de que la información almacenada en estos sistemas sea empleada por personas ajenas a ella para su beneficio propio al permitírseles conocer factores estratégicos de la alta gerencia, espionaje y venta de información a la competencia, uso de tiempo máquina y sus recursos sin autorización, destrucción de información por sabotaje o descontento del personal, etc.

Por las causas antes mencionadas, se ha hecho inminente la necesidad de contar con una metodología que permita administrar y proteger la información que reside en estos sistemas y en donde los factores que se estudiarán son:

- Controles de acceso.
- Criptografía.
- Clasificación de los datos.
- Seguridad en sistemas y computadoras.
- Seguridad en telecomunicaciones.
- Seguridad en programas de aplicación.

3.1. Control de accesos

Es el conjunto de mecanismos que permiten a los administradores de sistemas ejercer una dirección o impedir una influencia sobre el comportamiento, uso y contenido de un sistema. Este control es empleado para alcanzar los objetivos de seguridad del sistema, tales como la integridad y confidencialidad de los datos.

A continuación se mencionan algunos de los principales aspectos a considerar para una buena administración de controles de acceso:

- Propiedades, responsabilidades y controles.

- Autenticación de usuarios y administración de contraseñas.
- Administración del control de acceso.
- Software para control de acceso a equipos.

3.1.1. Propiedad y responsabilidad de los datos

La idea de propiedad de los datos es bastante simple y se refiere a la entidad de mayor nivel dentro de la organización que ha sido designada para ejercer los derechos y responsabilidades sobre los datos, siendo ésta una consideración básica para el control de accesos y control de cuentas. Actualmente se han establecido dos definiciones relacionadas a la propiedad de los datos, que son las siguientes:

- *Propietario de los datos*: Es la autoridad reglamentaria responsable para un tipo particular o categoría de información; o bien, es un individuo u organización responsable por los datos que maneja la corporación. Es también el individuo o grupo que tiene la responsabilidad de los datos y de especificar el manejo de ciertos procedimientos relacionados con la seguridad, tanto para los usuarios como para los custodios de estos datos.

- *Custodio de los datos*: Es el individuo o grupo a quien se le han confiado los datos para su procesamiento. El custodio de los datos tiene la responsabilidad de verificar que los datos del propietario estén íntegros y seguros.

Por lo que se refiere a la responsabilidad de los datos, ésta se define como la característica del control que asegura que las acciones de la entidad asignada pueden ser rastreadas; es decir, que el control permite que las actividades de individuos dentro de un sistema ACP[3] puedan ser auditables, para individuos quienes resultan ser responsables de sus propias acciones.

[3] ACP.- Access Control Package.- Paquete de Control de Acceso.

En el diseño de sistemas de seguridad, tanto en el diseño técnico como en el de procedimiento, existe una regla denominada del mínimo privilegio que es considerada muy básica, esta regla es un principio en el que a cada usuario se le otorga el conjunto de privilegios más restringido para el desempeño de tareas autorizadas.

3.1.2. Autenticación de usuarios y administración de contraseñas

La identificación de un usuario autorizado se hace a partir del significado de algún nombre o equivalente, reconocido por el sistema. Mientras que a la confirmación de que este usuario es realmente la persona a la que se le otorgó la autorización para accesar al sistema se le llama autenticación. La autenticación se hace a través de la definición de tres dimensiones estándar: algo que el usuario conoce (una contraseña o NIP[4]); algo que el usuario posee (una llave o una tarjeta de identificación); o algo que el usuario es (huella digital, reconocimiento facial). Por lo que, la autenticación puede ser definida como una identificación positiva de un individuo, con un grado de certeza suficiente para permitir ciertos derechos o privilegios dentro del sistema.

Autenticación basada en el conocimiento

El método más común de autenticación es el uso de algo que el usuario, y solamente él, conoce. Los ejemplos más comunes son las contraseñas y el número de identificación personal (NIP), relacionado con éstas. El principio es que sólo un usuario válido conoce la contraseña y NIP; por lo tanto, una contraseña y NIP correcto es una autenticación.

La falla principal de la autenticación basada en el conocimiento es la revelación del conocimiento porque el usuario "presta" su contraseña o bien; es común, que a la gente se le permita escoger su propia contraseña y muchas veces escoge contraseñas fáciles de adivinar o memorizar, contraseñas absurdas que después olvidan, anotan palabras o frases y después las pierden, etc. En resumen, para un sistema de seguridad, las contraseñas son un mecanismo muy débil de autenticación.

[4] Número de Identificación Personal

Autenticación basada en objetos

Una solución para el problema de administración de contraseñas es adicionar un segundo autenticador: un objeto de alguna clase. Éste puede ser una llave que desbloquee una terminal o computadora, una tarjeta que contenga información almacenada magnéticamente o de igual forma, una tarjeta inteligente o de identidad que forme parte del hardware mismo. De modo que, algo que uno posee es un autenticador.

El uso de tales objetos de autenticación mejoran la seguridad; pero, sin la ayuda de otros mecanismos es tan débil como la autenticación basada en conocimientos, ya que si el objeto se pierde (como en el caso de las contraseñas), puede ser usado por cualquiera que se apodere de él.

Autenticación basada en características

Una alternativa para evitar el problema de la divulgación de contraseñas o el extravío de objetos, es el uso de alguna características propia por el usuario válido que no pueda ser duplicada y utilizada para el acceso a sistemas.

El término general que involucra el uso de características del usuario para autenticación, es: autenticación biométrica; y puede ser definida como:

El uso de patrones específicos que reflejan las características únicas personales (tales como huellas, reconocimiento de voz o impresión de retina) para validar la identidad de los usuarios.

Un problema significativo en la autenticación biométrica es: que a pesar del uso de criterios lo bastante estrictos como para denegar el acceso a individuos que no coincidan con el patrón registrado, dejando entrar a aquellos que si están autorizados; aún no es posible que, por ejemplo, un dispositivo que identifique la voz del usuario permita el acceso en caso de malestares físicos (como resfriado o gripe); o bien, le es difícil o imposible distinguir entre estrés causado por falta de aliento (al llegar corriendo bajo una tormenta) y estrés causado por una situación de secuestro o bajo amenaza.

Problemas similares limitan el uso de dispositivos biométricos, tales como los que reconocen el patrón de tiempo de golpes en el teclado al accesar una contraseña.

Hay otros problemas relacionados con sistemas que usan biometría. Por ejemplo, para examinar el patrón de sangre en la retina, el ojo debe ser presionado contra el lector o escáner, pudiendo darse la transmisión de enfermedades que afectan a los ojos. Los métodos de biometría usados en autenticación incluyendo reconocimiento manual o computarizado son:

- Huellas.
- Impresión de retina (patrones de sangre en la parte trasera de cada ojo).
- Combinaciones de medidas de la mano tales como longitud de los dedos y ancho de las palmas (características geométricas).
- Patrones de voz.
- Patrones de tiempo de golpes en el teclado de una terminal.
- Fotografías.
- Reconocimiento facial.

Contraseñas

Las contraseñas son uno de los métodos más fáciles y efectivos de control de acceso (en situaciones no críticas). Al usuario se le asigna una identificación y se le asigna o crea una contraseña; de tal forma que, el sistema no permitirá la entrada para usar archivos o recursos protegidos, sin la correcta identificación y contraseña. Muchos sistemas multiusuarios tienen esta capacidad y con frecuencia no es usada o es usada incorrectamente.

Algunas reglas generales acerca de contraseñas, que permiten que éstas se vuelvan más seguras y sean una forma de autenticarse con el sistema, pero pueden ser un riesgo si no se aplican en su totalidad, son:

- No permitir repetidos intentos; es decir, desconectar después de algún número pequeño de intentos no exitosos.
- Registrar intentos de acceso no exitosos y desconexiones al sistema.

- Realizar revisiones a bitácoras de manera aleatoria.
- Nunca escribir una contraseña y cuenta juntas.
- Nunca pegar una contraseña en una terminal, en una agenda telefónica, en un escritorio, en una carpeta etiquetada "contraseñas" o en algún otro lugar obvio.
- Seleccionar contraseñas poco comunes (combinar datos numéricos y alfabéticos).
- No usar el número de empleado del usuario o nombres personales.
- Cambiar la contraseña frecuentemente.
- Las contraseñas deberán ser fáciles de recordar pero difíciles para adivinar.
- Nunca decirle a nadie tu contraseña o, cambiar ésta inmediatamente después que otro la use (si hay una necesidad válida para que alguien más la conozca).
- No permitir que otros vean cuando tu estás tecleando tu contraseña.
- El sistema no deberá desplegar la contraseña.
- Las contraseñas asignadas a los usuarios deben ser enviadas vía métodos de transmisión seguros.
- El archivo de contraseñas deberá estar encriptado.

Las contraseñas pueden ser escogidas en cualquier número de formas. En la actualidad, muchos sistemas permiten a los usuarios elegir su propia contraseña; por lo que, si éste es el caso, se debe instruirlos para que ésta sea poco común. Un método que produce en forma razonable buenas contraseñas y que son difíciles de adivinar es:

1. Escoger dos palabras o números que sean fáciles de recordar; por ejemplo: un nombre y una fecha (luis y 0198).

2. Combinarlas usando alguna regla, por ejemplo: alternar letras y números (l0u1i9s8, que resulta más difícil de adivinar que cualquiera de la dos por separado).

En principio, las contraseñas creadas por el sistema usando un generador de números aleatorios son más seguras; aunque, en la práctica, a la gente se le complica recordar este tipo de cosas y deciden mejor anotarlas. Lo mismo aplica para contraseñas largas, que aunque teóricamente son más seguras también es más difícil recordarlas.

Si el sistema genera una contraseña, ésta debe ser comunicada al usuario de alguna manera, siendo el canal de transmisión el que implica mayor riesgo; desde el descubrimiento debido a un error humano (correo perdido) hasta la intervención de las líneas de comunicación. Por lo que si se están usando sistemas generadores de contraseñas se debe poner especial atención en el procedimiento de entrega al usuario final.

Así que, para reducir el riesgo de intervención de líneas de comunicación, todas las contraseñas deben encriptarse una vez que están siendo introducidas por el usuario. Debiendo encriptarse, también, cualquier almacenamiento en tablas del sistema y antes de cualquier transmisión de datos. Aunque esto no siempre es posible, ya que se requiere de un proceso de encripción local que no está disponible en terminales tontas, por ejemplo. Idealmente, la encripción debe ser de un solo sentido y matemáticamente imposible lo contrario, así que las contraseñas de texto claro no puede ser obtenidas de una tabla de contraseñas encriptadas, aun con las herramientas mas sofisticadas.

La encripción es solamente una protección parcial porque, aunque la tabla de contraseñas puede estar encriptada, un intento de penetración puede darse usando versiones encriptadas de diccionarios ortográficos, listas de contraseñas comunes, etc. Así que cualquier conexión que involucre un canal de comunicaciones está sujeto a intervenciones (particularmente en redes); y por supuesto, cualquier información de autenticación en tal conexión, sea encriptada o no, puede ser copiada y usada para perpetrar un ataque a los sistemas.

3.1.3. Administración del control de accesos

En esta sección se analizará una lista de control, la cual cubre muchos de los asuntos relevantes en la administración del control de accesos. Dicha lista consiste básicamente de políticas, procedimientos e ideas de control relacionadas para la exitosa instalación y administración de sistemas de seguridad en controles de acceso (RACF, ACF-2,

VMSECURE, TOP SECRET)[5]. Estas ideas de control están descritas de manera genérica y significa que son aplicables para todos los sistemas del control de accesos. No obstante estas ideas de control pueden ser no aplicables para ambientes operativos específicos debido a características de disponibilidad o de implementación de los programas de control de accesos (ACP)[6], naturaleza del negocio que se está controlando, traslape con controles ya instalados, etc.

Dicha lista de control está dividida en 5 diferentes categorías y cada una presenta diferentes controles, los cuales conforman todas y cada una de las funciones de un ACP; las categorías mencionadas son:

1. Prerrequisitos para la implantación exitosa de un ACP.
2. Fuentes de entrenamiento para administradores y usuarios.
3. Revisión de bitácoras, monitoreo de eventos y preparación de reportes.
4. Administración de cuentas.
5. Consideraciones para el diseño de sistemas.

Una vez definidas las diferentes categorías de un ACP, a continuación se establecerán aquellos controles específicos para cada una.

Sección 1: Prerrequisitos para la implantación exitosa de un ACP

Aquí se establecen todos aquellos requisitos de ambiente para la exitosa instalación de un ACP.

1. Usar identificadores de usuario y contraseñas únicas para cada usuario (incluyendo administradores del ACP y en algunos casos, computadoras y procesos).
2. Establecer y forzar convenios de colección de datos estándar y nombre de recursos del sistema (facilita el uso de reglas de ACP).

[5] RACF,ACF-2,VMSECURE,TOP SECRET.- Paquetes de seguridad para control de acceso a equipos.
[6] Access Control Program.- Programa de Control de Acceso.

3. Documentar objetivos para la instalación de un ACP, incluyendo amenazas dirigidas.
4. Proporcionar un diseño del proyecto detallando, inclusive, estimados reales de recursos requeridos y un manejo aprobado del mismo.
5. Identificar a la(s) persona(s) especifica(s) responsable para el trabajo.
6. Asegurarse de preparar un sistema de categoría de riesgos y un plan en fases.
7. Listar los recursos que serán protegidos (terminales, transacciones, etc.)
8. Definir el objetivo del ambiente y cómo el ACP convivirá con otras medidas de seguridad.
9. Producir un cambio en las perspectivas de sistemas de seguridad apoyándose en los altos mandos y usuarios.
10. Establecer estándares de clasificación de datos sensitivos (y tal vez estándares de clasificación de datos críticos) e indicar como serán usados con el ACP.
11. Prohibir contraseñas que están siendo almacenadas como teclas de función en terminales o almacenadas en discos con programas de acceso automático.
12. Asumir que serán utilizadas tanto por accesos telefónicos como por cableado interno, incluso si actualmente sólo es empleado el cableado interno.
13. Anunciar las medidas de seguridad que proporciona el ACP y el hecho de que un servicio será liberado.
14. Restringir rigurosamente el uso de utilerías que puedan superar o engañar al ACP.
15. No hacer excepciones para cierto grupo de usuarios tales como personal de mantenimiento, vendedores o programadores de sistemas (o al menos hacerlo con gran restricción y bajo vigilancia).
16. Asegurarse que esté instalado, y trabajando eficientemente, un procedimiento de control para el cambio de programas de producción.
17. Mantener un enfoque global y no estancarse en detalles técnicos.
18. Asegurar que los propietarios de los datos, custodios y usuarios, están identificados y que son informados de su responsabilidad relacionada con el ACP.

Sección 2: Fuentes de entrenamiento para administradores y usuarios

Para que pueda llevarse sin problemas la administración y uso de un ACP, se debe de considerar la capacitación como una parte importante en el proceso de adquisición de un producto de software, debiendo definir dos grupos estratégicos de capacitación, que son:

Para Administradores:

1. Manuales.
2. Clases por parte del vendedor.
3. Probar el ACP, por medio de aplicaciones prototipo.
4. Grupos de usuarios.
5. Hojas informativas.
6. Asociaciones profesionales.
7. Consultores.
8. Instalar el sistema en modo preventivo solamente (sin estar bloqueando a alguien que accese un recurso) y monitoreando los resultados.

Para Usuarios:

1. Guías para el usuario (con definición de responsabilidades).
2. Clases impartidas por el administrador de seguridad.
3. Manuales en línea (no dejar al descubierto información).
4. Clases por medio de videos (duración de 10 minutos más o menos).
5. Fichas de referencia.
6. Secciones de seguridad en guías y manuales para el usuario.
7. Políticas, procedimientos, directrices del manual de seguridad y otros documentos.
8. No revelar firmas de acuerdos a empleados, cuando ellos se están contratando.
9. Acuerdos por parte del usuario especificando responsabilidades y procedimientos de seguridad.

Sección 3: Revisar bitácoras, monitorear eventos y preparar reportes.

Una parte importante del control es el hecho de contar con algún rastro o huella, en el caso de que la seguridad pretenda ser violada por cualquier intruso. Para esto se definen controles por monitoreo y revisión de actividades internas del ACP, así como la emisión de reportes de actividades. Los controles establecidos para estos casos son:

1. Revisar diariamente los reportes e investigar inmediatamente cualquier sospecha o evento significativo relevante de seguridad.
2. Definir quienes revisarán los reportes del ACP; preparar individuos responsables específicos para tomar acciones sobre puntos significativos en estos reportes.
3. Definir claramente a usuarios que representen una amenaza de seguridad para el ACP y las faltas que existan.
4. Cuando sea posible, usar resúmenes de actividades, en vez de tener que hacerlo a través de listados extensos.
5. Proteger bitácoras para que sean difíciles de modificarse o destruirse.
6. Realizar una copia de la bitácora de seguridad y subirla a un disco o copiarla a cinta.
7. Entre los datos que se deben registrar en las bitácoras están los siguientes: actividades exitosas, cambios en las reglas (cambios en identificadores de estado, en perfiles, etc.), intentos no exitosos, uso de capacidades de diagnóstico remoto, uso de herramientas de depuración de programas, rastreo total de ciertos identificadores o tipos de identificadores y entradas vía líneas de enlace.
8. Decidir cual reporte del ACP deberá ser guardado en forma confidencial.
9. Preparar una política con respecto al uso de bitácoras de ACP para actividades de control.

Sección 4: Administración de cuentas

El control de los usuarios en la administración de sistemas de información, es primordial para el asegurar la integridad y confidencialidad de la información, este control se basa en los siguiente:

1. Establecer una conexión rápida y automática con la aplicación del sistema de personal para, de esta forma, determinar cuando el personal termina y/o cambia de responsabilidades.
2. Proporcionar un mecanismo para que el personal administrativo notifique al ACP de la suspensión de un empleado y que a su vez se active una suspensión de la contraseña del mismo.
3. No saturar el sistema cuando se está instalando un ACP.
4. Establecer una jerarquía de personal para la administración de la seguridad e identificadores relacionados para accesar a privilegios y responsabilidades.
5. Automatizar los procesos de generación de reglas de acceso a los datos relacionados en el ACP.
6. Si es posible, juntar grupos de identificadores de usuario para que ciertas reglas puedan ser aplicadas globalmente.
7. El límite posible es, dejar que los propietarios de los datos, custodios y usuarios decidan que recursos del sistema deberán ser protegidos.
8. Cuando un identificador de usuario es cancelado o suspendido se debe asegurar que los datos involucrados no están eliminados pero que son manejados en forma apropiada.
9. Proporcionar las facilidades para que el administrador del ACP cancele un trabajo pendiente o una sesión.
10. Definir criterios de suspensión, tales como: número de intentos de acceso que excedan un cierto umbral, usuarios que no hayan cambiado su contraseña durante un determinado intervalo de tiempo, usuarios intentando accesar recursos no autorizados para él, cuentas inactivas, etc.
11. Evitar el sabotaje a las cuentas de los administradores desactivándolas en respuesta a cierto número de intentos incorrectos de entrada al sistema. Proporcionar opciones para alarmas y/o suspensión temporal de un identificador de usuario (por 15 minutos) mientras tal ataque está en progreso.
12. Proporcionar una cobertura técnica de respaldo las 24 horas.
13. Crear una base de datos ACP maestra que refleje privilegios en todas las máquinas controladas por un cierto ACP.

14. Asegurarse que todos los gerentes estén familiarizados y cumplan con los procedimientos.
15. La administración debe comunicar explícitamente a los programadores de sistemas que la instalación del ACP es de alta prioridad.
16. Establecer un procedimiento estándar para determinar como se atenderá el requerimiento de una contraseña por vía telefónica.
17. Establecer una política para verificar la autenticidad de una solicitud de cuenta.
18. Se deben proteger los procesos de producción, asegurándose de que cualquier operador no tenga los privilegios asignados para alterar procesos.
19. Los administradores del ACP no deben ser capaces de accesar a cualquier cuenta (excepto a la propia), aunque ellos pueden ser capaces de emitir nuevos identificadores de usuarios y sus contraseñas.
20. Instalar el ACP en un ambiente de pruebas, antes de que éste sea aplicado a un equipo de producción.
21. Si las circunstancias indican que la administración de la empresa no desea tener identificadores de usuario y contraseñas individuales, entonces pueden ser usados identificadores especiales de privilegios restringidos y compartidos en eventos, en los cuales la administración esté de acuerdo en tomar la responsabilidad por abusos cometidos.
22. Debe haber una lista de puntos a considerar para cuando un empleado deja de laborar en la empresa.
23. Debe ser adoptado un reglamento en el cual la combinación del identificador y contraseña del usuario es usado como la única base para verificar privilegios en todos los equipos.
24. Es necesario establecer un reglamento para el otorgamiento de un identificador de usuario y privilegios.
25. Debe existir un proceso rápido para otorgar identificadores de usuario bajo circunstancias especiales; dichos identificadores deberán ser temporales y expirar en un corto tiempo. Los usuarios deberán iniciar un requerimiento bajo el procedimiento acostumbrado.

26. Se debe proponer un grupo de identificadores temporales especiales para el uso de operadores, programadores de sistemas y desarrolladores de aplicaciones definiendo claramente los privilegios de estos identificadores.
27. Se deben establecer procedimientos especiales para eventos en los que el ACP esté fuera de servicio; estos procedimientos deben incluir restablecimiento de la base de datos, rutinas de recuperación, negar ciertos privilegios mientras el ACP no está disponible, etc.
28. Los empleados que se encargan de la administración del ACP deben ser parte del plan de recuperación de desastres.
29. Se debe establecer un reglamento especifico con respecto a la confidencialidad de los identificadores de usuarios.

Sección 5: Consideraciones para el diseño de sistemas

Una parte importante del sistema es todo aquello que convivirá con el ACP en un equipo; de ello dependerá, en buena parte, el buen funcionamiento y desempeño del software de seguridad. Los controles de esta última categoría son los siguientes :

1. Una contraseña que es nueva o restablecida por el administrador del sistema ACP, debe expirar en el primer uso que le de el usuario, forzando a éste para que introduzca una nueva contraseña.
2. Se deben establecer estándares de construcción de contraseñas.
3. Las contraseñas no deben ser desplegadas en forma legible.
4. Las contraseñas se deben almacenar siempre encriptadas, cuando una contraseña es proporcionada por el usuario se debe encriptar para entonces compararla con el valor en un archivo de contraseñas.
5. Aunque algunos ACP's no lo soportan, ciertos usuarios deben ser bloqueados al detectar cierto patrón de interacción con la máquina.
6. Pueden ser requeridas algunas modificaciones a utilerías del sistema y deben ser investigadas antes de la instalación de un ACP.

7. Cada usuario debe tener únicamente un identificador de usuario para todos lo sistemas a los cuales accesa.
8. Aunque todavía no estén muy estables, es necesario que estén bien dirigidos los procedimientos para consistencia y manejo seguro de accesos simples de usuarios a varios equipos.
9. Las políticas y procedimientos deben manejar consistentemente los datos en cualquier máquina que existente.
10. Instalar un esquema de acceso a la red, en donde el primer nivel verifique a cual computadora tendrá permitido conectarse el usuario y el segundo nivel verifique sus privilegios en un servidor al cual se ha conectado.
11. Para facilitar la administración, los identificadores de usuario deben ser los mismos a través de todas las máquinas, si se involucran los mismos usuarios.
12. Para manejar entradas concurrentes, un mensaje es enviado a todos lo usuarios indicando que un identificador de usuario se encuentra actualmente en uso; este mensaje debe ser también enviado al usuario quién ya estaba en sesión.
13. Se deben prohibir entradas concurrentes desde localidades separadas geográficamente.

3.1.4. Software para control de acceso a equipos

Una manera de implementar control de acceso en sistemas de computadoras es: usando software de control de acceso para este propósito, para lo cual, es importante considerar los siguientes puntos generales:

- A no ser que el sistema operativo sea inherentemente seguro, los sistemas de control de acceso no puede garantizar la seguridad.
- Todos los sistemas comerciales disponibles requieren modificaciones al software del sistema operativo durante su instalación.
- Los controles de acceso no mejoran la protección a la integridad de los datos.

La implicación de los dos primeros puntos es que: un sistema de control de accesos no mejorará la seguridad de un sistema operativo mal diseñado; y más bien, la reducirá por que la implantación, además de compleja, requiere de cambios que están sujetos a errores humanos. El tercer punto enfatiza que el control de acceso no es lo mismo que el control de la integridad de los datos, y que la integridad normalmente no tiene que ver con software de control de acceso. No obstante, los software de control de acceso se han vuelto populares desde que ofrecen en apariencia un mínimo de incremento en la seguridad, y desde que no requieren cambios masivos, tales como reemplazar el sistema operativo. En algunos casos, sistemas operativos nativos ofrecen poca capacidad de control de accesos, de esta manera, la apariencia de mejorar la seguridad algunas veces puede ser una realidad.

Los paquetes de software para control de acceso que a continuación se listan son los que actualmente están disponibles.

- ACF-2
- Omniguard
- RACF
- Top Secret
- VMSECURE

Todos estos paquetes de control de acceso funcionan alrededor de tres bases: entidades, demanda de accesos y recursos. Típicamente, las tablas mantienen la lista de entidades definidas, los tipos de acceso permitidos y los recursos que pueden ser accesados. Una entidad en este sentido puede ser un usuario, un dispositivo de entrada específico, un programa, un proceso en la computadora o cualquier otra cosa definida que pueda requerir recursos. Un recurso es una capacidad provista por la computadora o alguna entidad a la cual el acceso es deseado. Esto podría incluir capacidades de salida, colas de impresión, cualquier colección de datos, programas de utilería del sistema o cualquier cosa definida por el instalador de el software de seguridad. Un acceso podría ser un intento para leer desde o escribir hacia una colección de datos,

ejecutar un módulo de carga o cualquier otra acción típica de la operación de un programa. Por lo que un esquema simple debe definir tablas de:

- Usuarios
- Tipos de acceso .
- Recursos tales como colección de datos, módulos de carga, programas ejecutables, capacidades de entrada/salida (I/O).

Una implementación típica y simple de estas tablas haría que se tuviera otro conjunto de tablas que definan que tipos de acceso, a que recursos están disponibles y para que usuarios y cualquier contraseña u otros mecanismos de control que deban ser lo que otorguen al acceso. Estas tablas típicamente son almacenadas como una forma de colección de datos a disco. (VMSECURE usa las facilidades del sistema VM -*Virtual Machine*- y almacena cosas de una manera diferente, debido al concepto de máquina virtual del sistema operativo diseñado).

Todos los paquetes mencionados anteriormente tienen muchas herramientas para protección de las tablas y para recuperarse en el caso de problemas.

Cada uno de estos paquetes deben ser instalados de tal manera que los requerimientos de los recursos del sistema son canalizados por el sistema operativo antes que el sistema reconozca el requerimiento. Esto involucra "parches" o cambios a partes del sistema operativo. Algunos de estos paquetes pueden instalar estos parches automáticamente; algunos requieren intervención manual. Muchos también proveen la habilidad para definir salidas del usuario. Por ejemplo, la generación de contraseñas en forma aleatoria no es provista por todos los paquetes; sin embargo, todos los paquetes permiten una salida de usuario que puede enlazarse a un proveedor de contraseñas seleccionado de la organización. De manera similar, algunos paquetes dejan salidas de usuarios para imponer controles de personalización (generalmente más estrictos), además de los controles normales provistos por el software de control de acceso.

Fortalezas de los paquetes de software de control de acceso

Una de las fortalezas de los paquetes de software de control de acceso es la de proveer una relativa facilidad de uso para agregar, alterar, y borrar usuarios y recursos. Esto se puede hacer definiendo grupos de usuarios o en algunas otras formas. Se pueden aplicar cambios a las capacidades de muchos usuarios afectando grupos con comandos simples. Algunos de los paquetes permiten el uso de tarjetas de caracteres extravagantes, para que un comando simple pueda afectar, por ejemplo, a todos los usuarios cuyos identificadores contengan los caracteres "AC". Así, la carga administrativa de manejar un sistema con miles de usuarios y guardar el estado actual de la seguridad se ve disminuido significativamente.

Otra capacidad valuable de estos paquetes es la generación de reportes. Cada paquete provee habilidades para definir reportes usuales además de ser capaz de proveer gran cantidad de reportes estándar. Usando estos reportes, el administrador de la seguridad puede determinar el estado de usuarios, requerimientos, peticiones no usuales que pueden representar intentos de penetración, etc. Algunos de los paquetes tienen la capacidad de reportar en tiempo real, para que un intento de penetración pueda ser detectado al momento en que suceda.

Recomendaciones

Aunque todos estos paquetes de software de control de acceso están sujetos al principio básico de que no se puede asegurar un sistema inseguro por el simple hecho de adicionar controles de acceso; se tienen preocupaciones más pragmáticas que normalmente limitan la efectividad de proveer seguridad. Estas son básicamente cuestiones de organización y procedimiento y deben ser dirigidas como un problema de administración en lugar de un problema técnico.

Típicamente, cada sistema debe ser instalado, al principio, en un modo básico y después de adquirir alguna experiencia y efectuar algunas pruebas se deben instalar herramientas más poderosas para que sean implementadas apropiadamente. Es común observar sistemas donde los errores que se depuraron durante la fase de pruebas son

encontrados, nuevamente, durante la supuesta fase operacional más segura debido a que, a menudo, los privilegios son asignados en base a la posición organizacional en lugar de aplicar el principio del mínimo privilegio.

Software de red

Existen pocos paquetes de software de control de acceso para minicomputadoras, debido, tal vez, a que el uso típico de estos equipos se limita a ambientes donde la seguridad no es una preocupación mayor (tales como ambientes académicos). Estos paquetes se incluyeron en los sistemas operativos de minicomputadoras después que los sistemas *mainframe* habían ilustrado la necesidad de la seguridad y, así, las minicomputadoras proporcionaron buenos niveles de control de acceso como parte del sistema operativo básico.

Tampoco para las microcomputadoras existen paquetes de control de acceso; debido, principalmente, a que por naturaleza no son seguras ya que fueron diseñadas como máquinas de un solo usuario y el control de acceso no fue un considerado como parte de las fortalezas del diseño. Sólo cuando las microcomputadoras están en un ambiente que permite que varias personas compartan la misma máquina, entonces, el control de acceso llega a ser un punto de discusión. En este caso, algunos métodos de encripción pueden ofrecer alguna mejora a este problema; pero las microcomputadoras *stand-alone* son y serán ambientes de cómputo no seguros.

Cuando las micromputadoras están enlazadas dentro de redes, el problema de la seguridad empieza a parecerse al de aquellos *mainframes*. Para estos casos, el software de red ha incorporado capacidades de seguridad, que, típicamente, se implementan a lo largo de las mismas líneas como uno de los paquetes de software de control de acceso resumidos anteriormente. Algunos ejemplos incluyen *Novell Netware* y *Banyan Vines*.

3.2. Criptografía

La criptografía puede ser descrita como el uso de códigos secretos para proteger la integridad y confidencialidad de los datos. El estudio de este tema incluye lo siguiente:

- Usuarios
- Factores que afectan fortalezas relativas, por ejemplo:
    - Complejidad
    - Secreto
    - Características de la llave (por ejemplo, simetría, longitud, porcentaje de llaves débiles, facilidad de generación o selección de llave, etc.)
    - Otros
- Implementaciones (por ejemplo, DES, RSA, CCEP).
- Aplicaciones (por ejemplo, autenticación de mensajes, firmas digitales, correo digital, FIME (X9.9), STU).
- Manejo y administración (por ejemplo, distribución de llaves).
- Detección de errores y corrección de características de métodos de encripción.

3.2.1. Definiciones y características

Primero se definirá la encripción como el resultado de usar un algoritmo y una llave para cambiar texto claro, o la información normalmente comprensible, en texto cifrado; el cual no es leíble sin la aplicación de un algoritmo inverso y una llave, siendo esto último lo que se llamará desencripción. La herramienta de encripción puede ser cualquier cosa desde un lápiz y papel, software para computadora y/o circuitos integrados, dispositivos de propósito especial (uno de los más famosos es el dispositivo "enigma", usado por los alemanes en la segunda guerra mundial e interceptado por los aliados).

Históricamente, cualquier información que la gente ha tenido para enviar a alguien más a través de canales de comunicación que no son seguros han sido encriptados en algunos modos antes de su transmisión. Esta información podría ser cualquier cosa,

desde datos financieros o de crédito hasta información privada, personal o comunicaciones militares. La encripción ha llegado a justificar su costo porque proporciona una forma de verificar que la transmisión de los datos sea segura, salvando el obstáculo de la inherente vulnerabilidad de los canales públicos de comunicación de datos, particularmente microondas y transmisiones vía satélite;

Para entender más acerca de los términos y/o conceptos más usados para el conocimiento y aplicación de la encripción, revisar el apéndice A.

Características Generales de un Sistema Criptográfico

Actualmente todos los sistemas criptográficos deben de cumplir con tres requisitos para ser aceptados en el uso general de los sistemas de información automatizados:

1. Los algoritmos para encripción y desencripción deben ser eficientes para todas las llaves.
2. El sistema debe de ser fácil de usar.
3. La seguridad del sistema deberá depender solamente del secreto de las llaves y no del secreto de las transformaciones para encripción y desencripción.

Además de estas características generales, existen dos conjuntos de requerimientos que se deben de cumplir: confidencialidad y autenticidad (de los datos). La parte de la confidencialidad tiene ciertos requerimientos bien definidos en términos de factibilidad en computación, estos requerimientos son los siguientes:

1. No debe ser computacionalmente factible que sistemáticamente se pueda determinar el algoritmo de desencripción a partir de algún texto encriptado que se haya interceptado, aunque se descifre el texto original.
2. No debe ser computacionalmente factible determinar sistemáticamente un texto original a partir de texto encriptado que haya sido interceptado.

El efecto de estos dos requerimientos es que, sin la(s) llave(s), una persona no puede descifrar mensaje encriptados. Y, aun más, si un mensaje es descifrado, el trabajo

necesario para descifrar otro mensaje deberá ser el mismo, debido a que el algoritmo de desencripción no se conoce.

En el mismo orden, para que un sistema de criptografía sea aceptado para uso general, debe ser imposible, para un analizador de encripción, sustituir un texto cifrado falso por uno correcto sin ser descubierto. Esto lleva a dos requisitos de autenticidad más amplios :

1. No debe ser computacionalmente factible determinar sistemáticamente el algoritmo de encripción a partir de un texto encriptado dado, aún cuando el texto original se conoce.
2. No debe ser computacionalmente factible encontrar sistemáticamente un texto encriptado de tal manera que una eventual desencripción revele un mensaje de texto original que sea válido.

Como en el caso de la confidencialidad, estos dos requerimientos se deben cumplir, independientemente del número o longitud de los mensajes de texto cifrado interceptados.

De lo anteriormente expuesto, se tienen dos definiciones que son muy importantes, con respecto a los requerimientos de confidencialidad y autenticidad. Primero, la palabra "sistemáticamente" que es usada para conceder la posibilidad de que una suposición afortunada puede llevar a un caso en el que se vea afectada la seguridad, pero esto no deberá ser posible de hacer repetidamente, es decir, sistemáticamente. Y segundo, el término "computacionalmente factible" es un concepto matemático usado en la informática y que está basado en la teoría de los números; de tal forma que, llevándolo a la práctica, significa que se deberá hacer un gran esfuerzo, quizás de miles de años (aun utilizando supercomputadoras) para romper la codificación.

3.2.2. Llave pública y llave privada

Hoy en día son comunes dos sistemas básicos de encripción: de llave Pública y de llave privada. En un sistema de llave privada, la encripción y desencripción usan la misma llave y, obviamente, la llave debe ser guardada en forma secreta; ya que alguien con la llave puede encriptar y desencriptar los datos. En un sistema de llave pública se usan dos llaves, de las cuales una encripta y la otra desencripta; y, aunque las llaves están relacionadas matemáticamente, no pueden ser determinadas una a partir de la otra ni con el uso de métodos computacionales. Los términos "sistema simétrico" y "asimétrico" también son usados para indicar un sistema de llave privada o llave pública, respectivamente; por lo que, un sistema de llave privada que tiene una sola llave, usada tanto para encriptamiento y desencriptamiento, es un sistema simétrico; y, el uso de dos llaves separadas, una para encriptar y otra para desencriptar lo hace un sistema asimétrico.

De esta manera, alguien poseedor de la llave de encripción en un sistema de llave pública puede editar, encriptar y enviar mensajes a quienquiera pero únicamente el dueño de la llave de desencripción puede leerlos. Esto tiene la ventaja que solo una copia, o un número pequeño de copias, de la llave de desencripción (llave privada) necesita ser guardada de forma segura; por lo que cualquiera puede enviar datos encriptados usando la llave de encripción, (llave pública) pero solo un receptor con la posesión de la llave privada puede leer el mensaje.

Típicamente, un sistema de llave pública es matemáticamente complejo y los procesos de selección de llaves y encriptamiento consumen tiempo real; aun con la utilización de varios métodos matemáticos que facilitan el problema del cálculo. Por lo que se recomienda no usar técnicas de llaves públicas donde las llaves no cambian frecuentemente y la cantidad de datos a ser encriptados es pequeño y, usar para estos caso un sistema de llave privada que, parecen haber sido diseñados para ser procesados en la memoria de la computadora y pueden ser mucho más rápidos que los sistemas de llave pública.

Por último, pudiera resultar un poco superfluo hacer notar qué la selección de llaves de encripción es crítica, con relación al poder de los mensajes encriptados. Sin embargo, es un caso muy similar de selección de las contraseñas, ya que es difícil que las personas sean muy hábiles para seleccionar llaves poderosas. Entonces, el análisis efectuado anteriormente acerca de la selección de contraseñas aplica a lo que a llaves de encripción se refiere y los principios básicos de selección de contraseñas también se deben aplicar.

3.2.3. Administración de llaves

La administración de llaves se refiere al hardware, software y procedimientos asociados con generación, distribución y uso de llaves de encripción. Dados los algoritmos de encripción y desencripción que se ajustan a los requerimientos de facilidad de uso, seguridad y autenticación, el mayor problema de sistemas de criptografía esta centrado alrededor de las llaves. Si la seguridad del sistema de administración de llaves no es por lo menos tan avanzada como el la del resto del sistema de criptografía, entonces el sistema puede no ser confiable. En un sistema de llave pública, la llave pública por supuesto no necesita ser protegida. Sin embargo, en un sistema de llave pública y privada, por lo menos una llave se debe proteger.

Es claro que aquella aplicación que genera llaves debe estar sujeta a las más altas medidas de seguridad a través de varias combinaciones de encripción de llaves y operaciones dentro de la aplicación generadora, además de otras medidas que se aplican por procedimiento. Se puede reforzar la seguridad de la aplicación generadora de llaves por medio de implementaciones que usen hardware en lugar de software (más adelante se hablará del DES[7] y como se implementa un algoritmo en hardware).

[7] DES.-Data Encryption Standard (Estándar de Encripción de Datos).

La herramienta de generación de llaves puede diferir, dependiendo de si la aplicación es una protección individual de datos en un archivo, en un sitio seguro, en una red con transmisión de datos protegidos o una instalación de una mainframe. En el caso de un archivo, una llave es generada, y usada, teniendo una vida relativamente larga. Típicamente, esta llave queda como válida por el tiempo de vida del archivo de datos y se distribuye una vez por un destinatario propuesto.

Para mayor seguridad en una red o *mainframe* se debe de generar una llave por cada paquete de información que sale de un ambiente seguro y de algún modo se debe comunicar esta llave al destinatario.

Una vez usada, la llave no tiene ningún valor a futuro; ya que el tiempo de vida de esta pequeña llave puede ser muy corto, dependiendo de la frecuencia de comunicación de los datos en el ambiente, provocando con esto que muchas llaves deban ser generadas y distribuidas frecuentemente. Una alternativa que aminora la carga de trabajo y las exposiciones asociadas con muchas llaves es usar una llave por sesión. Esto quiere decir que se establece una llave para cada sesión de trabajo; ésta es usada a través de toda la sesión y se limita el problema de la distribución a una vez por sesión en lugar de una vez por paquete.

El siguiente paso en la administración de llaves es la distribución de éstas. En un ejemplo de una protección individual de archivos de datos, simplemente se almacena la llave por separado del sistema y se distribuye al destinatario por métodos diferentes al canal de distribución de texto original, dando esto una seguridad adecuada. Sin embargo, el uso de cadenas y bloques de texto encriptado puede fortalecer este proceso.

Este problema es más complejo para redes de computadoras o sistemas que involucren canales de comunicación combinados con altas frecuencias de generación y cambio de llaves. Generalmente se puede usar una jerarquía de llaves, donde es generada una llave maestra (que se debe cambiar por lo menos anualmente), ésta a su vez se almacena en una ROM o hardware similar que proporcione dicha facilidad; entonces, se

generan llaves submaestras usando la llave maestra, por orden de usuarios. El ciclo de vida de una llave sub-maestra debe ser determinado basado en las necesidades del ambiente específico, un mes es el tiempo común. Una vez que se genera, la llave sub-maestra estará siempre encriptada (usando la llave maestra). Un tercer nivel de jerarquía de llaves es la llave de sesión, la cual se utiliza únicamente durante una sesión en particular como se mencionó anteriormente, estando también encriptada una vez que se genera. Un cuarto nivel de jerarquía agregaría una llave por cada paquete de datos transmitido.

En tal esquema jerárquico, es común usar un método de llave pública para encriptar las llaves usadas en un aplicación de llaves privadas. Por ejemplo, el algoritmo RSA puede ser usado para encriptar llaves DES y las llaves DES usadas para encriptar datos actuales para su transmisión. Este método combina las ventajas de llaves públicas (más fuerte y mejor encriptamiento con distribución de llaves más simple) con los sistemas de llaves privadas (rapidez de uso); derivándose de esta unión un esquema en el que se requiere mayor esfuerzo para romper el sistema.

3.2.4. Nivel de enlace

Hay dos extremos básicos de encripción en una red de comunicaciones, enlace-por-enlace y fin-a-fin. Para ejemplificar dichos conceptos se definirán los nodos como una localidad (por ejemplo, una computadora, terminal, proceso terminal, un programa o un cambio de sistemas), donde entran los datos y son almacenados, encriptados, procesados, desencriptados o ruteados y salen los mismos u otros datos; y el enlace como cualquier línea de comunicación (por ejemplo, un portador público, un *bus* de datos o un disco removible) u otro método de transferencia de datos entre nodos.

En las figuras 3.1 y 3.2 se ilustran estos esquemas, donde un mensaje que pasa a lo largo de un canal es usado para simplificar los dibujos (en una aplicación, la siguiente parte de un mensaje completo podría pasar a lo largo de enlaces completamente diferentes y nodos para llegar al mismo destino). En las figuras, la M es el mensaje

original, la E es un algoritmo de encripción y la D es un algoritmo de desencripción. E(M) es un mensaje encriptado. $E_1, E_2, ..., E_n$ y $D_1, D_2, ..., D_n$ se refieren a los esquemas de encripción o desencripción empleados en nodos 1, 2, ..., n. Las partes de la red donde existen los mensajes en texto original son, por tanto, vulnerables y están sombreadas.

En una encripción de enlaces (como se muestra en la figura 3.1), el usuario necesita solamente conocer la(s) llave(s) necesarias para accesar el nodo más cercano. Cada nodo puede desencriptar, procesar, rutear, ser salida o por otra parte manipular y entonces encriptar los datos. Todos los datos en un enlace son encriptados, pero los datos pueden o no estar en texto plano dentro de un nodo. El usuario no tiene el control sobre éste y debe depender de la seguridad del nodo para la seguridad de los datos transmitidos.

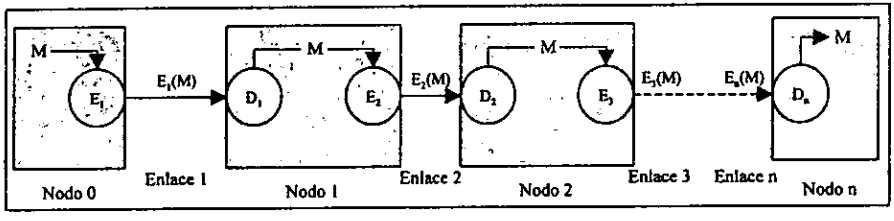


Figura 3.1 Encripción de enlaces.

En una encripción fin-a-fin, como se muestra en la figura 3.2, el usuario debe tener una llave de encripción por cada destinatario propuesto y cada par de comunicadores debe tener un método de intercambiar llaves y protocolos para transmisión. Los datos nunca están en texto plano excepto en el nodo originador y en el nodo que recibe al último. El usuario evita la mayoría de riesgos de interceptación durante la transmisión al costo de riesgos asociados con la administración de numerosas llaves y protocolos. También, desde los nodos y enlaces deben asignarse direcciones de algún modo ya que si se usa un analizador de tráfico se incrementa la probabilidad de tener éxito. Una vez más el usuario no tiene el control sobre de cómo las direcciones pueden ser asignadas o encriptadas por los enlaces o nodos.

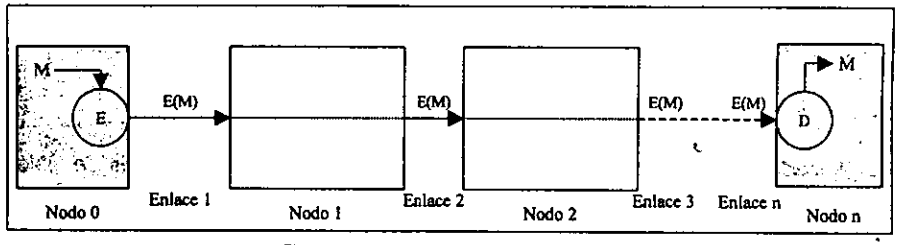


Figura 3.2 Encripción fin-a-fin.

Actualmente, en la práctica, alguna combinación de encripción de enlaces y fin-a-fin será encontrada en más enlaces de comunicación, con detalles que dependen de las necesidades de seguridad de los usuarios y de las características de los enlaces.

3.2.5. Modos básicos de encriptamiento

Actualmente existen dos modos básicos de encriptamiento, los cuales serán discutidos de manera muy clara; estos modos son: bloque de cifras y flujo de cifras.

Modo Bloque

En este modo, un mensaje es dividido en bloques sucesivos, básicamente de la misma longitud, para después encriptar cada bloque usando la misma llave (los bloques finales son ajustados a la misma longitud; esto asegura que en un ataque, los bloques se vean de un tamaño uniforme y no se puedan obtener datos útiles simplemente por observar la longitud del mensaje).

Los bloques pueden estar más expuestos a un analizador de criptografía que las propias cadenas de cifras debido a que un mismo bloque de texto plano generará el mismo texto cifrado con lo que se justifica un supuesto ataque basado en una ocurrencia esperada de cosas tales como espacios o palabras clave en un lenguaje de programación, con lo que se tiene una alta probabilidad de éxito de romper el encriptamiento. Sin embargo, los bloques pueden ser encriptados independientemente,

repitiéndolos y sustituyéndolos más fácilmente por lo que el encadenamiento de bloques es una estrategia que incrementa la dificultad de esta clase de ataques.

Encadenamiento de bloques

En un encadenamiento de bloques, los mensajes divididos y encriptados se colocan uno tras otro formando bloques más grandes con el fin de disminuir ataques que incluyen: inserciones, borrado y/o sustituciones. En este método, algunos de los bits del bloque previo de texto encriptado son insertados dentro de posiciones no usadas del bloque actual, con lo que se reduce, de manera sustancial, la vulnerabilidad, pero con el costo de la disminución de los bits para información que se tienen disponibles por cada bloque.

En una variante del encadenamiento de bloques, que se llama encadenamiento de bloques de cifras; se transmite un bloque entero de texto encriptado, que es considerado como un registro por ser exclusivo del siguiente bloque de texto original. A este resultado se le aplica el algoritmo de encripción usando la llave única, teniendo como efecto un flujo de cifras en forma asíncrona en el que cada bloque es dependiente en todos los bloques precedentes. De esta forma, el bloque final es usado como un control, exactamente como es considerada la última porción de un mensaje de texto encriptado en cifras asíncronas. De esta manera se evita la pérdida de bits utilizables en el encadenamiento de bloque, mientras estadísticamente se distribuye el contenido del mensaje de texto plano a través del texto encriptado entero.

Flujo de cifras

Un flujo de cifras rompe el mensaje en caracteres sucesivos o pequeñas unidades (bytes) y encripta cada carácter con un elemento de un flujo de llaves.

Un flujo de cifras asíncrono, es aquel en el que el flujo de llaves es generado independientemente del flujo de cifras. El flujo de llaves debe ser en verdad aleatorio y éste debe estar por lo menos tan largo como el mensaje (si el flujo de llaves es periódico, la conducta de la cifra considera un bloque de cifras para periodos cortos y de un flujo de cifras verdaderas para periodos largos). Si un carácter se pierde durante

la transmisión, el transmisor y receptor deben de resincronizar sus llaves generadoras para la eliminación del problema.

En un flujo de cifras asíncrono, cada elemento llave es derivado de algunos números fijos de caracteres precedentes del texto encriptado. Esto evita el problema de la resincronización después de un problema de transmisión, dado que la cifra se resincroniza por si misma después de recibir el número fijo de caracteres correctos de texto encriptado.

La última parte del flujo de un mensaje de cifras asíncrono depende del mensaje entero precedente, debido a que la llave y el texto encriptado resultante son dependientes por resultar de partes del mensaje mismo; esto significa que la porción final puede ser usada como un control para asegurar la transmisión completa del mensaje.

3.2.6. Analizadores criptográficos

Un analizador criptográfico se encarga de estudiar un sistema de encripción analizando sus entradas y/o sus salidas para obtener el texto original que contenga información confidencial y/o datos sensitivos. En esencia, un analizador criptográfico trata de romper el código de un texto encriptado que aparentemente no significa nada para obtener información provechosa.

Existe la duda de que si el concepto de "teóricamente seguro" tienen algún significado en criptografía, dados los recursos ilimitados de los analizadores criptográficos; lo que se sabe es que, el único código irrompible es uno que se obtiene usando un flujo de llaves aleatorias no repetidas, donde el número de llaves es igual o excede el número de mensajes posibles. Esto es conocido, también, como llaves de una sola vez.

Los analizadores criptográficos se basan, para su operación, en métodos numéricos y hacen uso del análisis estadístico para la generación de las llaves con las que intentarán romper la encripción; por lo que un sistema de encripción que se considera seguro es aquel que hace computacionalmente no factible la desencripción.

Existen algunas estrategias comunes de las que hacen uso los analizadores criptográficos, algunas de estas estrategias son:

- *Atacar solamente a texto encriptado.*- El analista tiene sólo el texto encriptado del cual desea determinar la llave.
- *Ataque a texto original conocido.*- El analista conoce algunas parejas de texto original y texto encriptado. Por ejemplo, si el texto encriptado representa un programa de computadora, puede esperar que palabras como begin, end, do, while, if , then, aparezcan con alguna frecuencia. Para ser más preciso, el analista sabría que la porción del texto encriptado se relaciona con un mensaje de clave de acceso si contiene los caracteres "LOGON".
- *Ataque a texto original seleccionado.*- El analista puede obtener texto encriptado que corresponde a un texto original seleccionado (éste es el caso más favorable para el analista). Una manera de obtener tales pares de texto original y texto encriptado es insertando elementos dentro de una base de datos y entonces observar los cambios en el texto encriptado almacenado.
- *Ataque a texto encriptado seleccionado.*- Con los sistemas de llaves públicas, el inverso del ataque a texto encriptado seleccionado llega a ser factible. El analista puede ser capaz de deducir la llave privada.

3.2.7. Características de detección y corrección de errores

Quizás la función de detección de error más básica de un esquema de encripción es aquella en la que uno puede descifrar un mensaje exitosamente sin que se tengan errores en el texto original. Sin embargo, otras características de detección de errores se pueden construir dentro de un algoritmo de encripción. Un ejemplo son los bits de paridad que son incluidos en el algoritmo de DES, donde los 64 bits usados para la llave incluyen 56 bits para la llave misma y 8 bits para indicar la paridad.

No es un propósito de este documento explorar los códigos de detección y corrección de errores; sin embargo, es importante mencionar que una característica de los

esquemas de encripción es la revisión de la paridad en el algoritmo de DES; además de que algunos incluyen la capacidad para usar el bloque final de un texto encriptado, o una porción de éste, como una forma de revisión para verificar la transmisión correcta y completa del texto encriptado.

3.2.8. Implementaciones: DES y RSA

DES, como estándar de encripción de datos, es el algoritmo más famoso de encripción por clave secreta o clave simétrica y fue desarrollado por IBM en la década de los 70's y adoptado por el gobierno de los Estados Unidos en Noviembre de 1976 después de un estudio dirigido a obtener un estándar de encripción oficial. Poco después, DES recibió el beneplácito de la Oficina Nacional de Estándares (*National Bureau of Standars*) y posteriormente del Instituto Nacional Americano de Estándares (*ANSI*).

DES emplea una llave de 56 bits y encripta los datos en fragmentos de 64 bits. Pero, ¿por qué una clave de 64 bits?. La verdadera historia está envuelta por el secreto del gobierno; sin embargo, algunos creen que la clave de 56 bits era lo suficientemente corta como para que la consolidada y tecnológicamente avanzada Agencia de Seguridad Nacional (*National Security Agency*, NSA) pudiera descifrarla si fuera necesario, pero lo suficientemente grande como para hacer el algoritmo DES impenetrable para cualquier otro.

DES recibe, como entrada a su procesamiento, bloques de datos de 64 bits que son sometidos a un total de 16 fases de transformación. Para cada fase, se tiene una clave (de fase) de 48 bits cuyo valor se obtiene a partir de la clave de 56 bits completa. Durante cada una de las fases, los 64 bits de datos y el valor de la clave de fase son introducidos a través de un conjunto de cajas conocidas como cajas <<S>> y una función separadora que desordena los bits. Además, antes, después y durante cada una de las fases, los 64 bits se permutan (el orden de los bits es alterado) de una manera específica. En cada uno de los pasos del proceso sólo se obtiene una única clave por fase a partir de la clave maestra de 56 bits. Al final, los 64 bits de la entrada original han sido convertidos en una salida de 64 bits, que parecen estar totalmente

alterados, pero que, sin embargo, pueden volver a transformarse en la entrada original utilizando el algoritmo de desencripción (consistente, básicamente, en ejecutar la encripción en orden inverso) y, por supuesto, la misma clave empleada para encriptar los datos en un primer momento. La figura 3.3 muestra el algoritmo de cifrado DES.

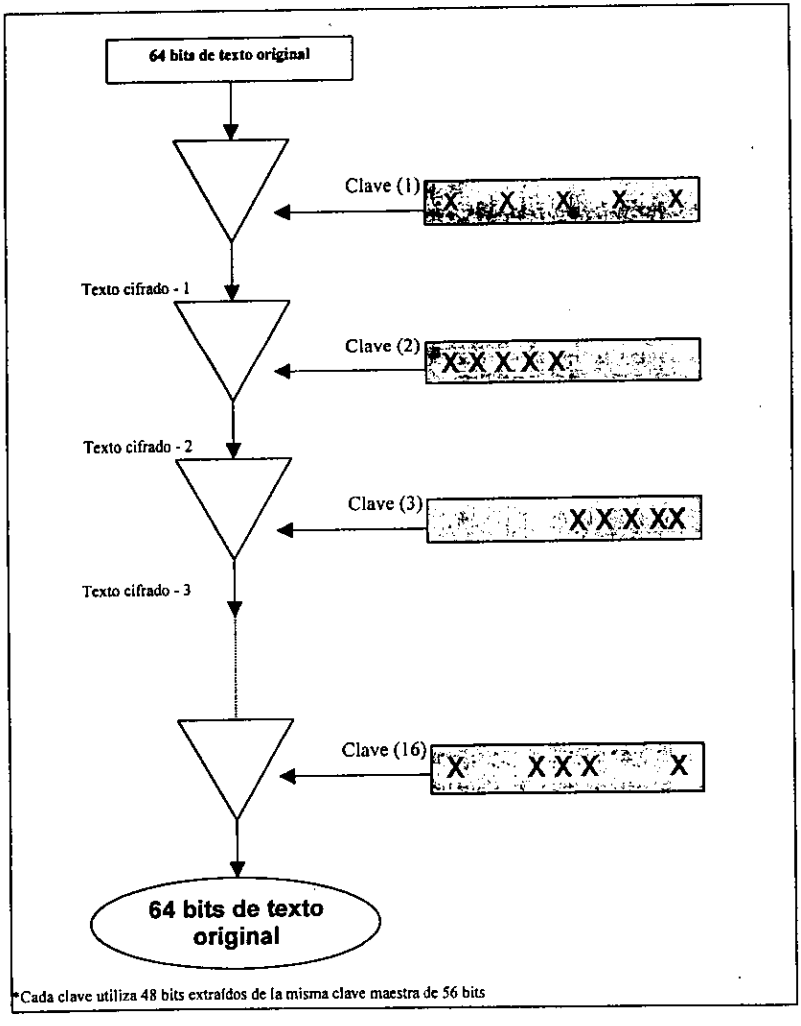


Figura 3.3 Proceso de cifrado DES.

Debido a las permutaciones antes, durante y después de cada fase, la ejecución de DES es mucho más lenta mediante software que mediante hardware. Para realizar una única permutación empleando software se requiere procesar un bucle 64 veces, situando cada uno de los 64 bits en el lugar correcto al mismo tiempo. Para realizar una permutación mediante hardware simplemente se usa un bloque con 64 terminales de entrada unidos directamente a 64 salidas, estando la permutación definida mediante la asociación entre conector de entrada y de salida. Los resultados pueden extraerse directamente de los conectores de salida.

Esto ha provocado que los posibles saboteadores del algoritmo DES se reduzcan a aquellos con los recursos suficientes como para construir un hardware de propósito general. Actualmente la mayoría de los piratas informáticos tendrían problemas para lograr reunir la tecnología necesaria para construir tal dispositivo.

Romper el DES

Las personas que implementan sistemas criptográficos deberían considerar el valor de la información protegida y durante cuánto tiempo la información debe mantenerse confidencial. En 1977, se estimó que costaría 20 millones de dólares construir una computadora de propósito especial con un hardware diseñado específicamente para de descifrar una clave DES en menos de doce horas simplemente mediante fuerza bruta, intentando cada posible clave, hasta encontrar la correcta. En el caso de que romper un encriptado conllevase tal nivel de esfuerzo, sería considerado un cifrado fuerte.

Sin embargo, las computadoras de hoy en día son más potentes de lo que eran las computadoras centrales en 1977 y, aun más, el costo de fabricar una computadora de propósito especial para quebrantar un algoritmo DES ha descendido a un costo estimado de algunos cientos de miles de dólares. Obviamente, no es deseo de nadie proteger mediante esta técnica las transferencias electrónicas interbancarias de billones de dólares.

Por otra parte, si el objetivo de la encripción es solamente proteger el acceso al servidor, y el posible penetrador se tiene que gastar cientos de miles de dólares para vulnerarlo; entonces, el encriptado bien puede describirse como suficiente.

El otro aspecto mencionado es el del periodo de conservación de la información confidencial. Supóngase que en la actualidad se encripta información que debe permanecer secreta durante diez años. Durante los últimos veinte años, las computadoras han duplicado su capacidad de procesamiento cada dos años aproximadamente. Actualmente, esta tendencia se está acelerando, y el ritmo al cual las computadoras incrementan su velocidad es, a su vez, cada vez más rápido. Como se ha visto, en el caso de utilizar DES de 1977, esto significaría que aunque hoy en día fuera imposible romper un código intentando todas las posibles claves mediante fuerza bruta; en el futuro, cuando las computadoras sean mucho más rápidas, podría ser factible.

Por cada bit adicional añadido a la longitud de la clave se dobla el número de valores que la clave puede tomar. Si la computadoras duplican su capacidad de procesamiento cada dos años o menos, siendo precavidos, por cada uno de los años que se desea que la información encriptada permanezca segura debería añadirse un bit a la longitud mínima de la clave.

Puesto que en la actualidad es posible fabricar una computadora específica para romper el DES por un par de cientos de miles de dólares, DES ya no se considera suficientemente seguro en los entornos en que se exige un encriptado fuerte.

Si en 1976 una clave de 56 bits era considerada suficiente, entonces nuestra proyección conservadora, veintidós años después, sugiere utilizar una longitud de clave de 76 bits o más. Si hoy en día es necesario un nivel de seguridad como el ofrecido por DES en 1976, ¿por qué no extender, simplemente, la longitud de DES o crear un nuevo algoritmo con claves más largas?.

El problema es que el camino está esparcido con esqueletos de técnicas de cifrado originalmente propuestas como seguras. Modificar el algoritmo DES es peligroso

porque si se intenta extender la longitud de la clave también debe cambiar la implementación del algoritmo y podría debilitarse la fortaleza criptográfica del mismo de manera sutil. Los investigadores han demostrado que pequeños cambios en el diseño del DES pueden comprometer seriamente la protección de la información cifrada respecto a algunos métodos sofisticados de ataque matemático. Nuevos algoritmos de cifrado, o cambios a implementaciones existentes, pueden no mostrar sus vulnerabilidades hasta dentro de algunos años.

Kerberos

Kerberos fue inventado para solventar los problemas de administración y distribución de claves secretas, en el que se tiene un grupo numeroso de usuarios pertenecientes a un único grupo o institución. La construcción de *Kerberos* se basa en el concepto de un centro de distribución de claves (KDC, *Key Distribution Center*) seguro y fiable. En lugar de tener que saber cientos de claves secretas, el usuario precisa conocer solo una clave secreta (la única empleada para comunicarse con el KDC). El siguiente ejemplo describe el funcionamiento de *Kerberos*.

Supóngase que el sujeto **X** quiere comunicarse de manera segura con el sujeto **Y**. **X** llama al KDC y dice: Hola KDC, soy **X**. Por favor, póngame en contacto con **Y**.

El KDC selecciona una clave de sesión aleatoria xxxxx para la conversación entre **X** y **Y**, y confecciona una tarjeta que **X** entregará posteriormente a **Y**. La tarjeta dice: "Hola **Y**, soy KDC, el sujeto que te entrega esta tarjeta es **X**; por favor, ¡utiliza esta clave de sesión xxxxx para hablar con él". Curiosamente esta es una tarjeta con una clave secreta que sólo **Y** y el KDC comparten. Esta tarjeta le denominaremos TARJETA_ENCRIPTADA_KDC_PARA_Y.

El mensaje que el KDC envía a **X** se encuentra encriptado con la clave secreta de **X** que sólo **X** y el KDC comparten. La tarjeta dice: "Hola **X**, soy KDC. Por favor utiliza la clave de sesión xxxxx para hablar con **Y**, tendrás que presentarte tu mismo entregándole esta tarjeta que yo te he dado TARJETA_ENCRIPTADA_KDC_PARA_Y.

X desencripta la respuesta procedente del KDC y recupera la clave de sesión xxxxx y la tarjeta para entregar a **Y**. **X** no puede añadir nada al principio o al final de la tarjeta, puesto que está cifrada con la clave secreta que únicamente **Y** y el KDC conocen.

A continuación **X** llama a **Y** y dice: Hola **Y**, soy **X**. El KDC me dio esta tarjeta para entregártela TARJETA_ENCRIPTADA_KDC_PARA_Y.

Y desencripta la tarjeta, sabiendo que sólo el KDC la puede haber fabricado utilizando la contraseña que ambos comparten, y recupera el nombre de **X** y la clave de sesión xxxxx. A partir de este momento, **X** y **Y** pueden comunicarse de manera segura entre ellos utilizando la clave de sesión xxxxx. Obsérvese que Kerberos ofrece identificación además de confidencialidad. **Y** sabe que **X** es quien dice ser porque únicamente el verdadero **X** sería capaz de desencriptar la clave de sesión compartida emitida por el KDC. De la misma manera, **X** sabe que **Y** es el verdadero **Y** porque sólo para el sujeto **Y** tendría sentido la tarjeta emitida por el KDC. La figura 3.4 ilustra el flujo de la información entre el KDC, **X** y **Y**.

Existen algunas artimañas adicionales para incrementar la seguridad, pero la ilustración proporciona la idea básica del funcionamiento de *Kerberos*. Por cierto el método criptográfico empleado en *Kerberos* es DES. El método de autoridad centralizada de *Kerberos* implica que es posible añadir fácilmente un nuevo usuario y, análogamente, si es necesario eliminar algún usuario, todo lo que hay que hacer es actualizar el centro de distribución de claves y, al momento, nadie será capaz de establecer nuevas conexiones con el usuario recién eliminado.

Pero, ¿qué hacer si se desea establecer conexiones aleatorias entre dos personas cualquiera del planeta? En el caso de organizaciones muy grandes, *Kerberos* puede gestionar el volumen mediante la replicación de KDC y dividiendo la organización en zonas; sin embargo, no está preparado para alcanzar tamaños como el de Internet. Además, no existe una autoridad central en Internet.

Esto da paso al tema más fascinante en criptografía: "Criptografía de clave pública/clave privada", representado por el algoritmo de intercambio de claves

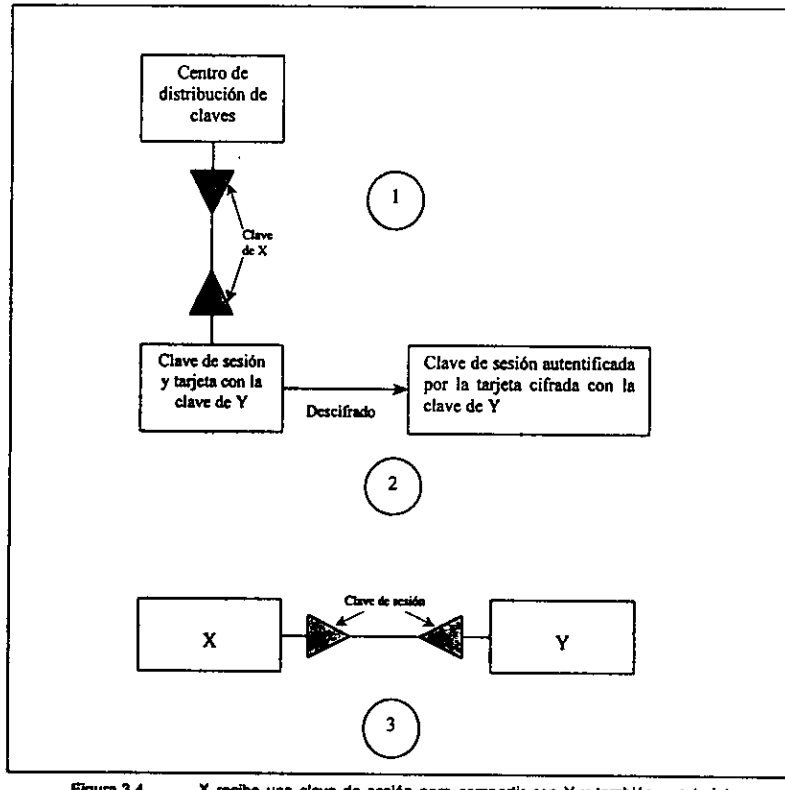


Figura 3.4 X recibe una clave de sesión para compartir con Y y también una tarjeta cifrada para Y. X redirige la clave de sesión a Y, quien confirma que procede del KDC mediante su clave secreta.

RSA – Clave pública / Clave privada

Hasta ahora se ha visto cómo dos partes que desean comunicarse de manera confidencial pueden intercambiar claves a través de un método físico de distribución, o bien emplear un centro de distribución de claves. Pero, ¿cuál sería su reacción si se le dijera que existe una manera para que dos personas, sin preparación previa, puedan establecer una clave de sesión secreta a través de una habitación atestada de gente mediante el intercambio de mensajes visibles para todo el mundo?.

Ron Rivest, Adi Shamir y Len Adleman realizaron un descubrimiento extraordinario en el dominio de la criptografía de clave pública, divulgado en 1978. Cuando la mayoría de las personas hablan sobre la criptografía de clave pública/clave privada, usualmente se refieren al algoritmo RSA. El encriptado RSA tiene la propiedad singular de funcionar utilizando un par de claves. Cualquier cosa que se encripte con una de la claves sólo puede ser desencriptada con la otra clave.

En el uso habitual de RSA cada persona genera un par de claves RSA, mantiene una de ellas secreta (la clave privada) y hace pública la otra clave (la clave pública). Debido a sus notables propiedades, RSA puede emplearse tanto para identificación como para cifrado, o ambos.

Mediante RSA, si lo que desea lograr es sólo un mensaje privado, éste se cifra utilizando la clave pública del destinatario, únicamente el destinatario puede encontrarle sentido al mensaje. Si única y exclusivamente se pretende conocer la identidad del remitente, el mensaje se cifra con la clave privada del remitente. Cualquiera es capaz de descifrar el mensaje utilizando la clave pública del remitente, pero sólo aquel que conoce la clave privada del remitente puede haberlo enviado. Las figuras 3.5 y 3.6 ilustran estos conceptos. En ambos casos, el sujeto **X** envía un mensaje a el sujeto **Y**. En la figura 3.5, sólo el sujeto **X** podía ser el remitente, al utilizar su clave privada, pero cualquiera podría leer el mensaje mediante su clave pública. En la figura 3.6, cualquiera podría haber enviado el mensaje empleando la clave pública del sujeto **Y**, sin embargo sólo el sujeto Y podría leerlo utilizando su clave privada.

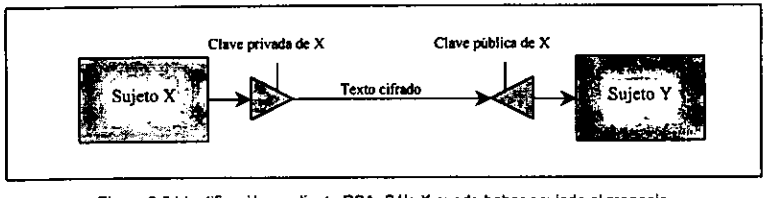


Figura 3.5 Identificación mediante RSA. Sólo X puede haber enviado el mensaje.

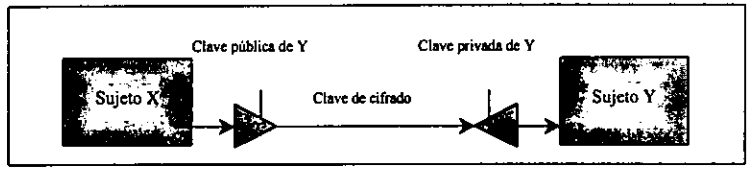


Figura 3.6 Confidencialidad mediante RSA. Sólo Y es capaz de leer el mensaje.

Los problemas surgidos en el establecimiento de un protocolo seguro para la comunicación entre el sujeto **X** y el sujeto **Y** sin la interferencia de alguien más ponen de manifiesto las dificultades en el diseño de un sistema seguro, incluso utilizando algoritmos criptográficos potentes.

Dado que habitualmente las claves RSA tienen una longitud mínima de 500 bits y, a menudo, esta longitud alcanza los 2000 bits y, por lo tanto, trabajar con RSA requiere una gran cantidad de procesamiento, resulta deseable reducir el volumen de datos cifrados mediante el proceso RSA.

Por ello, la manera usual de enviar un mensaje sería elegir una clave de sesión aleatoria DES y, entonces, utilizar técnicas RSA para transmitir únicamente una nota muy corta al receptor conteniendo la clave de sesión, seguida de la totalidad del texto del mensaje cifrado mediante el viejo DES habitual y utilizando la clave de sesión.

El receptor emplea su propia clave privada par abrir el sobre RSA y ver quién es el supuesto remitente. Con la clave pública del remitente, el receptor abre e identifica el anexo interior y recupera la clave de sesión. En este instante, es posible descifrar el propio texto del mensaje a una velocidad elevada usando la clave de sesión y la técnica habitual de descifrado para la clave secreta.

3.2.9. Ventajas y desventajas

La ventaja obvia de cualquier buen esquema de encripción, es que el material codificado no pueda ser usado sin la llave. Esto significa que, por ejemplo, uno no necesita preocuparse acerca de alguien que esté interviniendo la línea telefónica o interceptando la señal de microondas (la transmisión interceptada es inútil sin la llave). Similarmente, los datos encriptados en disquetes no son un riesgo el descubrirlos a menos que la llave venga acompañada en el disquete. En esencia, los datos encriptados en cualquier forma y en cualquier medio, asumiendo que un esquema DES o un equivalente o uno mejor es usado razonablemente, puede ser considerado como no sujeto a ser descubierto o usado por personas no autorizadas.

La encripción tiene desventajas, ya que si la llave se pierde, los datos o lo que sea no estarán disponibles para los usuarios autorizados quedando claro que para un intento de penetración cambia el énfasis para la llave. Así, la administración de llaves llega a ser una parte mucho más importante que la administración de la seguridad de los datos.

La desventaja potencial más grande de la encripción es probablemente la degradación del rendimiento de los equipos. Para usar cualquier dato o programa que está encriptado, primero debe ser encriptada la información, entonces almacenarla o transmitirla y después, desencriptarla; resulta obvia la afectación en el rendimiento de un equipo que utiliza información encriptada.

De algún modo, la llave necesaria para leer datos encriptados debe ser proporcionada al usuario propuesto. El método de comunicación de tales llaves debe ser extremadamente seguro, o el uso de las llaves de encripción es inútil. De cualquier modo las llaves necesitan ser transmitidas no tan a menudo como los datos encriptados.

El mejor consejo en encripción estaría en asegurar que el material extremadamente sensitivo (por ejemplo, tablas de contraseñas y códigos autorizados o llaves de encripción durante la transmisión) esté encriptado. El material que no es sensible no debe ser encriptado.

El incremento en la encripción de la información está siendo visto como necesario para la protección de la privacidad en aplicaciones tales como teléfonos celulares y para seguridad en áreas tales como transacciones financieras, intercambio electrónico de datos (EDI) y otras aplicaciones comerciales. Las aplicaciones de criptografía continuarán incrementando cuestiones de seguridad y privacidad.

3.3. Clasificación de los datos

Esta sección tratará con procedimientos para la preparación y comunicación de decisiones acerca de cómo deben manejarse los datos. Usualmente involucra la división de datos dentro de un número limitado de clases, todos los datos en una clase se manejan similarmente; y la etiquetación de los datos con el nombre del conjunto de procedimientos por los cuales son manejados.

A continuación se establecerán los conocimientos que se requieren para poder definir e implementar los procedimientos de la clasificación de los datos:

- Los elementos y objetivos de un esquema de clasificación.
- El criterio por el cual se clasifican los datos.
- Los procedimientos que se prescriben para tal esquema.
- Las diferencias entre programas de gobierno y comerciales.
- Las limitaciones de tales programas.
- Como llevar a cabo tal programa.

La clasificación de datos con respecto a su sensibilidad y otros criterios son un elemento importante de un plan de seguridad de la información. La clave es identificar las cosas que necesiten un manejo especial y etiquetarlas en orden para permitir al sistema aplicar controles de una u otra forma. Los datos y el personal necesitan se les asignen categorías: para los datos, su sensibilidad; y para el personal, los artículos que requieren o se permiten accesar.

Para entender más acerca de los términos y/o conceptos más usados para el conocimiento y aplicación de la clasificación de datos, las definiciones relacionadas a esta sección se encuentran en el apéndice A.

3.3.1. Elementos y objetivos de un esquema de clasificación

En el entorno de la seguridad de la información, el propósito de la clasificación de los datos es simple: ayudar a determinar que medidas de seguridad aplicar a que elementos de los datos. Un esquema de clasificación de datos debe incluir:

- Una política de seguridad que permita la clasificación de los datos.
- Alguna forma de marcar datos (como niveles de clasificación).
- Procedimientos y reglas que controlen el acceso a los datos.
- Procedimientos y reglas que permitan controlar el almacenamiento, la retención y la disposición de los datos.
- Controles (tales como, bitácoras para rastrear actividades de acceso).

La clasificación de los datos va de la mano con la clasificación del personal. Generalmente, el personal que posee un alto nivel de acreditación estará permitido accesar los niveles más altos de datos.

3.3.2. Criterios para clasificación de datos

Muchos criterios pueden ser usados en clasificación de datos, ya que todo lleva etiquetas tales como "confidencial", "secreto", etc. Una cuestión fundamental es que, desde una perspectiva de seguridad, casi cualquier dato debe estar clasificado y protegido; y desde un punto de vista de facilidad de uso, casi todos los datos deben estar libremente accesibles. Una posible metodología para la clasificación de datos involucra las siguientes características:

- Cantidad

- Edad y vida útil
- Alcance y número de asociaciones independientes
- Importancia

Cantidad

En muy claro que el volumen de datos tiene implicaciones en el procesamiento. Si se parte de la base de que una clasificación de datos con un nivel alto de sensibilidad implica una atención especial; ya que una cantidad muy grande de datos clasificados como de alto nivel tiene un impacto mayor en las operaciones normales y mayores requerimientos de los recursos de cómputo.

Edad y vida útil

Todos los datos tiene una vida útil. Generalmente los datos más viejos son los que menos valor tienen; por lo que, un esquema de clasificación deberá incluir revisiones regulares para asegurar que los datos que han sobrevivido a su vida útil no continuarán con una clasificación alta.

Alcance y número de asociaciones independientes

El nivel de clasificación de datos puede variar dependiendo de sus asociaciones con otros datos. Por ejemplo, los datos de la credencial de elector se usan frecuentemente para identificación y la privacidad es primordial; por lo que, estos datos merecen una clasificación mayor porque se asocian con muchos otros elementos de datos.

Importancia

Este término se aplica más comúnmente a sistemas de información, aunque también aplica a datos. En un ejemplo de información acerca de un plan de mercadotecnia, algunas formas financieras podrían ser muy críticas para una organización; por lo que,

si un competidor las descubre antes de que el plan esté en marcha, tendría información valiosa para hacer una estrategia propia de contabilidad. Consideraciones similares aplican para información táctica militar.

3.3.3. Procedimientos y manejo de un esquema de clasificación

Se iniciará con la revisión de los seis requerimientos fundamentales de seguridad que tienen que ver con controles de acceso:

- *Políticas de Seguridad*: Deben definirse políticas y procedimientos para reforzar al sistema.
- *Etiquetación:* Las etiquetas deben estar asociadas con objetos.
- *Identificación:* Se deben identificar entidades individuales.
- *Contabilidades:* Las pistas de auditoría deben de apoyar a la localización de acciones para entidades individuales.
- *Garantías:* El sistema debe ser capaz de una evaluación independiente para garantizar que el sistema da fuerza a las políticas de seguridad.
- *Protección continua:* Se deben reforzar continuamente los mecanismos de seguridad.

El manejo de un esquema de clasificación difiere principalmente en los primeros cuatro de estos requisitos.

Como se discutió anteriormente, una política de seguridad debe existir, y entre otras cosas, define niveles de clasificación y privilegios de acceso. Sin este requerimiento fundamental, ningún esquema de clasificación puede ser muy efectivo.

Es esencial que se efectúe la etiquetación de objetos para su correspondiente clasificación y, es posible que también sea necesario etiquetar algunas características como la de solo-lectura o niveles de acreditación de acceso permitido. Por ejemplo, una copia en firme deberá tener una clasificación en la parte inicial o encabezado de la copia, un título de página, la primera página y una terminación al final de la copia. Los

medios magnéticos deben estar en contenedores etiquetados cuando no están montados y las etiquetas internas deben incluir la clasificación de los datos.

Las cuentas de usuario incluyen: autenticación, pistas de auditoría, bitácoras y revisiones periódicas de cada cuenta. El objetivo es que debe ser posible rastrear acciones de entidades y, en último de los casos, a los seres humanos quienes efectuaron las acciones. En el contexto del manejo de la clasificación se incluyen políticas y procedimientos que definen autorización, custodia, propiedad y procedimientos similares; además de mecanismos para monitorear y dar fuerza a las políticas y procedimientos.

Entre los procedimientos que se deben definir en una política de seguridad están aquellos que se encargan de establecer los controles apropiados para la reproducción y almacenamiento de datos e información. Estos procedimientos tendrán una variación dependiendo del nivel de clasificación y de las necesidades de cada organización en relación con la clasificación de los datos.

3.4. Seguridad en computadoras y sistemas

En esta sección se resaltarán los atributos que debe tener todo especialista en seguridad de sistemas y cualquier relación que se tenga para garantizar que los sistemas de información no se vean afectados por ataques o intrusiones que afecten la integridad y confidencialidad de los datos. Por lo que se hablará de aspectos tales como:

- Seguridad en sistemas operativos.
- Estándares y guías presentes, base de cómputo confiable.
- Principios de diseño para seguridad en sistemas.
- Fallas comunes y métodos de intrusión.
- Código de virus para computadoras.
- Contramedidas.

3.4.1. Seguridad en sistemas operativos

Es evidente que la razón principal por la que deben existir sistemas operativos seguros, es la de proporcionar protección a la información que reside en sistemas computacionales, ya sea en medios magnéticos como discos duros o cintas; o en medios de solo lectura como láser, discos ópticos, cartuchos, etc. Esta protección está enfocada a dos grandes situaciones específicas: destrucción y accesos no autorizados.

Más importante que el proteger a la información resulta el entender las causas por las que algún individuo o grupo de trabajo desearía dañar la misma para hacerla inservible. Dentro de las más comunes se encuentran la inconformidad de usuarios al ser despedidos o no ser atendidas sus demandas, el dañar la imagen de un área de trabajo antagónica y, en algunos casos, simplemente por gusto.

Curiosamente, uno de los problemas más grandes hoy en día es la falta de conocimientos en el empleo de equipos computacionales; esto es, usuarios que no saben emplear el equipo o sus comandos, de allí que la capacitación es una necesidad imperativa.

La seguridad absoluta probablemente es imposible de conseguir; sin embargo, es posible alcanzar una seguridad razonable combinada con un usuario razonable para sistemas de información basados en computadoras. Hoy en día, se registran muchos eventos de penetración a sistemas de computadoras modernas; pero, definitivamente muchos menos y con más dificultad que los que se registraban antes, ya que hoy es más probable que se detecte el intento de penetración debido a otros controles instalados para defender los sistemas de cómputo. En el futuro, los sistemas diseñados para seguridad serán bastante más seguros.

Kernels, capacidades y validaciones de referencia

La palabra *Kernel* ha sido usada algunas veces para denotar la parte del sistema operativo que está residente en memoria en todo tiempo. Este término tiene un significado diferente en el contexto del diseño de sistemas operativos seguros.

En un sistema seguro, el *kernel* es un pequeño módulo que forma parte del sistema operativo. Todas las referencias a información y todos los cambios a privilegios deben pasar a través del *kernel*. Para esto el *kernel* necesita reunir tres condiciones básicas que son:

1. *Integridad.*- Todos los accesos a información deben pasar por el *Kernel.*
2. *Aislamiento.*- EL *kernel* por sí mismo debe estar totalmente protegido de cualquier forma de acceso no autorizado o alteración.
3. *Verificable.*- El *kernel* deben ser pequeño, bastante simple y que pueda ser demostrado que el *kernel* reúne especificaciones de diseño.

El desarrollo y comprobación de la seguridad del *kernel* usa conceptos matemáticos y técnicas que están más allá del alcance de este documento. Sin embargo, los desarrollos normalmente incluyen cuatro factores importantes:

1. Un modelo matemático define las reglas para demostrar que está garantizada la seguridad del sistema.
2. Especificaciones formales complementan la brecha entre el modelo matemático y la implementación actual del *kernel.* Las especificaciones formales también deben ser demostradas matemáticamente.
3. El *kernel* es desarrollado en un lenguaje de alto nivel que se puede verificar matemáticamente con exactitud.
4. Las implementaciones del *kernel* son verificadas matemáticamente, usando los tres elementos anteriores.

Si se encuentran las tres condiciones básicas y los cuatro elementos listados anteriormente están presentes, entonces el *kernel* puede ser considerado seguro. Así, el sistema operativo será seguro sí: el *kernel* ha sido verificado, si no se realizan cambios sin autorización y si todas las referencias pasan por el *kernel*.

Capacidades y validación de referencias

Para los propósitos de este documento, la validación de referencias y capacidades pueden entenderse si son considerados como parte de un sistema con un *kernel* de seguridad. (El *kernel* incluye validaciones de referencia y puede usar capacidades y así es más fuerte que con el solo tener validación de referencia o capacidades).

Una forma de validación de referencia es la llave de protección para almacenamiento, normalmente implementado en cualquier sistema de paginación. De manera más simple, si un proceso intenta realizar una referencia y no tiene la llave de protección, la referencia es denegada (en este caso por el *kernel*).

Las capacidades abarcan más que las llaves de protección, ya que incluyen no sólo el derecho para accesar algo, sino también que clase de accesos son permitidos. Cada posible acción física o lógica dentro de la computadora es asociada con una capacidad (bajo el control del *kernel* de seguridad, las capacidades son creadas, modificadas y, algunas veces revocadas, como las funciones de la computadora). Una capacidad, en términos de la computadora, puede incluir información acerca de que si está referenciado, entonces puede ser leído , escrito, ejecutado o borrado. Por ejemplo, si un proceso tiene la capacidad para ejecución de un módulo objeto, entonces al proceso no se le permite leer el código del módulo objeto, borrar éste o cambiarlo; únicamente puede correr el módulo.

El *kernel* de seguridad es responsable de examinar la capacidad que presenta un proceso que intenta accesar información. El *kernel* asegura que sólo pueden ocurrir acciones permitidas por la capacidad (referencia, cambios, borrado, ejecutando un

proceso, etc), y que la capacidad es asignada por las características de la información referenciada.

3.4.2. Base de cómputo confiable

El término de base de cómputo confiable se utiliza para definir la porción del sistema operativo de la computadora que contiene todos los elementos del sistema que son responsables de aplicar las políticas de seguridad y de apoyar el aislamiento de objetos (datos y código) en la cual está basada la protección.

TCB Presente

El criterio de evaluación TCB[8], está basado en seis requerimientos fundamentales de seguridad que tienen relación con la seguridad de sistemas de información y controles de acceso. Dichos requerimientos están apoyados en los conceptos y las funciones principales de un sistema operativo seguro. Estos requerimientos son:

1. Para el sistema debe haber una política de seguridad explícita y bien definida.
2. Las etiquetas de control de acceso deben estar asociadas con objetos (marcado).
3. Se deben identificar asuntos individuales (identificación).
4. La información de auditoría se debe guardar y proteger para que se puedan rastrear las acciones que afecten la seguridad (control de cuentas).
5. Los sistemas de la computadora deben contener mecanismos de hardware y software que puedan ser evaluados independientemente para proveer las suficientes garantías que las políticas de seguridad impongan al sistema (garantías).
6. Los mecanismos de control que dan fuerza a las políticas de seguridad se deben proteger continuamente contra falsificación y cambios no autorizados (protección continua).

[8] TCB.- Trusted Computing Base.- Base de cómputo confiable.

Los criterios de evaluación están agrupados dentro de cuatro divisiones (D, C, B y A); las divisiones C, B y A están subdivididas, a su vez, en clases. El rango que definen estas divisiones va desde la protección mínima en la división D hasta la clase A1, que es la más confiable. Las divisiones y clases para el TCB son:

- *División D: Mínima protección.*- Esta división está reservada para sistemas que no reúnen los estándares para cualquier clase de evaluación mayor.

- *División C: Protección discrecional.*- Las clases en esta división proveen protección discrecional a través de las cuentas de usuario que incluyen la capacidad de ser auditables.

- *Clase C1: Protección de seguridad discrecional.*- El TCB de un sistema clase C1 normalmente satisface los requerimientos de seguridad discrecional por proveer separación de usuarios y datos. Los usuarios individuales pueden proteger, a su vez, datos privados o de proyectos para que no puedan ser leídos o alterados por terceros.

- *Clase C2: Protección de acceso controlado.*- Los sistemas en la clase C2 dan más fuerza a controles de acceso discrecionales precisos, creando cuentas individuales por usuario, monitoreando sus acciones y auditando eventos relevantes de seguridad además de aislar los recursos.

- *División B: Protección mandatoria.*- Un TCB con este nivel preserva la integridad de etiquetas sensitivas y el uso de ellas a través de un conjunto de reglas de control de acceso mandatorias. Los sistemas en esta división deben llevar las etiquetas sensitivas con mayores estructuras de datos en el sistema. El desarrollador del sistema también provee el modelo de políticas de seguridad en el cual la TCB está basada.

- *Clase B1: Protección de etiquetado de seguridad.- Los* sistemas de clase B1 requieren todas las características especificadas para clase C2 y, además, deben presentar una declaración informal del modelo de políticas de seguridad, etiquetado de datos y controles de acceso mandatorios sobre los asuntos y objetos relacionados. Debe existir el término capacidad para etiquetar fielmente la información exportada.

- *Clase B2: Protección estructurada.*- Para los sistemas clase B2, el TCB requiere de un modelo formal de políticas de seguridad claramente definido y documentado, que sigue haciendo uso de lo discrecional y hace obligatorios los controles de acceso mandatorios encontrados en los sistemas clase B1, para ser extendido a todos los asuntos y objetos en el sistema de la computadora.

- *División A: Protección verificada.*- La diferencia critica entre la división A y la división B es que se usan métodos formales para que se puedan aplicar pruebas matemáticas en el análisis. Esta división se caracteriza por el uso de métodos de verificación de seguridad formal para asegurar que los controles de seguridad discrecional y mandatoria empleados en el sistema puedan proteger, de manera efectiva, la información clasificada o sensitiva almacenada o procesada por el sistema.

- *Clase A1: Diseño verificado.*- Los sistemas en clase A1 son funcionalmente equivalentes a los de clase B3 en el que no se han adicionado características de arquitectura o se han agregado requerimientos de políticas.

La figura 3.7 muestra la relación entre 27 criterios y las divisiones que se han definido aquí. Las divisiones están marcadas por sus siglas y los criterios están particionados más o menos dentro de cuatro categorías: documentación, garantías, cuentas y políticas de seguridad.

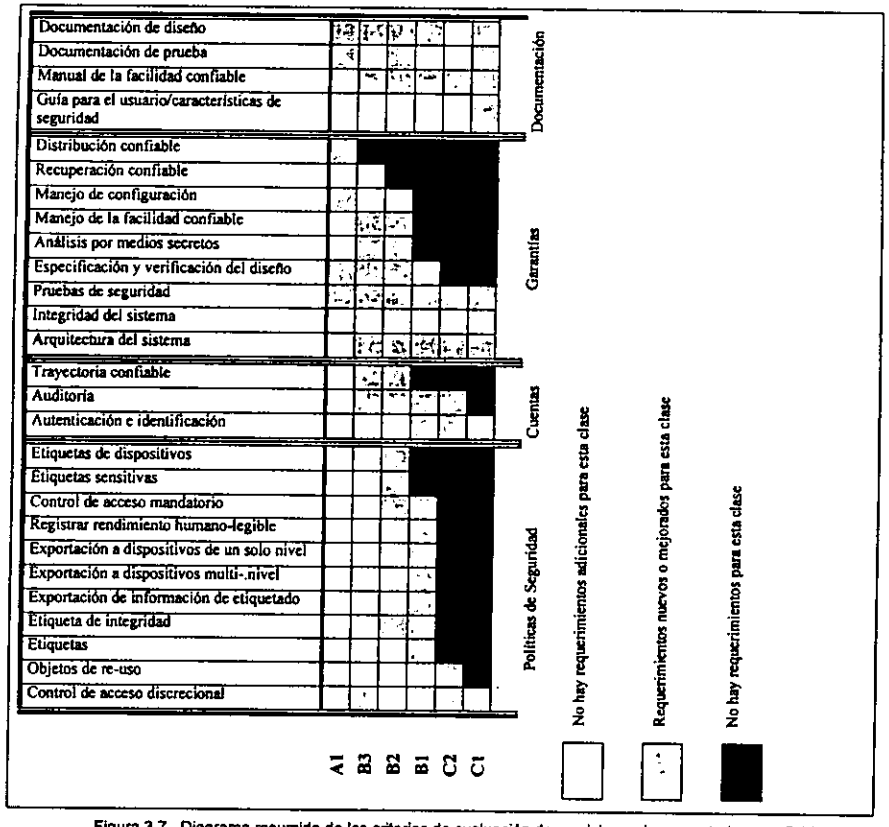


Figura 3.7 Diagrama resumido de los criterios de evaluación de un sistema de computadora confiable.

3.4.3. Principios de diseño para seguridad en sistemas

Como principios generales, existen varios criterios que contribuyen al diseño de sistemas que deben operar de forma segura, dichos criterios son descritos brevemente de la siguiente manera:

- *El último privilegio.*- Un proceso o persona debe tener solamente aquellos accesos y capacidades operacionales que requiere actualmente para el uso eficaz y adecuado del sistema.

- *Diseño Abierto.*- El sistema debe ser diseñado como un sistema abierto; esto es que, independientemente del hardware, permite ejecutar las aplicaciones y por ende el trabajo de los usuarios de cualquier tipo de equipo, reduciendo significativamente la curva de aprendizaje de los mismos al cambiar de plataforma de hardware.

- *Valores por defecto.*- Es sabido que los sistemas son susceptibles a fallas durante su ciclo de vida, y en lo que respecta a seguridad, algunos modos de falla deben ser diseñados para mantener los requerimientos de seguridad. Es como aplicar el concepto de protección continua, esto es, que una falla no debe violar los condiciones de seguridad establecidas.

- *Economía de mecanismos.*- Aquí, quizás, la regla básica para cualquier sistema sería "simplemente guárdelo", ya que algunas medidas de seguridad pueden ser muy rigurosas al aplicarse. Es importante señalar que el mecanismo más simple, y aquellos otros mecanismos semejantes que son implantados actualmente como elementos de las políticas de seguridad, son considerados para ser incluidos en el diseño.

- *Naturalidad (Factores Humanos).*- En esta parte está muy claro, con el simple hecho de que los procedimientos no sean aceptables, incómodos o interfieran con el trabajo efectivo, las personas encontrarán la manera de evitar dichas características. Los sistemas de seguridad deber ser utilizados para una completa protección con una interrupción mínima para atender requerimientos.

- *Protección continua.*- El último en está lista, pero no menos importante que los anteriores, esto es porque es crítico que las características de seguridad proporcionen protección continua, incluso en modalidades de fallas.

En base a estos criterios generales; el papel de los modelos de seguridad, en el diseño de sistemas seguros, puede ser una parte importante en el desarrollo de nuevas formas de protección a la información sensitiva en cualquier equipo de producción. Estos modelos de seguridad deben tener las siguientes características:

1. Ser precisos y sin ambigüedades.
2. Ser simples, concretos y, en consecuencia, fáciles de comprender.
3. Ser genéricos, esto es: solo trata de propiedades de seguridad y no restringe indebidamente las funciones del sistema o su aplicación.
4. Son una representación práctica de las políticas de seguridad.

Los primeros dos puntos deben ser obvios y el punto 3, combinado con el punto 4, logran que la condición de seguridad y tecnología de información no permitan pruebas formales de sistemas complejos. Por consiguiente, el modelo debe ser simple y una representación práctica de la política para que los argumentos informales de la seguridad del sistema puedan ser suficientes. El punto 3 manifiesta meramente que los modelos de seguridad deben tratar con problemas de seguridad y no estar confundidos con lo que es aplicación o problemas de seguridad no planeados. Éste es, en cierto sentido, un caso del principio de economía de mecanismos.

La elaboración de un modelo de seguridad involucra esfuerzos considerables y sólo vale la pena si el diseñador tiene libertad y recursos para diseñar un sistema con seguridad bien pensado. Si las únicas alternativas permitidas para restringir recursos o la política de administración es la de "tapar los huecos de seguridad" (realizar cambios para cerrar vulnerabilidades ya conocidas), esto implica que en un modelo de seguridad probablemente se derrochen esfuerzos.

Tipos de modelos de seguridad

En este documento se mencionarán dos tipos de modelos de seguridad muy relevantes, que permitirán una mejor comprensión de dichos conceptos y así poder aplicarlos a la

plataforma que se tenga actualmente en producción, de tal hecho se asumirán dos, y éstos son:

1. Modelos de no-interferencia
2. Modelos estado–máquina

Los modelos de no-interferencia involucran modos para prevenir casos que operen en un dominio y los afecten de cierta manera que se puedan violar la políticas de seguridad del sistema. Mientras estos modelos se mantienen para un uso futuro, no están a favor de esfuerzos útiles para un diseño real actual. En consecuencia, este documento se concentrará en modelos de estado-máquina.

Un modelo de estado-máquina describe un sistema, como un modelo matemático abstracto, con variables de estado que representan el estado de un sistema y la transición funcional, definiendo cómo el sistema se mueve de un estado a otro. Dichos modelos no son factibles para el modelo detallado de sistemas operativos complejos. Puesto que los modelos de seguridad sólo pueden tratar con seguridad las variables de estado pertinentes, un modelo de estado-máquina para un sistema de seguridad puede ser más sencillo. Por eso es importante identificar los pasos a seguir para desarrollar un modelo de estado-máquina, y para esto se han establecido seis puntos muy importantes que son:

1. Definir la seguridad de las variables de estado pertinentes.
2. Definir las condiciones para un estado seguro.
3. Definir la función para la transición de estados.
4. Demostrar que las funciones mantienen el estado seguro.
5. Definir el estado inicial.
6. Demostrar que el estado inicial es seguro en términos de la definición del estado seguro.

Una vez definidos estos puntos, demostrando que el estado inicial está seguro y que las funciones de la transición de estados están seguras, se puede demostrar que el sistema permanecerá en un estado seguro.

3.4.4. Fallas comunes y métodos de penetración

Aunque los sistemas de información computarizados sólo han existido durante las últimas décadas, ha habido una gran y dolorosa experiencia con problemas de seguridad. De los "*hackers*", principalmente aficionados pero a menudo con habilidades de muy alto nivel, a habido penetraciones profesionales a los sistemas de información y a cualquier valor almacenado en dichos sistemas. El valor de esta experiencia de seguridad en sistemas de información informatizados es que se han identificado varias fallas generales comunes a muchos sistemas operativos y, a su vez, se han identificado varias técnicas de penetración comúnmente repetidas. Si se han aprendido bien los conceptos establecidos en el contenido de este documento, entonces se aplicará ahora un plan bien establecido y principios de administración para controlar los problemas.

Fallas comunes del sistema operativo

Con el tiempo, se han usado muchos métodos para penetrar sistemas operativos; de igual forma muchos sistemas operativos comparten fallas comunes que hacen que la penetración sea más fácil de lo que debe ser. Algunas de estas vulnerabilidades son:

- *Encripción:* La lista de datos sensibles como la tabla de cuentas y identificadores de contraseñas deben estar encriptadas, para que cualquiera que administre el acceso a los archivos no pueda leerlos.

- *Aplicación:* Se puede tener un sistema de seguridad bien diseñado en el sistema operativo pero que no se usa apropiadamente en la organización.

- *Compartido Implícito*: El sistema puede colocar un sistema operativo sensible que controle información en el espacio de trabajo del usuario; bajo algunas condiciones, el usuario puede ser capaz de leer esto (por ejemplo, un error del programa, quizás deliberadamente inducido, lo cual causa un vuelco de memoria (DUMP) y que

también puede provocar una copia impresa de todo en el espacio de trabajo, incluso cualquier cosa que el sistema operativo pueda haber guardado allí).

- *Verificación de parámetros incompletos.*- Un defecto del sistema, que se da cuando todos los parámetros no se han verificado totalmente para la exactitud y consistencia del sistema operativo, puede hacer que el sistema sea vulnerable a penetraciones.

- *Verificando legalidad.*- El sistema no puede verificar los parámetros que un usuario le proporciona.

- *Línea desconectada.*- El usuario en un tiempo-compartido, o en otro modo del sistema remoto, puede colgar sin desconectar, otro usuario puede ser capaz de entrar sin validación propia. No todos los sistemas "cuelgan" propiamente cuando una línea está desconectada.

- *Descuido del Operador.*- Los operadores pueden montar, inadvertidamente, paquetes de discos o cintas en mal estado; o bien, en algunas ocasiones se ha informado de casos donde los penetradores han telefoneado al operador y lo han podido engañar para proporcionar información sensible.

- *Contraseñas.*- Al usar contraseñas, éstas pueden ser sencillas de adivinar, o el sistema puede permitir repetidos intentos.

- *Repetición.*- Los sistemas pueden permitir un número indefinido de intentos a los usuarios que intentan accesar. El sistema debe desconectar o debe colgar después de algún número pequeño de infructuosos intentos, y el evento debe informarse al operador o persona que se encarga de la seguridad.

- *Basura.*- Deben eliminarse copias impresas sensibles.

- *Técnicas de penetración específicas.*- Caballos de troya, virus, *worms*, *salami*, *piggyback*, engaño, compromiso humano, etc.

Se han usado varios métodos de penetración y, muchas veces, la penetración ha sido exitosa. Muchos de los métodos comunes hacen el uso de las fallas que se mencionaron anteriormente y, desgraciadamente, todavía es muy común encontrar que los sistemas son vulnerables a estos métodos, aunque los métodos son bien conocidos y muchas veces son fáciles de vencer. Un especialista de seguridad debe trabajar con personal de sistemas de información para asegurar que por lo menos estos "agujeros" comunes se tapen. Las técnicas más usadas son:

- *Acceso a través de las líneas.*- El acceso obtenido a través de un analizador activo por un usuario no autorizado, a un terminal inactiva momentáneamente de un usuario legítimo asignado a un canal de comunicaciones.

  Una terminal especial es usada para intervenir la línea de comunicación que es usada por un usuario legítimo mientras el usuario no está activo. Nunca deben abandonarse y desatenderse las terminales una vez que se han firmado en ellas y deben protegerse las líneas de comunicación.

- *Revisando o Hojeando.*- Es el acto de investigar a través de medios de almacenamiento para colocar o adquirir información sin necesariamente conocer la existencia o el formato de la información buscada.

  Las búsquedas del usuario a través del sistema o a través de archivos que intentan localizar información sensible. Normalmente se crea una tabla que lista lo que el usuario puede tener acceso, y el usuario se restringe a sólo esos accesos. Pueden darse contraseñas individuales a los archivos en algunos sistemas.

- *Negativa de uso.*- Acción o acciones que impiden a cualquier parte de un AIS[9] funcionar de acuerdo con su propósito proyectado. Esto incluye cualquier acción que causa la destrucción no autorizada, modificación o retraso de un servicio.

[9] Automated Information System.- Sistema de información automatizado.

- *Código oculto.*- Los programas pueden contener código no documentado que hace cosas, que no son las que describen los manuales. El apoyo pobremente controlado permite frecuentemente una oportunidad para un programador para insertar una rutina que no debe estar en el programa. Una biblioteca del programa y controles sobre el mantenimiento pueden hacerlo difícil o imposible.

- *Interrupciones.*- Un penetrador puede provocar la interrupción a programas o sistemas; algunos sistemas operativos permiten un proceso para entrar en un modo privilegiado con más acceso que el usual, mientras se está procesando una interrupción.

- *Desconexión de la línea.*- El usuario abandona la sesión o la línea "se cae," pero el sistema no tiene conocimiento todavía y no termina la sesión del usuario. Hasta que esta terminación suceda, otro usuario puede ser capaz de usar la sesión.

- *Bomba lógica.*- Es un programa de computadora residente que, cuando es ejecutado, verifica por condiciones en particular o estados particulares del sistema que, una vez que se cumplen, existen disparadores que inician la acción no autorizada.

- *Máscaras.*- Es un esfuerzo por obtener acceso a un sistema pasando como un usuario autorizado. El penetrador obtiene una identificación y contraseña y se firma en el sistema como la cuenta de alguien más. Un usuario que pretende ser alguien más tomando una línea como se mencionó anteriormente, es una forma de hacerse pasar por alguien.

- *Tejido de Red.*- El tejer una red es una técnica que se usa en redes de comunicación para obtener acceso al sistema de una organización.

- *Engaño del operador.*- Por ejemplo, un penetrador puede convencer a un operador que divulgue una contraseña.

- *Obtener el acceso no autorizado a un sistema vía la conexión legítima de otro usuario.*- El penetrador intercepta una línea de comunicación y sustituye su o sus propios mensajes al usuario legítimo y/o al sistema (por ejemplo, simula el programa de entrada y así consigue que el usuario proporcione su identificación e información de la contraseña).

- *Técnica del Salami.*- En la seguridad de datos, esta técnica corresponde a un engaño difundido por encima de un número grande de transacciones individuales; ej., un programa que no redondea correctamente cierra las cifras pero desvía los sobrantes a una cuenta personal.

- *Recoger la basura.*- Se pueden realizar búsquedas en la basura con el propósito de datos útiles.

- *Engaños.*- Es la acción deliberada de inducir a un usuario o recurso para que efectúe una acción incorrecta.

- *Falsificaciones.*- Son una modificación no autorizada que altera el funcionamiento apropiado de un sistema o parte de un equipo de una manera que degrada la seguridad que éste proporciona.

- *Análisis de tráfico.*- Es la inferencia de información por la observación de flujos de tráfico (presencia, ausencia, cantidad, dirección y frecuencia).

- *Puertas ocultas.*- Un software oculto o mecanismo de hardware que permiten engañar a los mecanismos de protección del sistema. Se activa de alguna manera pareciendo inocente; ej., una secuencia especial de llave aleatoria en una estación terminal. Diseñadores del software introducen frecuentemente puertas traseras en su código que les permite volver a entrar al sistema y realizar ciertas funciones.

- *Caballos de troya.*- Son programas que parecen tan inofensivos como inocentes, pueden estar disfrazados como un juego, utilerías o cualquier otro programa válido. Cuando se ejecuta, el caballo de troya entretiene al usuario con el juego o utilería

mientras, a la vez, causa daños en segundo plano. Con los caballos de troya, habitualmente la destrucción está bien oculta, de tal forma que el usuario no tiene la menor idea del daño que se está provocando al sistema.

- *Virus.*- Es un programa que puede infectar otros programas modificándolos incluso, posiblemente se desarrolle o se copie así mismo. Un virus puede ser considerado como: un mecanismo de liberación con un proceso de infección que apoya su propagación, y un cargador que es activado por algún evento.

- *Gusanos.*- Es un programa que cambia y destruye datos, como los virus; pero que también puede viajar y provocar daño desde una computadora a otra a través de redes como Internet. Un gusano, después de viajar a otro sistema informático, puede realizar muchas copias de sí mismo, consumiendo gran cantidad de tiempo y pudiendo provocar la caída de toda una red de computadoras.

Ésta no es una lista exhaustiva, sólo son algunos de los métodos de penetración más comunes. Las curas generalmente son algo obvias y muchas veces no cuestan mucho dinero ni degradan el desempeño de los equipos. Y, aunque esto no es un problema técnico, debe mencionarse que la mejor manera de comprometerse con los sistemas de información es dirigirse a aquellas personas involucradas en la administración, programación y tareas similares.

3.4.5. Código de virus de computadora

En los primeros tiempos de la computación, una de las computadoras *Mark II* falló sin motivo aparente. Después de emplear algún tiempo en su diagnóstico y pruebas, los técnicos encontraron el motivo: una polilla estaba estancada en el interior de la computadora. Este incidente dio lugar al nacimiento del término *bug*, que se utiliza hasta nuestros días para describir problemas y fallas de las computadoras. Aunque los *bugs* de los programas y del hardware no resultan agradables, existen otros tipos de *bugs* que podrían resultar incluso más peligrosos para la computadora y la red. Estos

son los *virus* (programas diseñados específicamente para dañar a la computadora y los programas ejecutados por ella). La necesidad de conocer y controlar la amenaza de los virus es especialmente importante, puesto que la red, que contiene cientos de computadoras, puede ser desbaratada e incluso inutilizada por un virus informático. Como resultado, cualquier discusión sobre la integridad y seguridad de los datos en la red se debe prestar mucha atención a los virus.

Los virus informáticos son programas que no sólo causan destrucción en la computadora, sino que también se propagan o infectan otros sistemas con los que tengan contacto. Virus, que en latín significa veneno, es un nombre apropiado, puesto que los virus actúan de manera muy parecida a como lo hacen sus homólogos biológicos, los cuales infectan células y después propagan la infección a otra parte. De acuerdo al diccionario, un virus es: <<un programa de computadora normalmente oculto bajo otro programa aparentemente inofensivo que produce copias de sí mismo y se introduce en otros programas, y que normalmente lleva a cabo acciones maliciosas....>>.

En un sentido genérico, los virus son programas de computadora que se ejecutan, como el software normal, pero tiene la habilidad adicional de replicarse o hacer copias de sí mismos. Un virus no tiene que ser necesariamente destructivo, algunos se parecen más a inocentes travesuras; por ejemplo, mostrar simplemente un mensaje divertido.

Aunque los virus son simplemente código informático (programas), dan la impresión de estar <<vivos>> puesto que hacen mucho más que devorar números o visualizar algo en la pantalla. Existen otros tipos de programas como los que se mencionaron con anterioridad, los gusanos (*worms*), caballos de troya y bombas lógicas, que suelen considerarse en la misma categoría que los virus, aunque son técnicamente diferentes.

Los virus fueron creados por piratas informáticos que querían probar si era posible escribir programas que pudieran no sólo afectar y dañar a las computadoras, sino que además fueran capaces de propagar su destrucción a otros sistemas. En los años

cuarenta, John Von Neumann observó que los programas podían hacerse de forma que se reprodujeran a sí mismos e incrementarán su tamaño. Su trabajo *Teoría y Organización de Autómatas Complicados* no tuvo mayor interés puesto que las computadoras no se utilizaban de manera extensiva y su discurso fue considerado en aquellos tiempos eminentemente teórico. Algunos años más tarde, en los cincuenta, un grupo de científicos de los laboratorios *Bell* comenzaron a experimentar con un tipo de juego en el que los organismos (código informático) de un equipo luchaban contra organismos del equipo oponente. El equipo con mayor número de organismos supervivientes era el ganador de este juego de <<Guerra Informática>>.

Más tarde, en los años sesenta, John Conway desarrolló software <<viviente>> capaz de replicarse a sí mismo. Conforme se iba desarrollando la idea de los programas <<vivientes>> a lo largo del tiempo, el reto de crear programas tipo virus se extendió entre la comunidad académica y de la investigación, y los estudiantes comenzaron a crear todo tipo de programas similares, normalmente como una distracción inofensiva. A lo largo de los años setenta, los piratas informáticos hicieron avances en este tipo de programas, dándoles el poder de producir mayores daños. Sin embargo, los ataques con virus eran algo poco común. Hacia la misma época, los delitos informáticos fueron en aumento, incluyendo el asalto a cuentas privadas y las transferencias bancarias ilegales. Ya en los años ochenta, con la llegada de las PCs, los virus hicieron su aparición en escena como una amenaza real.

El desarrollo de las tecnologías de virus, tales como las tecnologías fantasma y las capacidades de polimorfismo para burlar los escáner de virus, han ayudado a promover las tecnologías de virus a otro nivel. La industria de detección y protección antivirus ha trabajado duro para no quedarse atrás en la lucha contra el ataque de los virus y ayudar a proteger a la comunidad informática y, aún a la fecha, continúan en la lucha.

El software antivirus está diseñado para prevenir las infecciones por virus, explora el sistema en busca de virus, los borra e incluso proporciona al sistema una <<vacuna>> preventiva contra sus ataques. Aunque los distintos paquetes varían en cuanto a características, forma de operación, efectividad y adaptación a las distintas

necesidades, estos programas siempre realizan una o más de las siguientes funciones básicas:

- *Prevención.*- Esta característica está diseñada para evitar que los virus infecten las computadoras. Algunas de las técnicas empleadas incluyen la prevención de cambios en los archivos ejecutables (.com y .exe) y mensajes sonoros si cambia la tabla de asignación de archivos, el sector de arranque o si se prepara el disco duro para ser reformateado.
- *Detección.*- Esta característica busca virus en los discos y otras partes del sistema, y avisa si se sospecha que existe alguno. Se puede identificar el rastro de un virus buscando sus efectos y examinando los archivos y el sector de arranque. Los métodos utilizados incluyen la comparación de los archivos con un algoritmo o firma preestablecida o con dígitos de control (algoritmos numéricos especiales) para cada archivo.
- *Eliminación.*- Implica la eliminación del código del virus de los archivos y discos. Algo a tener en cuenta, sin embargo, es que es difícil estar seguro de que se ha eliminado por completo una infección, por este motivo es mejor borrar los archivos infectados y utilizar copias nuevas y limpias.
- Vacunación: Existe software antivirus que coloca código específico en los archivos ejecutables (.COM y .EXE) y posteriormente comprueba cambios en la firma u otras irregularidades cuando el programa se ejecuta.
- *Control de daños.*- Algunos programas antivirus intentan minimizar el daño causado por los virus. El control de daños preventivo incluye la utilización de avisos cada vez que se cargan programas en RAM, la protección del disco duro contra escritura cuando se ejecuta nuevo software y el mantenimiento de un copia de la tabla de asignación de archivos (FAT)[10]. El programa también podría guardar una copia de la memoria CMOS (que contiene la información de SETUP), para el caso en que ésta fuera borrada por un virus.

[10] File Allocation Table.- Tabla de asignación de archivos.

3.4.6. Contramedidas

Mucho de lo que se ha visto en esta sección, como el diseño de principios y contramedidas que, implementadas propiamente, pueden controlar o prevenir exposiciones a tipos de fallas y técnicas de penetración listadas en las secciones anteriores. Los controles de inferencia, puede limitar la exposición de algunos tipos de problemas de la base de datos; los paquetes de software anti-virales y las precauciones inteligentes pueden minimizar o eliminar problemas con virus.

En lugar de repetir una lista larga de contramedidas para cubrir esta parte, es notorio que la seguridad en sistemas pueden lograrse por:

- La aplicación cuidadosa de las técnicas del diseño y principios de ingeniería de software bien dirigida durante la creación del mismo sistema.
- La aplicación de una administración inteligente de controles de acceso y otras medidas de seguridad durante la operación.
- La práctica de la administración inteligente de procedimientos y emisión de políticas fuera de las áreas técnicas del sistema de información.

Muchos de los controles técnicos discutidos en diferentes secciones a lo largo de este documento son útiles y muchas veces necesarios, como lo son las cerraduras en puertas. Bien aplicados dichos controles, pueden mejorar la situación de seguridad de una manera real y, por supuesto, el aplicarlos en forma no adecuada pueden resultar peor que inútiles, llevando a un falso sentido el concepto de la seguridad. El núcleo fundamental de los requisitos anteriores es el termino llamado "administración inteligente"; faltando éste elemento, ningún sistema de información puede ser considerado seguro.

3.5. Seguridad en telecomunicaciones

En esta sección se describen los principios que permiten asegurar la integridad y confidencialidad en el manejo de mensajes que se transmiten a distancia, además del control y uso de la capacidad de las telecomunicaciones.

Se hacen consideraciones generales de problemas de comunicaciones que pueden suceder en los sistemas mientras continúa aumentando el tamaño de la redes de computadoras y su integración con otras redes; razón por la cual, los retos para mantener la seguridad de los datos aumentan significativamente. Aunque la tecnología de interconexión y herramientas de conectividad han hecho más fácil la comunicación y compartir la información, también ha sido una caja de Pandora exponiendo a las organizaciones a muchos más ataques contra la seguridad que pueden dañar los sistemas informáticos y los datos.

Habitualmente, las redes están conectadas al mundo exterior a través de una variedad de métodos, tales como tableros de noticias, Internet y mecanismos de integración de la telefonía, etc. Esto hace que las persona del mundo exterior tengan más posibilidades de obtener acceso a los servicios informáticos, incluso aunque no tengan ninguna relación con la empresa con cuyas computadoras intentan establecer contacto. Los piratas informáticos, los antiguos empleados, etc.; tienen el potencial de conectarse a los recursos informáticos y trabajar como si estuvieran sentados delante de ellas, pudiendo ocasionar un daño considerable.

En este apartado se establecerá el conocimiento de objetivos, riesgos, clases de ataques, defensas, etc.; explicando cada uno en las siguientes secciones:

- Fundamentos de las telecomunicaciones
- Tipos de ataque
- Emisiones electrónicas
- Comunicaciones
- Diseño de la red
- Sitios de ataque

3.5.1. Fundamentos de las telecomunicaciones

La comunicación de datos es la transmisión y recepción de los mismos, incluyendo, frecuentemente, operaciones como codificación, decodificación y validación. A la tecnología empleada para la transmisión de señales a grandes distancias se le llama telecomunicaciones; y, comúnmente, se logra usando la red de comunicaciones pública (o privada), un conjunto de reglas para la transmisión de la información (protocolo) y el equipo necesario (computadoras, unidades de control (*routers*), modems, terminales, etc...).

A continuación se relacionan las características de los medios de comunicación más empleados en base a la tecnología de transmisión, ancho de banda, potencial de conectividad, alcance geográfico, inmunidad al ruido, seguridad, aplicaciones y costo relativo.

Par trenzado

Aun cuando no es ideal, sobre todo para el enlace de computadoras, el par trenzado está disponible en todas las oficinas de un edificio y soporta confiablemente las redes LAN.

- *Tecnología de la transmisión:* analógica o digital.
- *Ancho de banda:* de 1 a 2 megabits, típicamente 64 Kbps para PABX[11].
- *Potencial de conectividad:* punto a punto y multipunto.
- *Alcance Geográfico*: a 10 millas (16 km).
- *Inmunidad al ruido*: inconstante, típicamente pobre.
- *Seguridad:* pobre, fácil de intervenir e insertar.
- *Aplicaciones:* PABX, redes de estrella, terminales en cascada y redes LAN en bus.
- *Costo relativo*: bajo.

[11] Private Automatic Branch Exchange.- Intercambio automático de trama privada.

Cable coaxial

Normalmente se encuentra tecnología de bus de cable coaxial en la mayoría de los sistemas de televisión por cable y enlaces de redes de alta-velocidad.

- *Tecnología de la transmisión:* Banda base y banda amplia.
- *Ancho de banda:* Banda base de 3-10 Mbps, banda amplia a 150 Mbps en total.
- *Potencial de conectividad:* punto a punto y multipunto.
- *Alcance Geográfico:* Banda base a 1 milla; banda amplia hasta 7 millas.
- *Inmunidad al ruido*: Banda base, 50-60 dB; banda amplia, 85-100 dB.
- *Seguridad*: difícil intervenir sin que sea detectado.
- *Aplicaciones:* Banda Base, dispositivos de señales en cascada; Banda Amplia, modo mixto (digital, video, voz).
- *Costo relativo*: Par trenzado < coaxial < fibra óptica.

Fibra óptica

Tecnología que está actualmente en boga, principalmente para enlaces críticos en muy grandes distancias.

- *Tecnología de la transmisión*: típicamente Banda Base.
- *Ancho de banda*: por arriba de 50 Mbps sobre 10 km.
- *Potencial de conectividad:* principalmente punto a punto, pero los sistemas en cascada son la principal base instalada.
- *Alcance Geográfico:* de 5-10 millas sin repetidores e ilimitado con repetidores.
- *Inmunidad al ruido*: no alterado por interferencia electromagnética y ruido.
- *Seguridad*: excelente (sumamente difícil instalar un analizador sin ser detectado).
- *Aplicaciones*: cables transatlánticos, redes locales, sistemas de telefonía.
- *Costo relativo*: relativamente alto en comparación con par trenzado o coaxial, pero se compensa con volúmenes de producción y nuevos desarrollos.

Radio (Paquetes)

Es un tipo de medio alternativo que permite conexión en lugares donde es difícil instalar otro tipo de infraestructura.

- *Tecnología de la transmisión*: técnicas de propagación de señales espectrales.
- *Ancho de banda:* Unos MHz con un promedio de más de 200 Kbps en datos.
- *Potencial de conectividad*: punto a punto.
- *Alcance Geográfico*: decenas de millas (limitado por curvatura de la Tierra alrededor de 70 millas).
- *Inmunidad al ruido*: variado, generalmente pobre.
- *Seguridad*: no seguro, aunque se usen métodos de encripción.
- *Aplicaciones:* estaciones terminales móviles (p.e.: teléfonos celulares).
- *Costo relativo*: considerado alto, pero está bajando.

Infrarrojo (onda de luz)

Cuando se mejoran los láseres de estado de sólido para las aplicaciones de fibra ópticas, esta tecnología provoca que caigan dramáticamente el precio y tamaño de los equipos.

- *Tecnología de la transmisión:* Pulsos cortos con poderosas técnicas de modulación.
- *Ancho de banda*: de 10-100 Kbps más de 10 millas y 1.5 Mbps más de 1 milla.
- *Potencial de conectividad*: línea de vista (punto-a-punto), multipunto (reflejado) en perímetro limitado.
- *Alcance Geográfico*: en promedio 1 milla para el ancho de banda superior, el máximo práctico de 10-20 millas.
- *Inmunidad al ruido*: no alterado por EMI[12] y el ruido.
- *Aplicaciones*: punto a punto, multipunto dentro de un cuarto.
- *Costo relativo*: alto en comunicación de datos, bajo en las aplicaciones caseras.

[12] ElectroMagnetic Interference.- Interferencia electromagnética.

La figura 3.8 ilustra los costos relativos por eventos de penetración comparando su efecto en varias tecnologías. Y la figura 3.9 ilustra el impacto en el uso de diferentes tecnologías de transmisión de los métodos punto-a-punto en redes complejas.

Como se puede observar, la relación existente entre las dos gráficas son las zonas en donde los ataques a los sistemas en información vía todas aquellas alternativas o medio de comunicación son realizados de acuerdo a la experiencia del personal con conocimientos de métodos y técnicas de penetración, ya que en función de la experiencia profesional o técnica se puedan ejercer diferentes acciones a los diferentes medios de enlace o comunicación en un ambiente sin las medidas adecuadas de seguridad.

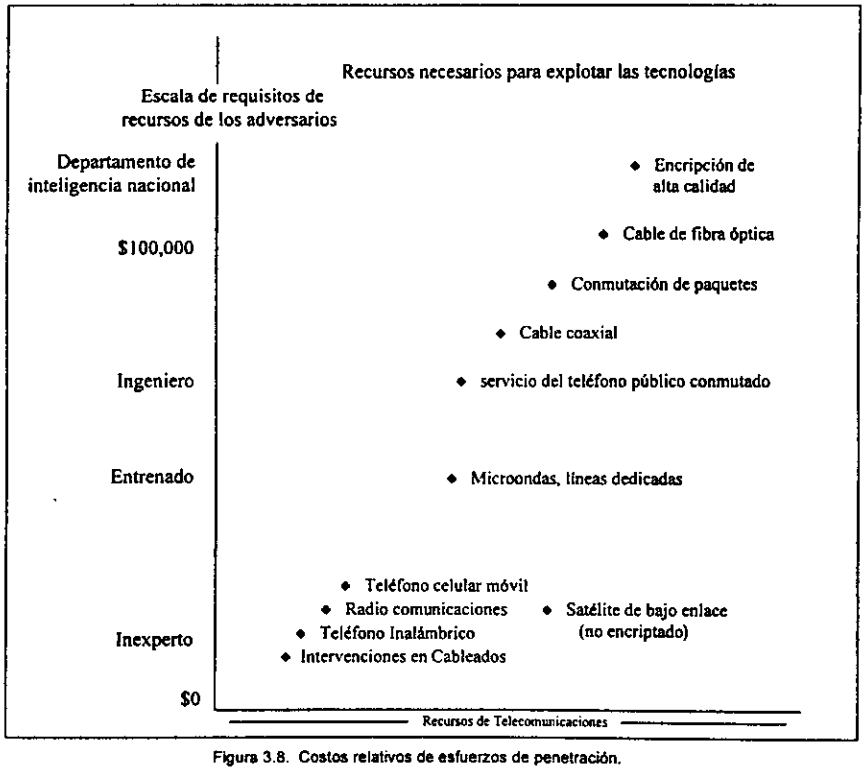


Figura 3.8. Costos relativos de esfuerzos de penetración.

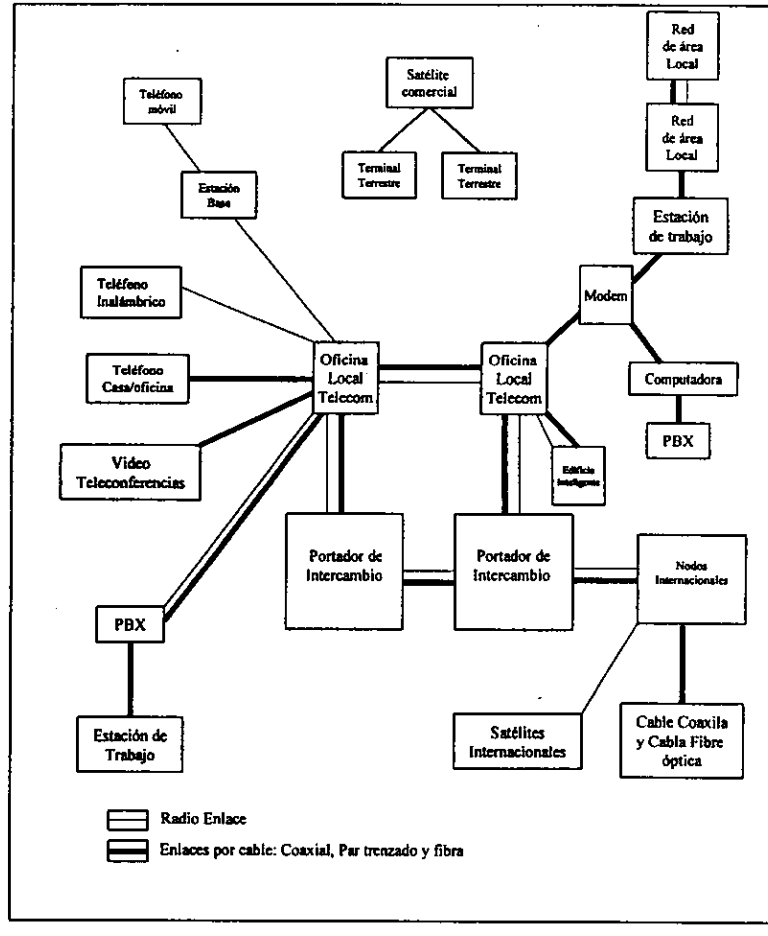


Figura 3.9 Vulnerabilidad de las telecomunicaciones.

Protocolos

Un protocolo de comunicaciones es el conjunto de rutinas que establecen las guías para determinar como y cuando las estaciones de trabajo deben de accesar el cable y enviar paquetes. Derivado de esto existen funciones que son esperadas por el establecimiento de una transmisión, éstas son:

- *Enmarcado:* delimitación de datos.
- *Direccionamiento*: identifica la fuente y destino del mensaje.
- *Sincronización:* el estado de las coordenadas del remitente y receptor, aseguran que se corrijan la transmisión y recepción de los datos.
- *Transferencia de datos:* la transferencia real de la información del remitente al receptor, después de que las funciones anteriores se han realizado.
- *Control de flujo:* es un mecanismo para evitar la transmisión más rápida, de lo que puede recibirse.

De igual forma el término genérico protocolo significa reglas o procedimientos de operación, derivándose los siguientes parámetros para un protocolo de transmisión en red:

- Características de línea direccional
- Velocidad de la línea
- Control de mensaje y convenciones del código

Y en lo que respecta a protocolos para sistemas de terminal-a-computadora se incluyen:

- Control del módem
- Caracteres de sincronización
- Identificadores de mensaje
- Terminadores de bloque de mensajes
- Control de la línea
- Procedimientos de manejo de errores
- Procedimientos de la terminación

Circuito de intercambio de paquetes

El circuito de intercambio es simplemente la conexión de dos dispositivos comunicándose sobre un circuito que se establece entre ellos. Típicamente el circuito se dedica a que las transmisiones se logren durante el período de la conexión. Esto

produce dos problemas: hay límites físicos en el número de circuitos y el sistema de comunicación está sujeto a la carga excesiva; además, una capacidad considerable es desperdiciada en enlaces típicos que no son usados continuamente (Por ejemplo, la capacidad de un circuito que está dedicado incluso mientras un usuario decide qué tecla presionar en la terminal durante el tiempo que no existe comunicación). Una solución que se ha implementado es el intercambio de paquetes.

En el intercambio de paquetes, los datos se agrupan dentro de paquetes, típicamente por arriba de 1,024 caracteres en longitud. Cada paquete contiene información de control del paquete como longitud y las direcciones del origen y destino. Las redes de intercambio de paquetes incluyen herramientas sofisticadas para determinar la ruta a aplicar a cada paquete para optimizar la utilización de la red y el tiempo de respuesta al usuario. En contraste con las redes de circuitos de intercambio, en el cual el usuario controla la duración de la conexión total, el intercambio de paquetes hace uso de porciones de la red, que podrían ser monopolizadas por el usuario, aunque esa porción no esté actualmente activa.

La mayoría de los sistemas de intercambio de paquetes soportan el protocolo X.25 de la CCITT[13], como un conjunto de estándares para redes de acceso publicas de intercambio de paquetes. La mayoría de las redes públicas y privadas en el mundo soportan el protocolo X.25.

3.5.2. Tipos de ataque

Hay dos tipos fundamentales de ataque: pasivo y activo. En un ataque pasivo a un sistema de telecomunicaciones se pretende evitar la detección del ataque y en un ataque activo se incluye la intervención de los medios y el flujo de la comunicación para borrar o alterar algo; aunque en una situación real, es común que se tenga una combinación de técnicas pasivas y activas.

[13] Comité Consultivo Internacional de Teléfonos y Telégrafos.

Un ataque pasivo a un sistema de telecomunicaciones por definición se limita a la observación en los medios sin alterar datos dentro del sistema. Los ejemplos incluyen escuchar a través de la intervención de cables, el descubrimiento derivado de la observación de una terminal y el análisis de tráfico.

Para transmisiones en par trenzado, una simple vuelta del alambre alrededor del cableado recogerá impulsos magnéticos que pueden pasarse a una unidad de análisis y la tecnología involucrada es muy simple y barata. En este sentido la protección involucra tanto la encripción como el control de acceso físico al cableado. Un elemento importante es controlar el acceso al cableado dentro del edificio o el ambiente local. Si el ambiente deja que la señal esté sujeta al control de acceso físico, la seguridad no es posible sin la encripción.

Las señales transmitidas a través de cable coaxial son mucho más difíciles de interceptar ya que las emisiones magnéticas del cableado son muy bajas y una intervención actualmente involucra romper el cable e instalar algún otro dispositivo. Tal acción es mucho más fácil de detectar que la simple colocación de un detector cerca de una línea de par trenzado. La protección se logra por medio del control de acceso físico al cableado y el monitoreo electrónico continuo para asegurar que las características del cable no cambian y reflejan la posible instalación de una intervención.

El uso de cable de fibra incrementa significativamente la resistencia de una red a ser intervenida debido a que es muy difícil romper el cable para instalar un aparato de intervención, contrario al cable coaxial; y se requiere equipo especializado para instalar un aparato de intervención y hacer uso de la señales interceptadas. Puesto que las señales en el cableado de fibra óptica están en la forma de pulsos de luz de láser, las emisiones electromagnéticas que podrían usarse para intervenir la línea son esencialmente inexistentes.

En el análisis de tráfico, un penetrador no necesita saber el contenido de los datos, su interés podría ser quién envió a quién y cuando. Por ejemplo, el gerente de contabilidad para una firma local que tiene contacto telefónico regular con bancos suizos y con

conocidos corredores de apuestas es un riesgo potencial de seguridad. De manera semejante, los mensajes encriptados a los destinos conocidos pueden producir eventos específicos; el análisis de tráfico puede determinar quién envió los mensajes que causaron los eventos. El análisis de tráfico puede ser vencido enviando mensajes encriptados a los mismos destinos bajo horarios precisos para que el penetrador no puedan decir cual mensaje condujo a una serie de eventos. Esto claro, solo funciona cuando el número de originadores y destinos es fijo y pequeño.

Los ataques activos en redes son aquéllos en los que los datos dentro de la red se alteran. La alteración podría ser por la modificación de datos existentes, inserción de nuevos datos, supresión de datos existentes o replicando una señal legítima más del número de veces que la red la esperó.

Ataques tales pueden burlar la seguridad y lograr la penetración. Por ejemplo, la secuencia de acceso de un usuario legítimo podría modificarse para conectar a otro usuario simultáneamente, una secuencia de acceso legítima podría ser replicada por un penetrador, un comando de final de sesión podría ser borrado, un comando de final de sesión podría cambiarse por una secuencia de acceso insertada, o una secuencia de acceso podría ser insertada en un enlace establecido.

La protección contra los ataques activos involucra el trío estándar de prevención, detección y reacción. Los controles de acceso y los controles físicos (como el uso de cable coaxial o de fibra óptica), hacen más difícil que un penetrador inserte datos en la red. El uso de varias formas de encripción y autenticación incrementan la dificultar para que un penetrador modifique o inserte datos exitosamente.

3.5.3. Emisiones electrónicas

Los sistemas de información que emplean dispositivos eléctricos y electrónicos son expuestos a varios riesgos de seguridad, accidental e intencional. Estos riegos incluyen:

- Fallas de energía

- Ruido y otras RFI (interferencias de radio frecuencia, incluyendo EMP[14])
- Emanaciones

El profesional de seguridad debe estar consciente de que incluso el equipo eléctrico y electrónico relativamente simple está sujeto a riesgos de emanación. En muchos casos, el equipo necesario para realizar tal intervención electrónica es bastante simple y barato. Un receptor de microondas simple dentro de varios kilómetros de un enlace satelital detecta, y posiblemente registra para después procesar, señales enviadas vía satélite a cualquier usuario de la estación receptora. Los platos de televisión satelital pueden comprarse por menos de lo que uno se imagina, esto permite ilustrar la disponibilidad de sistemas completos para interceptar y procesar señales satelitales. En otros casos, por ejemplo con transmisión del láser aéreo, la interceptación y procesamiento es mucho más difícil; sin embargo, cualquier transmisión de señales sólo puede ser considerada segura cuando se hace uso efectivo de herramientas de encripción de alta calidad.

3.5.4. Comunicaciones

Las comunicaciones como valor-agregado se refieren al producto de una compañía de telecomunicaciones que adquiere infraestructura de comunicaciones y entonces agrega algún valor, por ejemplo proveyendo una forma de acceso más fácil, insertando rutinas de corrección de errores, compartiendo entradas a servicios de información, etc.

Los ejemplos de redes de valor-agregadas incluyen *Datapac* en Canadá, *iNet 2000* en Canadá y los Estados Unidos, *Tymnet* y *Telenet* en los Estados Unidos, *JANET* en el Reino Unido, *EARN* (Red de Investigación Académica Europea) en Europa, y otros. Los servicios comerciales ofrecen correo electrónico, otra clase de servicios y acceso a todo lo que de compras de programas en línea, bibliotecas y periódicos, se refiere (se han registrado más de 3,000 redes de valor-agregado a partir de enero de 1990).

[14] ElectroMagnetic Pulse.- Pulso Electromagnéticos.

Estándar de comunicaciones OSI

Las características físicas de dispositivos de transmisión y los medios de comunicación sirven para limitar y mejorar la habilidad de comunicar vía digital, voz y recursos de vídeo. La transmisión de banda base (no modulada) es aquella que se toma como la tecnología de comunicación de computadora a periférico, y su uso se limita a la transmisión de datos digitales (como con la transmisión de fibra óptica). La tecnología de banda ancha es más difícil de implementar y controlar en un ambiente cambiante, además de ser más costosa; sin embargo, ésta aún sirve como un medio para el manejo de la voz, televisión y datos digitales.

En los años ochentas y noventas, se han concentrado los esfuerzos de la Organización de Estándares Internacionales (ISO por sus siglas en inglés), para establecer un estándar universal de comunicaciones llamado *Open Systems Interconection* (OSI), que permite acabar con las más grandes dificultades encontradas en la tercer y cuarta capa del modelo de comunicaciones utilizando el protocolo TCP, siendo de hecho el estándar más usado.

La Organización de Estándares Internacionales (ISO) se fundó en 1946 con 25 países de miembros de una carta constitucional. Hoy, el centro de operaciones está en Ginebra, Suiza; y comprende grupos de normas nacionales de 89 países. El ISO ha estado trabajando en grupos enfocados a los estándares de comunicaciones durante muchos años.

Para una mejor referencia, la tabla 3.10 resume las siete capas del modelo de comunicación. La siete capas están consideradas en dos grupos funcionales, "la plataforma de servicio de la aplicación" (capas 5 a 7) y la "plataforma de servicio de transporte" (capas 1 a 4). La función de la plataforma de servicio de transporte es recibir datos libres de error de un sistema a otro; el papel de la plataforma de servicio de aplicación es interpretar el flujo de dígitos binarios y presentarlo al usuario en una forma que tiene sentido para él. Estas capas se ilustran gráficamente en la figura 3.11.

Capa	Nombre	Propósito
1	Física	La transmisión del flujo binario al medio de la transmisión.
2	Enlace de datos	La transferencia de unidades de información al otro extremo de un enlace físico, es responsable de la integridad de los datos.
3	Red	Intercambio y ruteo de información.
4	Transporte	La integridad de datos de extremo-a-extremo y calidad de servicio; arma y desarma paquetes de datos para la Capa 3.
5	Sesión	La coordinación de interacción entre los procesos de extremo-aplicación; el lenguaje inglés traducido a tecnología de red.
6	Presentación	La conversión de código y formateo de datos; estándares de terminales y reglas de despliegue
7	Aplicación	La aplicación y contenido de la información desplegada en Capa 6.

Tabla 3.10. Modelo de Referencia ISO para interconexión de sistemas abiertos (OSI).

Protocolos de seguridad ISO/OSI

En 1989, se publicó la segunda parte de los estándares ISO/OSI que incluye la norma de seguridad 7498-2. No es apropiado reproducir el estándar en este documento, pero los practicantes de seguridad de la información deben saber lo que se encuentra en la sección 7498-2 y se recomienda consultar a la propia norma para detalles. Aquí se presenta un bosquejo de los servicios de seguridad y mecanismos de seguridad incluidos en la arquitectura de OSI, y su relación con las siete capas del modelo OSI mostradas en la figura 3.11.

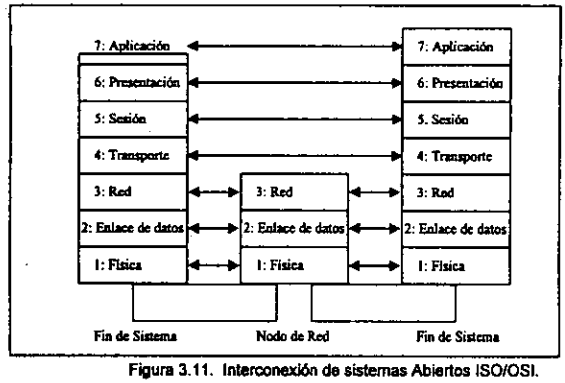


Figura 3.11. Interconexión de sistemas Abiertos ISO/OSI.

Servicios de Seguridad

Los servicios de seguridad básicos que serán proporcionados por mecanismos que pueden cubrir varios servicios y su ubicación en la arquitectura variará de instalación a instalación. Hay cinco grupos de servicios, con subclasificaciones en algunos casos, éstos son:

1. Autenticación, incluyendo:
   - Autenticación de entidades iguales
   - Autenticación de origen de datos
2. Controles de acceso
3. Confidencialidad de los datos, incluyendo:
   - Confidencialidad de conexión
   - Confidencialidad de desconexiones
   - Confidencialidad del campo selectivo
   - Confidencialidad de flujo de tráfico
4. Integridad de los datos, incluyendo:
   - Integridad de conexión con recuperación
   - Integridad de conexión sin recuperación
   - Integridad de conexión de campo selectivo

- Integridad de desconexión
- Integridad de desconexión de campo selectivo

5. No cancelación, incluyendo:
   - No cancelación con prueba de origen
   - No cancelación con prueba de entrega

Mecanismos de Seguridad

De igual forma, existen ocho mecanismos que pueden incorporarse dentro de la(s) capa(s) apropiada(s) para proporcionar los servicios mencionados con anterioridad, estos mecanismos son:

1. Encripción
2. Firma digital
3. Control de acceso
4. Integridad de los datos
5. Autenticación de intercambio
6. Flujo de tráfico
7. Control de ruteo

Mecanismos de Seguridad Penetrantes

Actualmente cinco mecanismos se clasifican como "los mecanismos de seguridad penetrantes", y son aquéllos que no son específicos a cualquier servicio particular dentro del estructura de OSI, éstos son:

1. Funcionalmente confiable
2. Etiquetas de seguridad
3. Detección de eventos
4. Pistas de auditoría de seguridad
5. Recuperación de seguridad

La relación entre los servicios y mecanismos es ilustrada en la tabla 3.12.

Servicios \ Mecanismos	Encriptamiento	Firma digital	Control de Acceso	Integridad de los datos	Autenticación de intercambio	Flujo de tráfico	Control de ruteo
Autenticación de entidades iguales	Y	Y	*	*	Y	*	*
Autenticación de origen de datos	Y	Y	*	*	*	*	*
Controles de acceso	*	*	Y	*	*	*	*
Confidencialidad de conexión	Y	*	*	*	*	*	*
Confidencialidad de desconexiones	Y	*	*	*	*	*	*
Confidencialidad de campo selectivo	Y	*	*	*	*	*	*
Confidencialidad de flujo de trafico	Y	*	*	*	*	Y	*
Integridad de conexión con recuperación	Y	*	*	Y	*	*	*
Integridad de conexión sin recuperación	Y	*	*	Y	*	*	*
Integridad de conexión de campo selectivo	Y	*	*	Y	*	*	*
Integridad de desconexión	Y	Y	*	Y	*	*	*
Integridad de desconexión de campo selectivo	Y	Y	*	Y	*	*	*
No cancelación con prueba de origen	*	Y	*	Y	*	*	Y
No cancelación con prueba de entrega	*	Y	*	Y	*	*	Y

Y: Sí, se considera que el mecanismo es apropiado, por si solo o en combinación con otros mecanismos

*: Se considera que el mecanismo no es apropiado

Tabla 3.12. Relación entre Servicios y mecanismos.

En la tabla 3.13, todos lo servicios se indican con una "Y" para la capa siete, la capa de la aplicación. Se espera que las aplicaciones (como sistemas operativos, por ejemplo) proporcionen alguna medida de seguridad por sí mismas.

Servicios \ Capas	Capa Física	Capa de enlace de datos	Capa de Red	Capa de transporte	Capa de presentación	Flujo de tráfico	Capa de aplicación
Autenticación de entidades iguales	*	*	Y	Y	*	*	Y
Autenticación de origen de datos	*	*	Y	Y	*	*	Y
Controles de acceso	*	*	Y	Y	*	*	Y
Confidencialidad de conexión	Y	Y	Y	Y	*	*	Y
Confidencialidad de desconexiones	*	Y	Y	Y	*	*	Y
Confidencialidad de campo selectivo	*	*	*	*	*	*	Y
Confidencialidad de flujo de trafico	Y	*	Y	*	*	*	Y
Integridad de conexión con recuperación	*	*	*	Y	*	*	Y
Integridad de conexión sin recuperación	*	*	Y	Y	*	*	Y
Integridad de conexión de campo selectivo	*	*	*	*	*	*	Y
Integridad de desconexión	*	*	Y	Y	*	*	Y
Integridad de desconexión de campo selectivo	*	*	*	*	*	*	Y
No cancelación con prueba de origen	*	*	*	*	*	*	Y
No cancelación con prueba de entrega	*	*	*	*	*	*	Y

Y: SI, el servicio debe incorporarse para la capa como una opción del proveedor.

*: No proporcionado

Tabla 3.13. Relación entre los servicios y capas de OSI.

Red digital de servicios integrados (ISDN)

ISDN es una arquitectura de red que usa tecnología digital para apoyar servicios integrados que usan líneas telefónicas de par trenzado y es bastante compatible con ISO/OSI. El principio es que todo los servicios de comunicación actualmente disponibles no estarán habilitados por circuitos separados pero si por un solo enchufe en la pared. Tales servicios incluyen: voz, circuitos de comunicaciones y comunicaciones de paquetes de datos, circuitos de intercambio, servicios correo y facsímil. Los usos propuestos incluyen: correo de voz, la combinación de voz y transmisión del datos en una línea, identificación de algún visitante y estadísticas en progreso como tiempo y costo. La integración de dichos servicios permitirá otras aplicaciones como la telemetría de una casa (por ejemplo, para los sistemas de seguridad y el control del medio ambiente).

Otras ventajas incluyen una libertad relativa del ruido y interferencia debido a la señal digital y accesar a muchos servicios diferentes a través de una sola línea y un número pequeño de interfaces. Los estándares para ISDN del CCITT son los estándares de series I; ISDN ocupa las tres capas más bajas de la estructura del ISO/OSI (física, enlace de datos y red).

IEEE 802

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) instituyó el proyecto 802 en febrero de 1980, en el cual se definieron los estándares para las redes de área local. IEEE 802 consiste en seis normas:

- 802.1, Define la relación con ISO/OSI.
- 802.2, Define el control del enlace lógico.
- 802.3, Acceso CSMA/CD[15].
- 802.4, Acceso por señal de bus.

[15]Carrier Sense Multiple Access with Collision Detection.- Portadora de accesos múltiples con detección de colisiones.

- 802.5, Acceso por señal de anillo.
- 802.6, Acceso a red de área metropolitana.

Para 1988, de la 802.2 a la 802.5 habían sido aprobadas por la comisión de estándares de la IEEE.

- *802.2, Control de enlace lógico:* La norma 802.2 de IEEE define protocolos para una o más conexiones lógicas para un solo medio. Cada estación asignada al medio usa un medio de comunicación común para el método de acceso. Los procedimientos de control son similares al protocolo X.25 de la CCITT.

- *802.3, Acceso CSMA/CD:* Cuando se conectan estaciones múltiples a un solo portador, existe la posibilidad de que más de una estación esté transmitiendo simultáneamente. La transmisión simultánea sin algún método de compensación produciría interferencia de señal. Un método de compensación requiere que la estación asegure que el medio está libre; esto es CSMA/CA[16] (Anulación de la colisión). Ethernet usa CSMA/CD, y las colisiones son detectadas tomándose las medidas para asegurar que la retransmisión ocurra, en un horario durante el cual el medio se encuentra libre.

La tabla 3.14 resume las características esenciales de la IEEE 802.3, y la figura 3.15 ilustra la relación entre las capas del modelo OSI y la IEEE802.3.

- *802.4, Acceso por señal de bus y 802.5, Acceso por token ring*: El uso de un medio compartido puede ser coordinado por el paso de una señal y puede conferirse el derecho para controlar la red momentáneamente a la estación que recibe la señal. La topología de la red no es relevante para la estación individual debido a que la señal simplemente sigue la red a lo largo de cualquier topología proporcionada y en todos los casos la señal pasa en la dirección de cada estación en orden descendente. El estándar de red de área local *token ring* de IBM, es un ejemplo significativo de IEEE 802.5, otro ejemplo es NetWare de Novell.

[16] Carrier Sense Multiple Access with Collision Avoiddance.- Portadora de Accesos Múltiples con Anulación de Colisiones.

	10Base5 (Estándar Ethernet)	10Base2 (Ethernet delgado)	10*mplia36 (Ethernet banda amplia)	1Base5 (LAN-Estrella a 1MB)
Ancho De banda	10 Mbps	10 Mpbs	10 Mpbs	1 Mpbs
Medio de comunicación	Cable coaxial grueso	Cable coaxial delgado	Cable coaxial de Televisión	Cable par trenzado
Distancia	500 metros	200 metros	3.6 km	500 metros
Topología	Bus	Bus	Bus	Estrella

Tabla 3.14. Visión global de la IEEE 802.3.

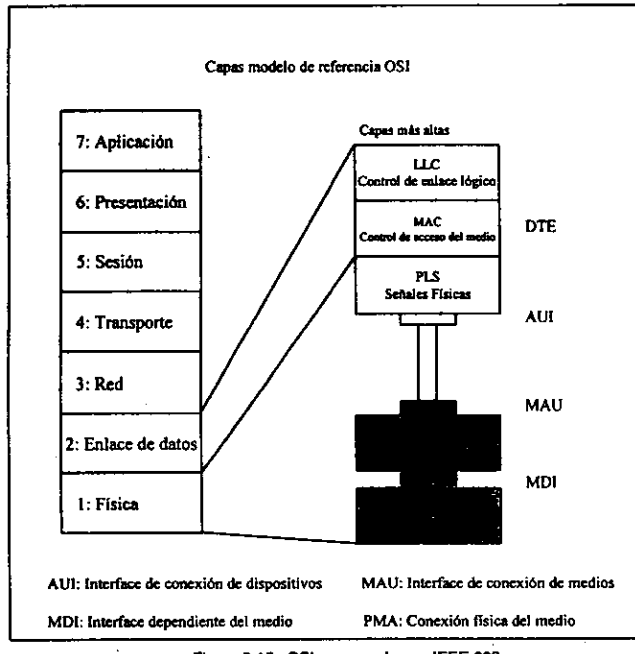


Figura 3.15. OSI comparado con IEEE 802.

3.5.5. Diseño de red

En esta sección se comparan las ventajas y desventajas de las tres topología de red básicas (bus, estrella y anillo) y sus variantes; en la figura 3.16 se muestra a manera de tabla y en forma resumida esta comparación.

La tecnología de bus primaria en uso es IEEE 802.3, y un ejemplo muy significativo ha sido *Ethernet*, que es un sistema de contención cuyo modo de operación es CSMA/CD. Una muy buena Red de Área Local (LAN) *Ethernet* puede degradarse rápidamente dentro del 50% de la retransmisión para cada dispositivo en el bus por intervalos cortos de tiempo. El sistema 802.3 es efectivo y tan extenso como la mayoría de los dispositivos que no son dependientes de su comunicación con otros dispositivos en el bus (a excepción de algunos dispositivos de impresión).

Topología	Ventajas	Desventajas
Bus	Medio de transmisión pasivo. Impacto de falla localizado. Utilización adaptable.	Técnica de acceso de canal.
Estrella	Simplicidad. Ruteo central. Decisiones de no ruteo.	Seguridad del nodo central. Carga de nodo central.
Anillo	Simplicidad. Retardos predecibles. Decisiones de no ruteo.	Modos de falla con *efecto global*: • Falla del nodo. • Regeneración de la señal.

Figura 3.16 Tabla de comparación de topologías de red.

Redes en estrella

Las redes de estrella o descentralizadas son aquellas en las cuales el procesamiento primario es realizado en un nodo central, con todos los nodos remotos unidos a ese nodo central. Los nodos pueden ser terminales, estaciones de trabajo inteligentes u otras computadoras.

Redes Jerárquicas

Las redes jerárquicas son aquellas en las que se unen computadoras en una jerarquía, creando una habilidad computacional esencialmente distribuida. Las jerarquías pueden formar parte de una red central (estrella) o también pueden ser interconectadas en una configuración de anillo o en una combinación de ambos.

Redes de anillo

La red de anillo es una serie de computadoras totalmente-conectadas o nodos de grupos de computadoras, formando un circuito cerrado. Las redes de anillo pueden ser graficadas como nodos unidos para formar un círculo o bien, pueden formar un círculo con conexiones cruzadas. Con la interconexión completa, la red anillo permite el funcionamiento completo de todos los otros nodos si un nodo queda inoperante.

Redes de Área Local

Las redes de área local (LAN) operan con una gran cercanía geográfica y se caracterizan porque no dependen de una computadora central, pudiendo configurarse tanto con terminales inteligentes como con terminales tontas.

3.5.6. Sitios de ataque

Existen varios puntos de vulnerabilidad en cualquier red de telecomunicaciones, en la figura 3.9 se ilustraron la mayoría de ellos. Dependiendo de su dispersión, también una red local puede compartir muchos de estos puntos de ataque, sin tomar en cuenta aquellos que se relacionan con radio enlaces o el uso de infraestructura de servicio público.

Generalmente un ataque puede hacerse a cualquier tecnología empleada en una red o en sus puntos finales, donde una tecnología se une con otra (por ejemplo, intervenciones a lo largo del cableado o en las terminales donde el par trenzado se conecta a un PABX), por lo que las amenazas o riesgos se relacionan más con el tipo de información dentro de un canal y con características del canal que con cualquier otro factor.

Es fácil intuir que los puntos de ataque a una red pueden estar relacionados con cualquier componente o dispositivo conectado a la misma; y que, dependiendo de la topología utilizada, pueden limitarse algunos riesgos; sin embargo, sigue siendo válida la recomendación de poner especial atención en puntos y riesgos ya identificados, tales como:

- Terminales o estaciones de trabajo.
- Equipos de interconexión o enlace (modems, pad, routers, etc...).
- Medios de conexión (par trenzado, coaxial, etc..).
- Gabinetes o tableros de conexiones.

Los enlaces entre elementos de una red están expuestos a ataques de comunicaciones activos y pasivos; sin embargo, las características de vulnerabilidad de par trenzado, cable coaxial, fibra óptica y radio enlaces ya fueron discutidos en una sección anterior; por lo que aquí solamente se vuelven a señalar para destacar que, aunque la red puede encerrarse en una zona de máxima seguridad, es esencial un mecanismo de encripción de probada eficiencia para la transmisión de señales que pasan a través de estos medios. Esto último puede evitarse sólo en el caso remoto de que el o los enlaces y el resto de la red pueden ser controlados de alguna otra forma. Algunos ejemplos de tales controles podrían incluir *bunkers* subterráneos o aeronaves, en los que el control administrativo ofrece un alto grado de seguridad, el personal es confiable y la seguridad del perímetro es relativamente fácil de preparar y sumamente difícil de penetrar. En caso de que no se pueda lograr semejante perímetro de seguridad, se deben implementar, como ya se mencionó, mecanismos de encripción de señales combinados

con firmas digitales y esquemas de verificación globales a todos los posibles puntos de penetración para, de esta forma, asegurar un nivel de protección razonable.

3.6. Seguridad en programas de aplicación

Un factor que afecta bastante, en lo que a sistemas de información se refiere, son las aplicaciones mal desarrolladas o que tiene serios problemas de desempeño y que provocan grandes pérdidas a las organizaciones. La seguridad en programas de aplicación se refiere a los controles que son incluidos en los programas desarrollados para algún uso particular, incluyendo la estructura para soportar la separación de obligaciones, la segregación de funciones, revisiones, conciliaciones, confirmaciones y otra acciones; también se contemplan bitácoras, hojas de control y otros registros permanentes. De igual forma se incluyen algunas definiciones básicas, además de las complementarias que se podrán encontrar en el apéndice A.

3.6.1. Controles de software: Desarrollo

Existen dos problemas reales en el desarrollo de aplicaciones, los *bugs* y los errores humanos. En donde los b*ugs* son cosas que se encuentran mal en los sistemas de información, el término *bug* de computadora ha sido atribuido a un técnico que encontró una polilla muerta aplastada entre los contactos de una computadora digital muy antigua y que había causado un mal funcionamiento de la misma. En esencia, existen dos razones por las cuales los sistemas de información tienen *bugs*, éstas son:

- Las especificaciones están mal.
- La aplicación no iguala a las especificaciones.

Las exposiciones de seguridad más grandes son los errores y la falta de entrenamiento, es decir, cuando un analista de sistemas comete un error describiendo el sistema

propuesto o cuando un usuario se olvida de que un elemento crítico es aparentemente insignificante, puede tener como consecuencia un *bug* del sistema; o bien, cuando un programador escribe el código mal, por error, éste es también un *bug* de programa (una sintaxis o error de aplicación). Si todos los analistas de sistemas fueran perfectos y todos los programadores siempre escribieran código perfecto y todos los usuarios realmente supieron exactamente lo que ellos necesitan, entonces ahí puede no haber ningún *bug*. En el mundo real, nadie es perfecto y pueden ocurrir los errores.

En negocios que procesan grandes volúmenes de información, hasta el 85 % de los recursos se dedican al mantenimiento de programas, que incluyen: el cambio de programas derivados de nuevos requerimientos y/o cambio de circunstancias operativas. Muchos mantenimientos, desafortunadamente, consisten en la corrección de problemas que no debieron haberse permitido que ocurrieran en un principio.

Desde un punto de vista de seguridad y control, la mejor idea es evitar tener errores en todos los sistemas o programas y el mejor momento para efectuar esto es lo más pronto posible en el proceso de desarrollo; el corregir un error de diseño del sistema pueden costar sencillamente hasta 1,000 veces más durante el periodo de mantenimiento que durante el diseño y antes de que cualquier código sea escrito.

Principios generales de ingeniería de *software*

Dos principios básicos son la base del *software* bien construido: estratificación y modularidad, donde la estratificación es el principio de construir procesos en capas para que cada capa se encargue de un tipo de actividad específica. El lenguaje estructurado de computadora utiliza una forma de estratificación (el concepto de datos ocultos o globales contra las variables locales que llegan a actuar en esta instancia). Las característica técnicas formales forman una capa entre las política de seguridad, el modelo de seguridad y la aplicación. En este caso el problema es seleccionar la estratificación para que cada capa sea lo suficientemente concisa y clara para permitir una prueba convincente, ya que cada capa es relativamente cerrada a la siguiente en cantidad de detalle y para que la correspondencia de capa a capa pueda ser

demostrada. Otro ejemplo de estratificación son los protocolos de ISO/OSI y los estándares de seguridad asociados; ahí, la estratificación está basada en las características físicas y lógicas de los recursos de comunicaciones.

La modularidad se refiere a dividir las actividades en segmentos bastante pequeños de piezas individuales, que son comprensibles y razonablemente pueden sujetarse a pruebas de exactitud o comprobaciones exhaustivas. Un ejemplo se encuentra en el diseño de compiladores, donde típicamente la sintaxis del lenguaje se describe en términos matemáticos y un módulo se crea para cada elemento primitivo en la descripción formal.

Métodos estructurados

Una aplicación de los principios generales de estratificación y modularidad apenas discutida es el análisis estructurado y la programación estructurada que fueron desarrolladas en lo años 70s por Constantine y Yourdon, entre otros. Ellos usaron diagramas de flujo de datos y la consideración de ciertas características matemáticas de la gráficas formadas por los diagramas de flujo de datos para deducir principios que, si se siguen, reducirán las posibilidades de insertar *bugs* en los sistemas y programas, además de minimizar los problemas eliminándolos cuando son descubiertos.

En esencia, el análisis estructurado involucra la identificación de actividades realizadas por una organización y el flujo de los datos que manejan esos procesos (no es el mismo que el término técnico usado anteriormente sobre la seguridad en sistemas operativos). Los programas se escriben usando código modular que corresponde a los procesos (a un mismo nivel detallado, por supuesto), y usando el diccionario de datos desarrollado. Los módulos, en sistemas o en programas, no deben afectar, debiendo ser lo bastante autónomos como para realizar una sola función lógica.

Librerías de programas

Una herramienta, que ayuda a controlar a los intrusos y a los cambios no autorizados de los sistemas bajo desarrollo, es el uso de librerías de programas que normalmente

están contenidas en la computadora, y en donde se puede tener a algún administrador responsable de asegurar que las librerías de programas se mantengan y se controlen según las políticas y procedimientos apropiados.

Todas las copias de los diccionarios de datos, programas, módulos de carga y documentación deberían estar bajo el control de librerías de programas. El administrador responsable de dichas librerías debe asegurar que los programas no sean adicionados a la biblioteca de producción hasta que sean probados y autorizados propiamente. Los programadores no deben permitir el acceso a los programas de producción, sólo el responsable del programa debe poder alterar cualquier programa de producción.

Diccionario de Datos como control

Cuando los programas están en vías de desarrollo, los programadores pueden desear, o se esfuerzan para inventar nombres para los elementos de los datos que son comunes entre varios programas. El diccionario de los datos, como parte de un sistema administrador de la base de datos o como parte de una librería de programas, es una lista de cada elemento de los datos con sus respectivas características; es decir, es una referencia cruzada que permite conocer qué programas usan tal o cual elemento de los datos, qué archivos están ahí y algunos otros datos similares.

El diccionario de datos sirve como un control, particularmente en conjunto con librerías de programas, cuando los programadores requieren usar nombres de variables desde una librería de programas. Esto asegura que todos los programadores usen el mismo nombre (permitiendo realizar cambios a un elemento fácilmente, quizás automáticamente en muchos programas escritos por personas diferentes), y donde existe un control sobre la creación de nuevos nombres (el responsable de los programas).

Conversión e Implementación

Cada nuevo sistema que debe ser implementado requiere de la conversión de datos, a veces de muchos datos, en el formato acostumbrado en un sistema anterior o en un nuevo formato para el nuevo sistema.

Deben revisarse los controles que aplican a los datos antes del proceso de la conversión y mantener los controles equivalentes durante la conversión. Los datos introducidos en el nuevo sistema deben estar tan completos y exactos como estaban antes de ser convertidos y los nuevos datos deben mantener la integridad del sistema anterior (al menos; idealmente el nuevo sistema tendrá estándares mayores).

3.6.2. Controles de software: Mantenimiento

El mantenimiento programando involucra la producción cambiante de programas para arreglar sus errores y la modificación de programas para producir resultados diferentes por muchas razones (nuevos requerimientos, por ejemplo). Por lo que, para mantener el control sobre la seguridad del sistema se necesita alguna separación de responsabilidades, como la siguiente:

- Los operadores no deben ser programadores y no deben poder cambiar programas.
- Los programadores no deben poder cambiar los programas que se encuentran en producción directamente.
- Los analistas de los sistemas normalmente no necesitan tener acceso en absoluto a los programas, particularmente los programas de producción.
- Los usuarios no deben tener acceso al centro de cómputo o a los programas.

Controles de prueba

Todos los cambios a cualquier sistema de producción necesitan ser probados y la administración de usuarios tiene la responsabilidad de velar por los datos de la organización, por lo que se requiere una adecuada administración del usuario para

cerrar el ciclo con los resultados de las pruebas. El responsable de los programas debe mantener los datos de las pruebas usados durante la aplicación del sistema que era la base para el establecer la aceptación del usuario; este banco de datos de prueba puede usarse para probar modificaciones y estar seguro que el sistema trabaja como se pensó después de los cambios. Las pruebas nunca deben hacerse con datos o archivos de producción o en una corrida en paralelo, por lo que debe usarse una copia separada que contenga los archivos maestros en lugar de las versiones que se encuentran en producción. Algunas organizaciones tienden a tener un equipo especial para sus pruebas de desarrollo o alquilar cierto tiempo de proceso de máquina.

Control de cambios

Uno de los métodos más comunes para arreglar sistemas ha sido insertar código en los programas de producción que hacen alguna otra cosa diferente a lo que se supone que el programa hace (disminuir el balance de una cuenta de préstamo de una persona o aumentar el balance de la cuenta verificada, por ejemplo). Así que es necesario establecer un mecanismo de control de cambios para asegurar que todos los cambios son: autorizados, probados y registrados.

Como se mencionó anteriormente, los programadores no deben tener acceso a los programas de producción, ni debe permitírseles hacer cambios sin los apropiados registros y autorizaciones. La mejor manera de asegurar esto es usar una librería de programas y un responsable de dichas librerías, además de las bitácoras apropiadas y las formas de aprobación. Se deben de registrar y autorizar cosas como: petición del cambio, ejecución del cambio, documentar el cambio con comentarios en los programas, manuales, instrucciones de operación y dondequiera que sea necesario; pruebas del cambio, modificación del programa de producción, etc.

En algunas organizaciones no se permite a los programadores iniciar requerimientos de cambios, ya que el requerimiento debe venir del usuario. Esto puede ser incómodo, pero proporciona un nivel de control excelente.

Idealmente, el proceso de cambio debe ser un proceso similar al proceso de desarrollo de sistemas. El proceso de desarrollo incluye una propuesta del proyecto, un estudio de viabilidad, análisis alternativo, diseño del sistema, diseño de programas y construcción, pruebas, aprobación, aplicación y seguimiento. Un cambio a un sistema existente necesita ser tratado con el mismo cuidado, aunque pueden abreviarse algunos elementos del proceso de diseño del sistema completo.

3.6.3. Garantía

La garantía es el proceso por el que una autoridad apropiada certifica que un sistema reúne ciertas especificaciones, este proceso puede involucrar uno o varios de los siguientes factores:

- Integridad
- Comprobación
- Verificación y especificación
- Manejo de facilidades
- Manejo de la configuración
- Planes de desastre y contingencia
- Grados de confianza

3.6.4. Especificación formal y verificación

El estratificación involucrada para la creación de un sistema seguro incluye políticas (una consideración externa, expresada formalmente o informalmente); tales como el modelo de seguridad, la especificación formal, la verificación y la implementación. Esta sección trata de la especificación formal y de la verificación.

Usualmente los métodos de especificación formal y verificación son aplicados principalmente al diseño de software para sistemas. La razón es que hay una gran cantidad de esfuerzos que se requieren para especificar y verificar cualquier software

de tamaño realista. Ha sido necesario aplicar dichas prácticas a software de sistemas una vez que las fallas o la falta de seguridad afecta todo lo demás. De hecho, la especificación y la verificación son medios para garantizar al máximo que el software de los sistemas funciona como se desea.

Cuando un programa de aplicación se aproxima a la complejidad y a la naturaleza de un sistema operativo completo, los métodos formales se vuelven más justificables. Un sistema manejador de base de datos (DBMS) puede ser un ejemplo semejante de un programa de aplicación, debido a que el DBMS tiene esencialmente la responsabilidad de manejar todos los datos en un sistema y proporciona una consulta muy sofisticada, programación y capacidades de administración; para muchos usuarios, el DMBS es el sistema operativo.

3.6.5. Seguridad en sistemas de base de datos

Un sistema manejador de base de datos (DMBS) es un programa de aplicación, sin embargo, un DBMS es considerado a menudo como "más que una aplicación." Esto es porque el DBMS esencialmente tiene la responsabilidad para manejar todos lo datos en un sistema y a la vez provee de una gran capacidad de consulta, programación y capacidades de administración de datos.

Un DBMS proporciona normalmente algunas cosas como un lenguaje de consulta, un generador del reportes, un lenguaje para especificar la estructura de la base de datos y la manera cómo los elementos de los datos serán guardados y recuperados. Típicamente, estos lenguajes permiten la capacidad de programación para soportar consultas sofisticadas, reportes o afinación de la estructura del DBMS. El propósito básico de un DBMS es el colectar los datos de una organización dentro de un formato que permita hacer referencias cruzadas, minimizar la duplicación de la información y, generalmente, optimizar el uso y los acceso a los datos de la organización. Para la mayoría de los usuarios y a menudo incluso para el administrador de la base de datos, el DBMS es el único componente del sistema operativo que ellos necesitarán o usarán.

En los ambientes de bases de datos, el DBMS realiza o contempla internamente ciertas funciones que garantizan que dicho manejador se mantiene lo más seguro posible, por lo que también se consideran algunos factores que puedan afectar al DMBS; y esto se debe a que si no existen tampoco los controles a nivel del sistema operativo es posible que los sistemas de información puedan verse afectados, así como la información contenida en ellos. Se han identificado una serie de elementos que se podrían considerar como amenazas para el DBMS, entre ellas se encuentran:

- Descubrimiento directo de los datos
- Modificación no autorizada de los datos
- Contaminación de los datos
- Agregación
- Caballos de Troya y otros códigos maliciosos
- Canales secretos o escondidos

Controles de acceso

Muchos DBMS's proveen sus propios controles de acceso a diferentes niveles de aplicación, incluyendo el control de la contraseña para identificar a los usuarios. Algunos permiten la definición de capacidades permitidas a los usuarios y el control subsecuente a mayores o menores niveles de granularidad de tales accesos.

Una base de datos tiene inherentemente una granularidad equivalente por lo menos al nivel de los elementos de los datos individuales. Esto significa que los accesos y otros controles pueden ser aplicados a un nivel muy detallado, inclusive mucho más que un sistema administrador de archivos tradicional.

Controles de DBMS

Como se ha mencionado, la mayoría de los DBMS's proporcionan un segundo nivel de identificación del usuario y autenticación, además de cualquier otro control que pueda ser proporcionado por el sistema operativo. Generalmente, ésta es una facilidad simple

de identificación y contraseña, pero podría ser tan sofisticado como cualquier otro esquema de identificación/autenticación.

Debido a la granularidad fina inherente a un DBMS, es posible asignar etiquetas a los elementos de los datos individuales. Si esto se hace, y si el proceso de identificación incluye información de clasificación del usuario, entonces el DBMS puede controlar el acceso por usuarios individuales a los elementos de los datos individuales.

Existen diversos controles en el DBMS que proporcionarán una garantía de seguridad y, en aquellos ambientes en donde el riesgo o probabilidad de ataques o penetraciones es muy alto, los controles son definidos como:

- Controles de acceso
- Controles de Inferencia
- Controles de cuentas
- Controles de identificación y autenticación
- Controles de Auditoría

Cuestiones de diseño de un DBMS

El propósito de un DBMS es proporcionar acceso fácil a una gama amplia de datos corporativos y la razón básica para agregar esta capacidad es que el DBMS, inherentemente con los elementos de los datos a un nivel alto de granularidad, pueden aplicar controles individuales a los usuarios individuales y a los elementos de los datos (a un precio en el uso de almacenamiento y rendimiento). Por otra parte, las reglas para crear sistemas operativos confiables aplican igualmente para crear un DBMS confiable.

Algunas reglas de protección para que los DBMS's tengan un desempeño y funcionalidad apropiado son:

- *Kernel* confiable
- Filtros confiables
- Encripción

- Rendimiento
- Almacenamiento
- Garantías

3.6.6. Controles de integridad

Un problema que debe valorarse es el equilibrio entre el control de accesos y la integridad de los datos, y esto no es porque los dos sean de alguna forma incompatibles, más bien, mucha de la atención a la seguridad de las computadoras se ha invertido en la preocupación por el acceso y el descubrimiento de la información. Por ejemplo, el TCSEC[17] (*Orange Book*) es un esquema de controles de acceso; y la mayoría de las aplicaciones de software de seguridad han sido en esencia paquetes de software de control de acceso.

Política de integridad

Muchos de los esquemas de control de acceso dependen de una política de seguridad para cuidar la integridad de los datos, pero como el control de acceso en el futuro se derivará de una política externa con respecto al control y descubrimiento de información, también una política de integridad debe estar basada en una política externa. En el caso del control de accesos, las políticas organizacionales, las leyes y directivas de la rama ejecutiva (en el caso del TCSEC), son la base eventual para las políticas formales, modelos e implementaciones finales.

La política de integridad no es tan confiable como el control de acceso, porque la "integridad" es considerada una virtud abstracta y la definición de lo que las palabras significan son de contexto sensible. Sin embargo, la "integridad" de la información es más que un contexto-sensible, ya que uno pudiera esperar que una política de integridad hiciera restringida mas de una aplicación. Robert Courtney describe que esa

[17] Trusted Computer System Evaluation Criteria.- Criterios de Evaluación de un Sistema de Computadora Confiable.

integridad tiene dos componentes: la calidad de los datos y la seguridad de esa calidad; la "calidad de los datos" consiste de cinco elementos:

- Exactitud
- Integridad
- Precisión
- Oportunidad
- Confidencialidad

Mecanismos de integridad

Los mecanismos para implementar una política de integridad, tales como las técnicas MAC[18], encripción, revisiones, comprobaciones, tiempos de impresión, bitácoras y pistas de auditoría pueden servir para implementar las facetas de la necesidad de asegurar los cinco elementos de calidad de datos. No obstante, si estas técnicas son incluidas en una publicación básica, como es la práctica común en la construcción de programas de aplicación, pueden pasarse por alto fallas mayores o inconsistencias. Existe una necesidad primordial dictada por un modelo para implementar una política de integridad que define cómo y cuándo deben ser incluidos tales mecanismos específicos.

3.6.7. Auditoría

El control más básico es la segregación de deberes, la cual esencialmente limita la oportunidad y tentación. La segregación de deberes puede definirse como "la separación de funciones incompatibles (dándoles los mismo deberes a dos o a más personas) para fortalecer el control interno". Las actividades de un proceso son divididas entre varias personas, de esta forma los errores cometidos por una persona tienden a ser asignados a la próxima persona en la cadena, por lo que las actividades no autorizadas requieren de la confabulación de por lo menos dos personas.

[18] Message Authentication Code.- Código de Autenticación de Mensajes

Además de esta regla básica se pueden encontrar otras reglas, en materia de seguridad, proporcionadas por personas del ambiente computacional. Estas guías ayudan a garantizar un buen control interno y a definir "las funciones incompatibles", y están definidas de la siguiente manera:

- No permitir el acceso combinado a capacidades sensibles.
- Prohibir la conversión y el encubrimiento.
- La misma persona no puede originar y aprobar transacciones.

Todos estos principios están relacionados con la separación de deberes, por lo que, en forma manual o automática, los sistemas deben ofrecer separación de deberes y responsabilidades. La definición exacta de este principio viene de los contadores profesionales y auditoría de personas. Este principio, actualmente, consta de dos partes:

- Ningún individuo solo debe tener la responsabilidad por un proceso completo de cualquier transacción o grupo de transacciones.
- La consumación de un fraude debe requerir la colusión de por lo menos dos individuos.

Los profesionales de contabilidad usan un significado, de la palabra "control", algo diferente al que usa la gente del ambiente computacional. Contadores y auditores están interesados en la protección de los recursos de una organización y asegurar que se usan los recursos de acuerdo con las intenciones de los directivos y gerentes. Cuando un contador o auditor dice "el control," normalmente se relaciona a un control interno y lo relaciona al uso de recursos y a la prevención de fraudes. Las personas desde un punto de vista computacional acostumbran la palabra "control" para relacionarla a la previsibilidad, capacidad de recuperación y calidad de un sistema de computadora. De alguna manera los usos que se le dan no son incompatibles.

Los principios del EDP en el "diseño estructurado" y "programación estructurada" son aplicaciones a nivel de detalle del principio de control y encaja bien con la modularidad necesaria. El profesional de computadoras usa principios de acoplamiento y cohesión

para expresar las mismas preocupaciones lógicas. La cohesión se refiere a la unidad interior de un programa o módulo del sistema; la cohesión alta corresponde a la alta granularidad. El acoplamiento se refiere a las interacciones entre los módulos y control de las estructuras, por lo que el acoplamiento de bajo nivel corresponde (aproximadamente) a la separación de deberes.

El programador de computadoras normalmente está trabajando a un nivel de detalle, donde las interacciones entre las personas y programas no están asociadas, o ha sido especificado por el diseñador del sistema. El análisis y diseño estructurado deben incluir consideraciones de interacciones entre las personas.

Aquellos sistemas que tienen integridad, auditabilidad y control son los únicos que cualquier profesional debe diseñar o permitir.

Auditoria de sistemas de información

No hay "principios generales de auditoría aceptados" que definan una auditoría de un EDP (como una subdisciplina dentro de la auditoría interna) o una auditoría de seguridad. Una cita de Charles Cresson Wood ilustra la situación presente, particularmente para las auditorías de seguridad: *No se han documentado los controles específicos que constituyen un estándar de cuidado debido a que no se han puesto de acuerdo con cualquier organismo oficial, aunque la investigación en la frecuencia de uso de ciertos controles de sistemas de información ha demostrado que los controles aceptados generalmente de hecho existen. Ciertas organizaciones continúan manteniendo sus propias medidas de seguridad de base de datos, pero éstas son propietarias y generalmente no están disponibles para el principiante.*

Parte del problema es que el promedio de cambios en tecnología de cómputo es mucho mayor que el promedio de los organismos oficiales. Este fenómeno no es único para auditoría; las leyes y sistemas legales enfrentan problemas muy similares.

La auditoría de un EDP está definida como el proceso de coleccionar y evaluar evidencia para determinar si un sistema de computadora salvaguarda recursos, mantiene integridad de los datos, logra metas organizacionales eficazmente y consume recursos eficientemente. Los objetivos de una auditoría están organizados alrededor de seis fases comúnmente llamadas "ciclo de vida de desarrollo de un sistema": iniciación, definición, diseño del sistema, programación y entrenamiento, evaluación y aceptación e instalación y operación.

3.6.8. Controles específicos

Los controles específicos en programas de aplicaciones varían mucho de un programa al siguiente, por ejemplo: la edición de los datos de entrada es común para todos los programas bien diseñados; sin embargo, el tipo y nivel de corrección apropiado para un programa interactivo, controlado a través de una interfase gráfica del usuario (GUI)[19], es completamente diferente del apropiado para un sistema de proceso por lotes fuera de línea. El tipo, tiempo de proceso y la naturaleza de las medidas correctivas también difieren enormemente, aunque las verificaciones de consistencia internas también son comunes en todos los programas bien diseñados; sin embargo, por su propia naturaleza, ellos pueden diferir de totalmente de una aplicación a la siguiente, o incluso de un conjunto de subrutinas a otras dentro de la misma aplicación.

Teniendo presente las advertencias ya mencionadas anteriormente, una lista de controles específicos comunes a la mayoría de los programas de aplicación podrían incluir:

- Controles de acceso (contraseñas, autenticación, capacidades, señales, controles de escritura, lectura y ejecución, etc.).
- Ediciones (sintaxis, racionalidad, verificación de rangos, verificación de dígitos, ...).
- Cuentas (transacciones totales, sumas parciales, sumas de procesos en lote, balances).

[19] Graphical User Interface.- Interfase de usuario gráfica.

- Bitácoras (quién, qué sistema, cuándo).
- Bitácoras (tiempos de impresión, antes de y después de las imágenes,...).
- Verificaciones internas (rangos de parámetros y tipos de datos, las referencias de dirección válidas y legales, códigos de terminación,...).

Con esta pequeña revisión a controles específicos se concluye el capítulo dedicado a la seguridad lógica, que tiene que ver con las medidas o controles que permiten mantener a salvo la información contenida en los equipos de proceso. Prácticamente se concluye, también, la descripción de controles, tanto físicos como lógicos, que conforman un buen esquema integral de seguridad para centros de cómputo. Sin embargo, se requiere estar preparado para afrontar situaciones en que fallen todos los controles implantados, por esta razón se incluye el siguiente capítulo, en el que se hablará de la metodología para la elaboración de un plan de acción que se utilizará en casos de contingencia que afecten al centro de proceso.

4

PLAN DE CONTINGENCIAS

A lo largo de los tres capítulos anteriores se ha subrayado que aunque se cuente con la mejor tecnología de control de acceso, aunque se construyan los centros de cómputo más protegidos y aunque se tengan las mejores herramientas de control de software, no es posible asegurar que la probabilidad de dañar los recursos informáticos pueda reducirse a cero. Siempre existirá algún riesgo no contemplado o algún penetrador los suficientemente hábil para burlar los controles establecidos y provocar algún desastre en la información, los equipos o, en general a todas las instalaciones.

La finalidad de incluir este capítulo es precisamente la de estar preparados para afrontar un desastre en el centro de cómputo, es decir, que se esta partiendo de la base de que existe una incertidumbre en relación a que el desarrollo de las actividades dentro del centro siempre estén bajo el control de los responsables del mismo. Y

aunque es muy sano pensar en que la calidad de las instalaciones y el perfecto orden y cuidado que se tienen dentro del centro de proceso van a permitir siempre un ambiente de operación seguro; si no se cuenta con un plan de acción previamente establecido para afrontar la posibilidad de que algo salga mal, entonces el esquema de protección y seguridad que se ha planteado en los capítulos anteriores puede venirse abajo, y desaparecer con todo y centro de proceso de un momento a otro ante la presencia de algún evento intencional, accidental o natural. El plan de acción que aquí se menciona consiste en una serie de procedimientos perfectamente detallados que contemplen, por escrito, todas y cada una de las actividades que deberán desempeñarse en situación de contingencia.

En este capítulo se hará un listado de los procedimientos necesarios para afrontar las contingencias y para una adecuada y pronta recuperación de la operación, tomando en cuenta la mayoría de las amenazas que se tienen en cualquiera centro de proceso informático, mismas que ya fueron definidas en capítulos anteriores. Se señalarán también las previsiones que deben tomarse con los medios de respaldo y almacenamiento de información, que son la base de la recuperación de un centro de cómputo; tanto en la instalación original como en algún centro de proceso alterno, por lo que se analizarán las necesidades y condiciones bajo las cuales será necesario trasladar la operación a una instalación alterna.

4.1. Procedimientos básicos

Un plan de contingencias es un plan de acción detallado que permitirá enfrentar una situación "anormal" y en caso necesario reasumir o recuperar la operación en el punto donde se encontraba antes del evento anormal ocurrido. También se le puede llamar "plan de recuperación" y está conformado por una serie de procedimientos, uno para cada elemento involucrado en la operación, por lo que el plan de acción global es una interrelación de procedimientos particulares.

4.1.1. Preparación de documentos

Las guías para la preparación adecuada de un plan de contingencias forman parte del plan mismo, es decir, que los primeros procedimientos que se deben hacer del conocimiento del responsable del centro de cómputo son aquellos que le permitirán hacer un levantamiento de información de los recursos con que se cuenta en el centro de proceso, generalmente estos procedimientos son elaborados por el responsable de la seguridad de la empresa, quien será también el encargado de dar seguimiento a la elaboración del plan de cada centro de cómputo en particular. En esta primera parte se deben incluir procedimientos para:

- *Levantamiento de información*: Describe paso a paso que información se debe documentar de los equipos de proceso, dispositivos periféricos, sistemas auxiliares, procesos, sistemas operativos, bases de datos, software de seguridad, aplicaciones, etc. Se pueden incluir formatos especiales para organizar la información y los correspondientes instructivos de llenado de los campos definidos en los formatos.

- *Cuestionario de comunicaciones*: Describe la manera de documentar los recursos de comunicación que se tienen en el centro de cómputo, dando especial atención a los medios de enlace alternos para determinar las alternativas de respaldo que pueden manejarse para las comunicaciones.

- *Integración del comité de recuperación*: Indica quienes deben ser los integrantes de un grupo de decisión que se reunirá cuando se presenta una contingencia; para autorizar y dar seguimiento a las labores de recuperación. Se detallan también las actividades de cada uno de los integrantes, el sitio de reunión en una contingencia y las responsabilidades de cada uno de ellos según su área de trabajo.

- *Integración de brigadas*: Indica al responsable del centro de cómputo, la manera de proceder para formar brigadas de contingencia y/o protección civil para hacer frente a eventos no previstos. Se detallan responsabilidades de cada tipo de brigada y la capacitación que deben tener cada una de ellas.

- *Integración de directorios*: Detalla la información necesaria para facilitar la localización de las personas involucradas en la operación del centro de cómputo desde los operadores hasta las autoridades a quienes se debe informar de la situación de contingencia; por lo que se deben integrar directorios de: personal operativo, responsables de la operación, proveedores, áreas de apoyo técnico, brigadistas, comité de recuperación, servicios de emergencia y, en algunos casos, clientes.

4.1.2. Contingencia interna

Los procedimientos para atender contingencias menores dentro del centro de cómputo deben ser desarrollados por los responsables de la operación del mismo, debiendo incluir los procedimientos básicos para:

- *Restablecimiento de software*: Contiene las actividades (y los responsables de ejecutarlas), que deben seguirse para atender una falla en el software instalado; ya sea aplicación, sistema operativo, base de datos o alguna otra herramienta instalada.

- *Restablecimiento de hardware*: Se detallarán todas y cada una de las actividades necesarias para recuperar la operación de alguno de los componentes físicos del centro de cómputo; llámese equipo de proceso, periféricos, equipo auxiliar o equipo de comunicaciones.

- *Restablecimiento del ambiente de comunicaciones:* Se deben definir las actividades y los responsables de atender fallas en los medios de comunicación o en los equipos involucrados. También deben detallarse los medios alternos y la manera de efectuar los cambios entre uno y otro.

Una de las maneras habituales de atención a alguno de estos tipos de fallas, es hacerlo por vía telefónica y una vez evaluando la gravedad y posibles soluciones, el técnico se desplaza al lugar con las herramientas y refacciones necesarias para una rápida

reparación; así que para la atención de este tipo de contingencias es necesario tener a la mano la información recabada en la sección anterior, ya que la persona que atiende telefónicamente puede requerir la versión del sistema operativo, el modelo del equipo dañado, etc.; por lo que, tener esta información ya documentada puede facilitar la recuperación y evitar pérdida de tiempo para el técnico que atiende la falla.

4.1.3. Desastres mayores

Para decidir los procedimientos que deben incluirse en esta sección, es necesario contar con un análisis de los riesgos que pueden afectar a una instalación, ya que actualmente existen una gran cantidad de procedimientos oficiales generados por la Secretaria de Gobernación en los que se indica que hacer en caso de que se presente alguno de los desastres previstos. De manera general los procedimientos que se incluyen con mayor frecuencia son los siguientes:

- Procedimiento para casos de incendio.
- Procedimiento para casos de inundación.
- Procedimiento para casos de amenaza de bomba.
- Procedimiento para casos de manifestación o motín.

Según la zona donde se ubique el centro de cómputo se puede enriquecer la lista con los siguientes procedimientos:

- Procedimiento para casos de sismo.
- Procedimiento para casos de huracanes.
- Procedimiento para casos de derramamiento de químicos.

En todo caso estos procedimientos, aunque sean generales, se deben adaptar a cada centro de proceso asignando responsables a cada actividad.

4.1.4. Después de un desastre

Es probable que la mayoría de los desastres señalados en la sección anterior, en caso de suceder alguna vez, no generen un problema mayor para un centro de cómputo que se ha diseñado con todas las prevenciones de seguridad analizadas en los capítulos anteriores, pero dado que se está hablando de eventos excepcionales en magnitud se deben efectuar algunas actividades especiales para comprobar el buen estado de las instalaciones o en su caso proceder ordenadamente al seguimiento y reparación de los daños, por lo que se deben incluir procedimientos para:

- *Reunir al comité de recuperación*: Se debe acordar una manera de contactar con los miembros de este comité, generalmente se asigna previamente un lugar de reunión, pero debe preverse que hacer en caso de no poder reunirse ahí, o la asignación de suplentes para casos en que los propietarios resulten afectados por el desastre.

- *Registro de actividades en bitácora de contingencias*: Todas las acciones acordadas deben documentarse y notificarse a cada responsable de ejecutarlas. Es muy útil la elaboración previa de formatos, así como los instructivos de llenado de éstos, debiéndose incluir una casilla para marcar las actividades concluidas y otra para las observaciones necesarias.

- *Búsqueda de personal*: Una de las actividades primordiales después de un desastre es la localización del personal involucrado en la operación del centro de cómputo, tanto para comprobar que no fue afectado por el desastre como para apresurar la recuperación de la operación; por lo que, en este procedimiento, se deben incluir jerarquías de búsqueda (en domicilio, en lugar de trabajo, en sitio de concentración externo, etc...) sin olvidar que se cuenta con un directorio para facilitar la localización.

- *Evaluación de daños*: El comité de recuperación debe estar formado por representantes de varias áreas operativas, quienes serán los responsables de

evaluar los daños existentes en su respectiva área de competencia, para después hacer un reporte general y trazar la estrategia de recuperación más apropiada.

- *Restablecimiento externo*: Una de las posibilidades que se deben contemplar es el hecho de no poder recuperar la operación en el mismo centro de proceso debido a los daños que se tienen, por lo que se deben detallar los pasos a seguir para trasladar la operación hacia un centro de proceso alterno.

Los procedimientos relacionados en las cuatro secciones anteriores son, de manera general, los necesarios para conformar el plan de contingencias; sin embargo, en caso de requerirse se deberán desarrollarse procedimientos particulares que incluyan la recuperación de procesos especiales o poco comunes.

Por otro lado, para facilitar el desarrollo y posterior consulta, los procedimientos deben desarrollarse con un formato estándar diseñado de común acuerdo entre el responsable del centro de cómputo y el responsable de la seguridad de la empresa. También se deben desarrollar resúmenes de actividades (*check list*) de consulta rápida, que deben tenerse a la mano para consultar de inmediato.

4.1.5. Mantenimiento del plan de contingencias

Una última consideración en relación con los procedimientos del plan de contingencias es que se debe implementar un programa de mantenimiento y actualización, principalmente de la información que se considera que puede tener cambios a corto plazo. Los principales cambios que deben documentarse, son:

- Versiones de software instalado.
- Procesos operativos.
- Características de equipos instalados.
- Personal operativo, de apoyo o responsables de área.
- Proveedores, clientes o servicios de emergencia.

Lo anterior no quiere decir que sólo la información técnica o los directorios pueden sufrir cambios, solamente se señala que es en estos conceptos donde se pueden presentar cambios más frecuentemente y que el resto de las actualizaciones tienen un ciclo de vida mucho más largo. Por ejemplo, para efectuar cambios a algún procedimiento, generalmente hace falta pasar por varias fases de pruebas, tanto de escritorio como reales, para después hacer la liberación de una versión nueva de dicho procedimiento.

4.2. Política de respaldos

Aunque los procedimientos de un plan de contingencias son el soporte para hacer frente a las contingencias y desastres en un centro de cómputo, existe un recurso de apoyo sin el cual sería infructuoso cualquier esfuerzo que se haga para recuperar la operación por muy perfecta que sea la ejecución de los procedimientos. Este recurso invaluable es un respaldo de la información en algún medio externo al procesador y que debe guardarse lo suficientemente lejos del mismo para evitar que sea afectado por el mismo evento de desastre. Por lo que el manejo de los medios de almacenamiento o respaldo, debe estar contemplado en las políticas de seguridad de cualquier empresa y, aun más, debe reservarse una política particular para respaldo, la cual debe incluir lo siguiente:

- Periodicidad de los respaldos,
- Resguardo,
- Verificación y
- Reciclaje.

4.2.1. Periodicidad de los respaldos

De manera general, tal como debe ser una política, se deben definir periodos de tiempo adecuados para efectuar el respaldo de:

- Sistemas operativos
- Configuración del sistema

- Aplicaciones
- Bases de datos
- Pistas de auditoría
- Bitácoras

Por supuesto que una política no puede especificar los periodos en que se deben efectuar los respaldos señalados, pero si prevé que cada una de las áreas responsables debe definir normas, procedimientos y herramientas automatizadas para la ejecución de rutinas de respaldo. Por ejemplo, en la tabla 4.1 se ilustran los periodos recomendables para cada uno de los componentes citados arriba.

Componente	Periodicidad
Sistemas operativos	Cada 6 meses o cada vez que ocurra un cambio en la versión.
Configuración del sistema	Cada mes o al ocurrir un cambio en la configuración.
Aplicaciones	Cada 3 meses o cada vez que se libere una nueva versión.
Bases de datos	Diario, al término de las operaciones del día.
Bitácoras	Diario o al agotarse el espacio asignado para la bitácora.
Pistas de auditoría	Diario o al agotarse el espacio asignado para este fin.

Tabla 4.1. Periodicidad de respaldos.

4.2.2. Resguardo

La política de respaldos indica que se debe contar con los lugares adecuados, dentro y fuera de las instalaciones, para el resguardo de los medios de almacenamiento utilizados en los respaldos de información. Por esta razón, en cada centro de cómputo se debe de contar con cajas de seguridad y/o bóvedas a prueba de fuego, inundación y otros riesgos, para almacenar ahí los dispositivos utilizados.

Adicionalmente, se debe prever la generación de un respaldo más de cada componente, el cual debe ser guardado fuera de las instalaciones del centro de

proceso; por lo que se debe contratar el servicio de bóveda de seguridad en algún banco o servicio de protección de valores, verificando la suficiente lejania con el centro de proceso para evitar que el mismo desastre afecte a ambas instalaciones. Otro lugar donde se puede almacenar un respaldo es en un centro de cómputo de la misma empresa, que esté ubicado en otra ciudad, lo cual no tendría un costo de almacenamiento; aunque en este caso debe tomarse en cuenta otro riesgo, debido a que generalmente no se cuenta con vehículos especiales, protegidos para el traslado; se tendría que evaluar el costo de este servicio comparado contra el almacenamiento en un banco o en un servicio de protección, que generalmente incluyen el costo de traslado.

4.2.3. Verificación

Otro factor que debe considerarse en una buena política de respaldo, es el hecho de verificar que la información respaldada se encuentra en buen estado, ya que sería muy lamentable en un caso de recuperación de desastre se intentara "bajar" un respaldo y resulte que la información está dañada, no es utilizable o simplemente no existe.

Una manera fácil, aunque no muy confiable, de verificar que un respaldo se llevo a buen término es comparando la cantidad de bloques de información que se almacenaron contra la cantidad de bloques que reporta ocupados el dispositivo de almacenamiento utilizado. Es más recomendable contar con un equipo adicional en el que se pueda "bajar", fuera de la operación normal, el respaldo obtenido, verificar su integridad, generar otra copia y enviarlo después a su lugar de almacenamiento final. Sin embargo, esto último no siempre es factible por lo que el área responsable deberá desarrollar o adquirir alguna herramienta para verificar que el respaldo se efectuó correctamente.

4.2.4. Reciclaje

Por último, la política de respaldos debe prever la reutilización de los dispositivos de almacenamiento; según ésta se deben conservar tres respaldos consecutivos de la

información después de lo cual un dispositivo puede volver a ser utilizado considerando un ciclo de almacenamiento de la información en versiones que se denominan abuelo, padre e hijo. Esto es, que un medio de almacenamiento que se utilizó hace tres días para respaldar la base de datos, puede volver a utilizarse hoy para hacer un respaldo nuevo de la misma base.

Lo anterior implica que se debe tener un estricto control de las versiones de respaldos que se manejan en la cintoteca, por lo que se recomienda que la información mínima con que se debe identificar un dispositivo de almacenamiento es la siguiente:

- Localidad
- Nombre del sistema o aplicación
- Fecha de respaldo
- Frecuencia de uso
- Nombre del operador
- Fecha de expiración de la información y
- Número de inventario

Para la reutilización de dispositivos de almacenamiento o respaldo, debe tenerse en cuenta el ciclo de vida útil de los mismos; es decir, que no debe utilizarse un disquete más de 30 veces (dato del fabricante) o un disco óptico mas de 150 veces, porque se pondría en riesgo la información almacenada. Debido a esto, también es necesario que la política contemple la elaboración de algún procedimiento para deshacerse de los medios que ya no se utilizarán en el centro de cómputo y que antes de deshecharlos se deben pasar por un proceso de borrado, para evitar que la información almacenada sea utilizada por personal ajeno.

4.3. Operación en centro de cómputo alterno

El último punto a considerar para que un plan de contingencias esté completo, es contemplar la posibilidad de que la recuperación no se pueda llevar a cabo de manera inmediata en el centro de cómputo original; por lo que es necesario hacer las

previsiones pertinentes que permitan la recuperación en alguna instalación alterna que proporcione las facilidades para reasumir la operación básica, por lo menos. Los motivos para no poder operar en el centro original pueden ser muchas, desde falta de servicio en las comunicaciones o daños menores a la infraestructura de proceso o/y equipos auxiliares, hasta la destrucción total del inmueble donde se ubica el centro de cómputo. Por esta razón, el proceso de elección de la mejor opción debe ser cuidadosamente analizado desde la definición de los requerimientos tanto de equipamiento como de programas instalados; hasta las facilidades y condiciones de seguridad que debe proporcionar el centro de proceso alterno (seguridad en el acceso a instalaciones, confiabilidad de equipos auxiliares instalados y sobre todo capacidad para albergar los recursos básicos de operación de los huéspedes), sin olvidar que este proceso debe culminar con la formalización de un convenio escrito en el que se delimiten las responsabilidades y obligaciones de las partes involucradas.

4.3.1. Definición de requerimientos

En la sección 4.1.1., se habló de que una primera fase en la preparación de un plan de contingencias es la documentación de los recursos existentes en el centro de cómputo y de la conveniencia de elaborar formatos de presentación para facilitar la consulta; esta información refleja la cuantificación de los recursos que se utilizan en el centro de cómputo, por lo que serán estos mismos recursos los que se solicitarán en el centro de proceso alterno. A grandes rasgos la información documentada debe contener lo siguiente:

- *Información de procesadores principales:* Marca, modelo, sistema operativo y capacidad de memoria (RAM y disco duro).
- *Equipos periféricos:* Marca, modelo, capacidad, tipo de puerto utilizado, tipo de enlace utilizado, ubicación y a que procesador están conectados.
- *Equipos auxiliares:* Marca, modelo, función, capacidad, ubicación, porcentaje de uso y sistemas que lo utilizan.

- *Descripción de aplicaciones:* Nombre, lenguaje de programación, espacio requerido para programas, espacio para datos, ruta de instalación, nivel de servicio, compatibilidad entre equipos y personas responsables del desarrollo y mantenimiento.
- *Descripción de procesos por aplicación:* Nombre del proceso, aplicación a la que pertenece, prioridad, periodicidad de ejecución, tiempo de ejecución, tipo de proceso, suministros que utiliza y departamento que lo ejecuta.
- *Características de sistemas operativos:* configuración actual, definición de perfiles de usuario, números de licencia y áreas responsables.

Esta información, aparte de servir para definir requerimientos al momento de solicitar apoyo para la recuperación, también sirve de referencia en el caso de que se desee proporcionar el apoyo para la recuperación de algún otro centro de cómputo, ya que se tiene a la mano la información de los recursos existentes y los que están en uso por lo que se puede definir de inmediato si se tienen las condiciones para facilitar el apoyo al centro de cómputo que lo esté solicitando.

Aparte de los requerimientos técnicos de los equipos, las aplicaciones, los procesos y los sistemas, es necesario definir de antemano el espacio físico que se ocupará para efectuar procesos manuales o simplemente para permitir que se ubiquen las personas que se trasladarán para dar soporte a la operación por lo que se debe elaborar una lista del personal que asistirá a la instalación anfitriona. También se deben relacionar los suministros que se trasladarán al centro alterno, así como aquellos que proporcionará el centro anfitrión y, por último, se debe garantizar la existencia de recursos financieros para cubrir los gastos que se generarán en el traslado de personal, envío de paquetería, viáticos, etc.; por lo que, al menos, se debe asegurar la presencia en el comité de recuperación de un representante del área de finanzas de la empresa, que será quien se encargue de facilitar estos recursos, ya que la mayoría de las veces no es posible mantenerlos disponibles en todo momento.

4.3.2. Elección del centro alterno

Existen varias alternativas que deben analizarse desde puntos de vista diferentes, debiendo prevalecer aquella que proporciona mayor nivel de seguridad a la información procesada y, obviamente, con la menor cantidad de riesgos posible. Aunque en algunas ocasiones los niveles directivos optan por la alternativa más económica, debe ser labor del área de seguridad convencerlos de que no se deben asumir riesgos si pueden evitarse; sobre todo si el negocio de la empresa es precisamente vender los servicios de proceso informático. En la tabla 4.1., se hace una análisis comparativo de las alternativas de centros alternos; definiendo los tipos de centros alternos que pueden estar disponibles actualmente y haciendo referencia a sus respectivas ventajas y desventajas que deben servir como puntos de evaluación al momento de decidir por la elección de una u otra alternativa como la mejor solución para una empresa.

Tipo	Descripción	Ventajas	Desventajas
Sitio equipado (hot site)	Es un centro de cómputo totalmente habilitado con equipo y comunicaciones. Puede ser un sitio comercial o privado.	• Puede seleccionarse una variante que encaje con los requerimientos de tiempo para la recuperación. • Requerimientos específicos para su uso. • Oportunidad de pruebas regulares. • Se pueden especificar necesidades de equipo.	• Es muy costoso. • Problemas posibles en caso de desastres múltiples. • Puede no tener espacio de trabajo suficientes. • Puede estar muy alejado de centro original.
Puro cascarón (cold site)	Es una oficina equipada con servicios eléctrico, aire acondicionado y comunicaciones; pero sin mobiliario y/o equipo instalado.	• Bajo costo. • Flexibilidad Geográfica.	• Dificultad para hacer pruebas. • Puede pasar mucho tiempo para ser activado. • Puede haber dificultades para trasladar muebles y equipo al momento del desastre.

Tabla 4.1. Alternativas para centro de cómputo alterno (continua...).

Tipo	Descripción	Ventajas	Desventajas
Acuerdos de ayuda mutua	Es un acuerdo con otra empresa mediante el cual se proveen el uno al otro algún espacio para proceso en casos de desastre.	• Libre de costo (o muy bajo)	• Los acuerdos pueden no estar fundados legalmente. • Probable falta de capacidad para manejar el exceso de trabajo crítico.
Facilidades en un segundo centro	Prever espacio y capacidad en un centro de cómputo de la misma empresa, el cual puede ser usado para albergar los procesos críticos.	• Bajo costo. • Control total.	• Dificultad para hacer pruebas. • Puede causar un desastre en el segundo centro. • Se puede sobrepasar la capacidad del anfitrión.

Tabla 4.1. Alternativas para centro de cómputo alterno.

4.3.3. Convenio de respaldo en centro alterno

Debe documentarse un acuerdo formal, por escrito, sea cual sea la alternativa seleccionada para contar con un centro alterno que permita a un centro de cómputo su recuperación fuera del sitio original en caso de que la magnitud del desastre así lo requiera; en este acuerdo de debe dejar bien claro que existen obligaciones y responsabilidades para ambas partes involucradas. Cuando se contrata este servicio con alguna empresa ajena, resulta obvio que debe existir un contrato con el detalle de los requerimientos del solicitante y una descripción, también detallada, de los que serán cubiertos por el prestador de servicio. Sin embargo, también se debe establecer un acuerdo formal cuando el convenio se celebra con algún centro de cómputo de la propia empresa, esto con el fin de evitar contratiempos al momento del desastre y de agilizar la recuperación de la instalación colapsada.

En el apéndice B se muestra un ejemplo de cómo debe ser la redacción y los elementos que debe tener un convenio de respaldo. Este formato debe usarse en la documentación con centros de cómputo de la misma empresa y puede usarse cuando se trata de documentar un convenio con una compañía externa.

Con esto se concluye toda la información relacionada con la implementación de un esquema integral de seguridad para centros de cómputo, recordando que se incluyeron temas tales como: los antecedentes de la seguridad informática, los aspectos relevantes de una infraestructura física para la protección de los recursos, las herramientas de control lógicas que permiten preservar las propiedades de la información almacenada y, por último, la metodología para recuperar un centro de cómputo cuando hayan fallado todas las medidas precautorias tomadas.

Sólo resta hacer un ejercicio práctico en el que se reflejen los temas tratados y su aplicación a un proyecto real de centro de cómputo de la Secretaría de Hacienda y Crédito Público. Ya que como se mencionó en el objetivo de esta tésis, la idea es que este documento sirva como guía para los líderes de proyecto que tienen a su cargo la construcción de centros de proceso.

5

CASO PRÁCTICO

Uno de los objetivos principales del presente trabajo es que sirva a los líderes de proyecto para considerar todos los requerimientos de seguridad al momento que se enfrentan al reto de remodelar o construir un centro de cómputo. Este caso práctico permitirá evaluar la efectividad con que se ha resuelto el problema planteado ilustrando paso a paso la manera de usar adecuadamente esta referencia.

Generalmente, el proceso de remodelación o construcción de un centro de cómputo comienza con la designación de un líder de proyecto. A partir de ese momento, la persona asignada inicia una investigación de campo para averiguar las facilidades de espacio y recursos existentes en el lugar destinado para el nuevo centro de proceso y, una vez recabada esta información, pueda estar en posibilidades de apoyarse en este manual para definir todos los requerimientos e integrarlos como parte de un solo proyecto que se someterá a autorización. Así que este caso práctico inicia con el requerimiento de construcción de un nuevo centro de cómputo, para el que se darán algunos antecedentes referentes a los riesgos del lugar elegido con lo que se podrán

establecer las características constructivas y las prevenciones que se deben tomar para protegerlo del entorno. Enseguida se irán incluyendo cada una de las consideraciones de seguridad física y lógica descritas a lo largo del presente trabajo, haciendo las observaciones pertinentes y/o los cálculos e ilustraciones necesarias con el fin de incluir todos los aspectos relacionados con la seguridad del centro de proceso.

El caso práctico es el siguiente:

5.1. Nombre del proyecto:

"Nuevo centro de cómputo para la aduana de Cd. Acuña, Coahuila".

5.2.Antecedentes

Esta aduana está localizada a un costado del río Bravo, que sirve como frontera entre E.E.U.U. y México, y el terreno destinado a la construcción del nuevo centro de cómputo está ubicado en uno de los patios fiscales propiedad de la SHCP. Los riesgos principales, derivados de su ubicación geográfica, son:

- Probabilidad de desbordamiento del río, por lo que se debe elegir la parte más alta del terreno disponible y de ser posible aumentar la altura construyendo una plataforma de al menos 1 metro. Además considerar tratamiento especial a las canalizaciones subterráneas para evitar filtraciones de agua.

- El patio fiscal colinda con colonias populares, por lo que se debe construir una protección perimetral de malla ciclónica a 3 o 4 metros del centro de cómputo.

- El tipo de suelo es arenoso de baja compactación, lo cual obliga a construir una estructura de cimentación especial basada en un estudio especializado de mecánica de suelos.

- Existe una subestación y planta de emergencia con capacidad suficiente para soportar la carga que representa el centro de cómputo; sin embargo, el local donde se alojan la subestación y la planta requiere de algunas adecuaciones para reforzar la seguridad, ya que prácticamente cualquier persona tiene acceso a este lugar.

Con esta información recabada en una visita previa se puede ya iniciar el repaso a los requerimientos de seguridad según el orden de este manual.

5.3. Seguridad física - parámetros constructivos

En este caso no es necesario efectuar un análisis para definir la localización geográfica del centro de cómputo debido a que el terreno ya existe, por lo que será necesario adaptar las medidas de seguridad para disminuir los riesgos, tanto de inundación como la colindancia con zonas populares, detectados durante la visita previa; además de sujetarse a las condiciones de servicio eléctrico y de comunicaciones existentes. En el plano 5.1, se muestra la ubicación sugerida del nuevo centro de proceso, tomando en cuenta que esta área está más elevada que las zonas de circulación vehicular según indican las curvas de nivel en el mismo plano, con lo que se previene una posible inundación; además, se localiza cerca de las áreas operativas con lo que se minimizan las distancias del cableado de comunicaciones. Se aprovecha, también, la canalización y registros existentes para la alimentación eléctrica del centro de cómputo; además de instalar una cerca de malla ciclónica alrededor para evitar la aproximación de personas ajenas al mismo.

En el plano 5.2 y 5.3 se presentan las dimensiones y las características constructivas tanto de muros y techo como de la cimentación necesaria en este tipo de terreno para soportar la estructura del local.

A excepción de la planta de emergencia, se instalarán los equipos auxiliares dentro del centro de cómputo; sin embargo su correspondiente cálculo y planos se describirán en secciones posteriores.

Por lo que se refiere a la distribución de áreas internas, en este caso, sólo se construirá el espacio para procesadores y para equipo de telecomunicaciones debido a que las áreas de impresión, archivo y operación se encuentran en las oficinas ubicadas en la cercanía y están convenientemente protegidas, por lo que se reservarán las canalizaciones necesarias para comunicar adecuadamente las dos secciones.

Seguridad física - control de acceso

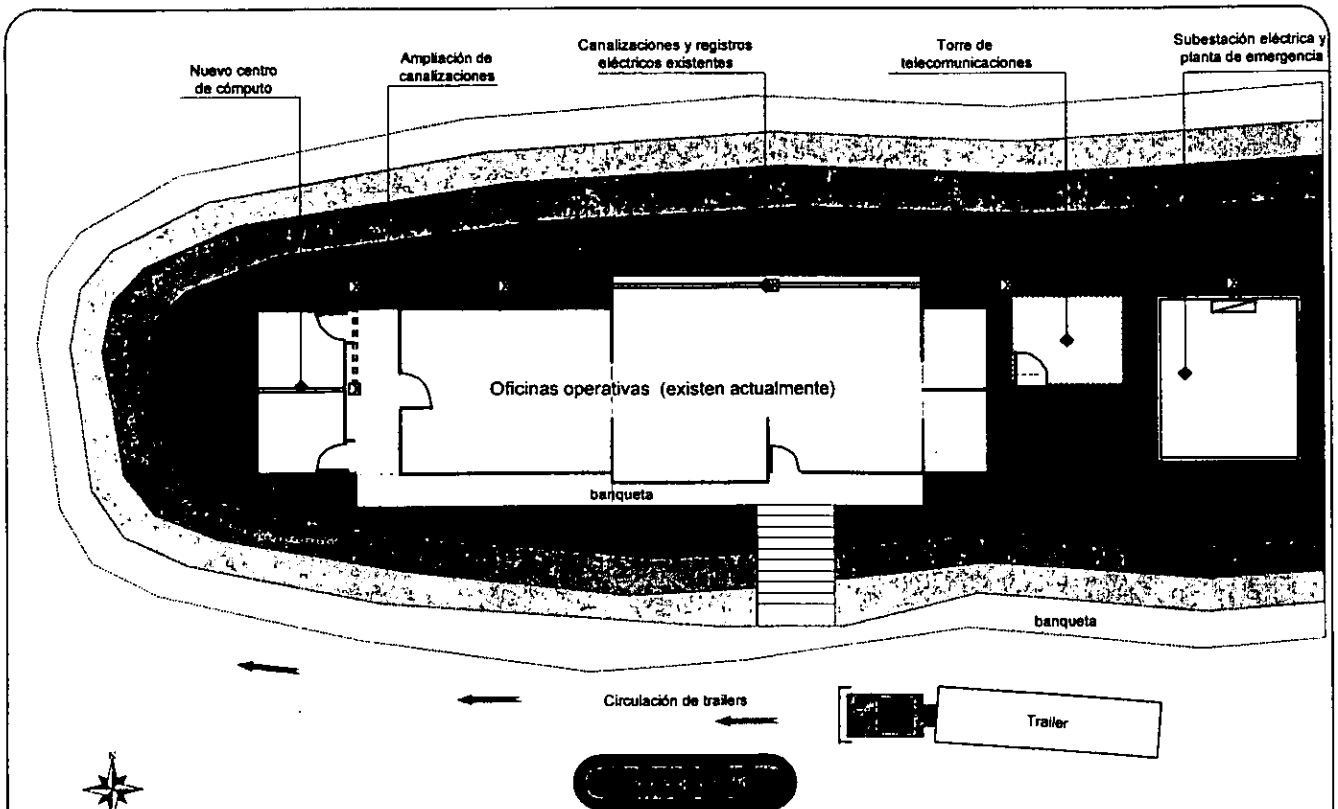
Se elegirá un sistema de control de acceso clasificado como de alta seguridad de tipo biométrico que reconoce la geometría de las manos del personal autorizado para tener acceso a las áreas de procesadores y/o de comunicaciones. El sistema tiene las siguientes características:

- Lectora con postes sensores que se ajustan para detectar la relación de dimensiones entre los dedos y la palma de la mano, guardando la información en una plantilla de 9 bytes y teniendo una velocidad de reconocimiento de 2 segundos. Este dispositivo cuenta además con un teclado numérico para introducir un código de acceso de hasta 10 posiciones asociado a cada usuario. Este teclado también se utiliza para programar el menú de opciones para control del dispositivo, por lo que debe incluir un *display* de cristal liquido.

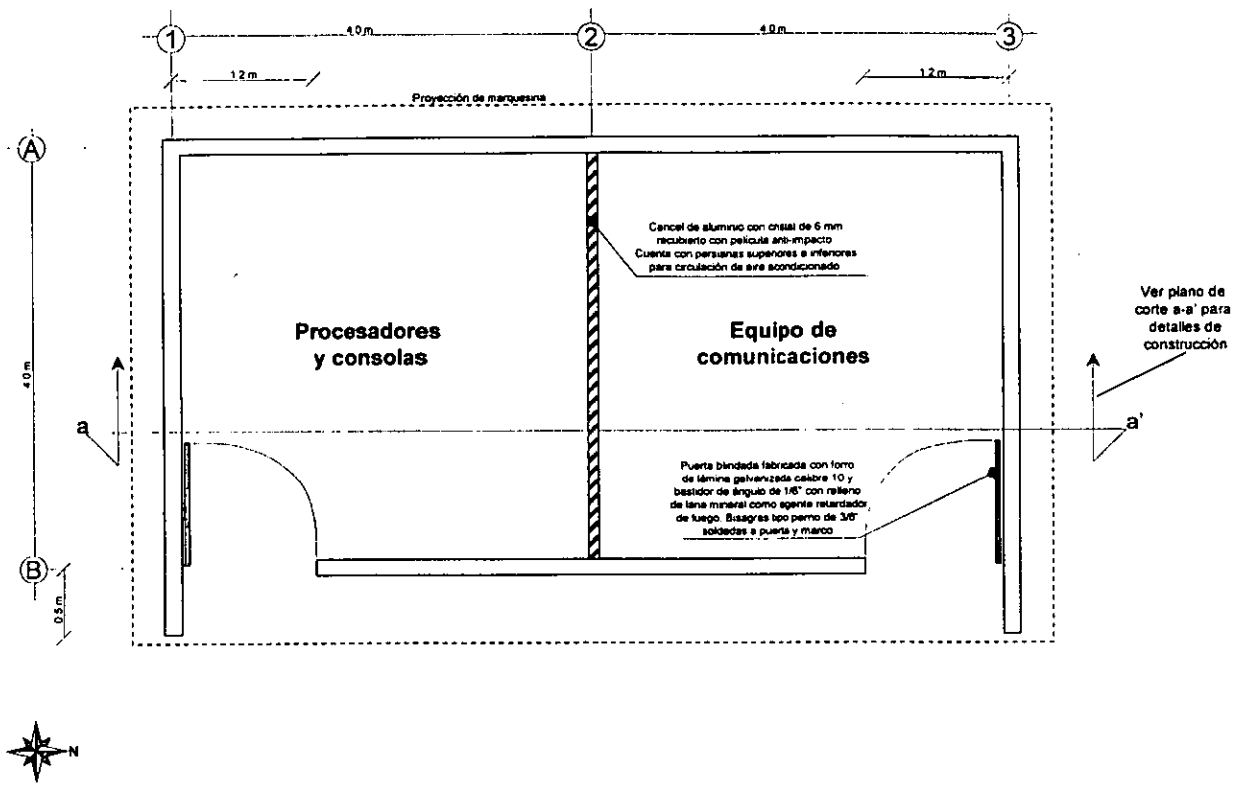
- Tablero de control con capacidad para registrar hasta 20,000 usuarios, controlar la cerradura asociada, emitir alarmas, programar horarios y tener espacio en memoria para almacenar hasta 1600 eventos. Debe tener, también, puerto serial para impresora y tarjeta para red *ethernet*; con el software para monitoreo, programación y control a través de una PC local o remota.

- Batería de estado sólido, libre de mantenimiento, que soporte el equipo y active la cerradura durante al menos 8 horas en caso de falla en el suministro de energía eléctrica.

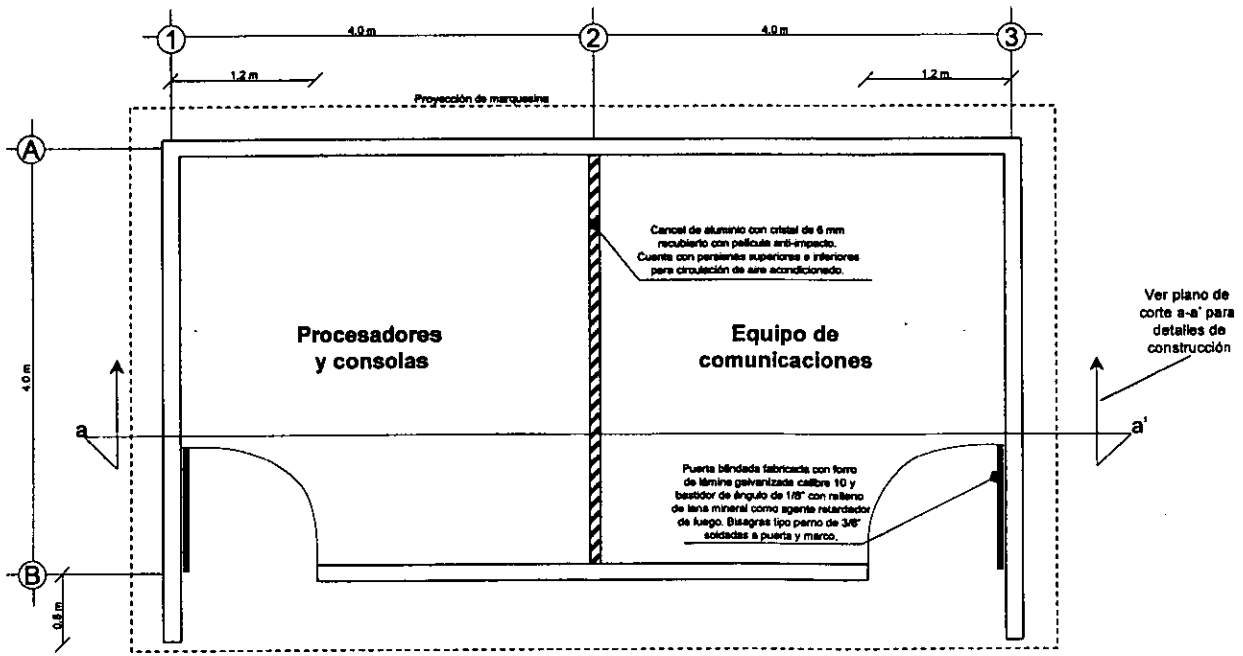
- Botón de liberación interno para activar la cerradura desde el interior.



Logotipo de la empresa	Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.				Logotipo del cliente
	Nombre del plano: Croquis del conjunto	Ubicación: Cd. Acuña, Coah.		Clave del plano Plano 5.1	
	Visto Bueno:	Aprobó:	Fecha	Revisó: Fecha	Escala Sin escala



Logotipo de la empresa	Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.				Logotipo del cliente
	Nombre del plano: Planta Arquitectónica	Ubicación: Cd. Acuña, Coah.	Clave del plano: Plano 5.2		
	Visto Bueno:	Aprobó:	Fecha:	Revisó: Fecha:	Escala: 1:50



Logotipo de la empresa	Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.						Logotipo del cliente
	Nombre del plano: Planta Arquitectónica	Ubicación: Cd. Acuña, Coah.			Clave del plano: Plano 5.2		
	Visto Bueno:	Aprobó:	Fecha:	Revisó:	Fecha:	Escala 1:50	

- Cerradura tipo electroimán de 1500 Lbs., instaladas en la parte superior de la puertas blindadas.

Se instalarán dos controles de tipo biométrico, uno en cada puerta y se colocarán empotrados sobre la pared por la parte exterior, para lo cual se deben dejar las preparaciones necesarias para el cableado eléctrico y de comunicación con el tablero de control y las chapas electromagnéticas.

Seguridad física – Instalaciones eléctricas

En los planos 5.4, 5.5 y 5.6 se especifica el diagrama unifilar, los cuadros de carga y la distribución del servicio que deben cumplirse para el centro de cómputo.

Dentro del local debe utilizarse canaleta plástica y sus respectivos accesorios para la distribución de los contactos, tanto de servicio normal como de servicio regulado. Se utilizarán tableros de distribución sobrepuestos en la pared que cumplan con especificaciones de la Norma Oficial Mexicana (NOM-I). En el exterior se utilizarán canalizaciones en tubería de PVC de 4" enterradas a 0.50 m de profundidad en trincheras y registros preparados y sellados para no permitir formación o acumulación de humedad; estas canalizaciones se conectarán con las ya existentes para instalar los cables de alimentación eléctrica desde la subestación y planta de emergencia.

Para el sistema de tierra se instalarán 3 varillas en pozos de tierras colocadas en configuración delta a 1 metro de distancia entre ellas, estarán "sembradas" frente al centro de cómputo y se conectarán al interior a través del registro instalado en esta misma área. Se considera que con la tres varillas es suficiente ya que la resistencia de terreno en este lugar es de 50 ohms y la conexión en paralelo de las mismas permitirá 16.66 ohms, cuando las NTIE indican que un parámetro adecuado para tierras físicas es que se encuentre la resistencia entre 8 y 25 ohms.

Seguridad física - UPS

Como se aprecia en el cuadro de cargas del tablero "B", plano 5.5, el consumo total de los equipos que se conectarán al UPS es de 6220 Watts y dado que en las perspectivas a futuro no se vislumbra algún aumento importante en la cantidad de equipos que se instalarán dentro del centro de proceso, entonces se da un sobredimensionamiento del 25 % de la carga instalada. Por lo que se considera que la capacidad del UPS a instalar será de 10 kVA y debe ser de tipo ON-LINE, con un banco de baterías que soporte la carga durante 15 minutos en las condiciones más críticas.

Las consideraciones básicas a partir de los cuales se deduce la capacidad del UPS son los siguientes:

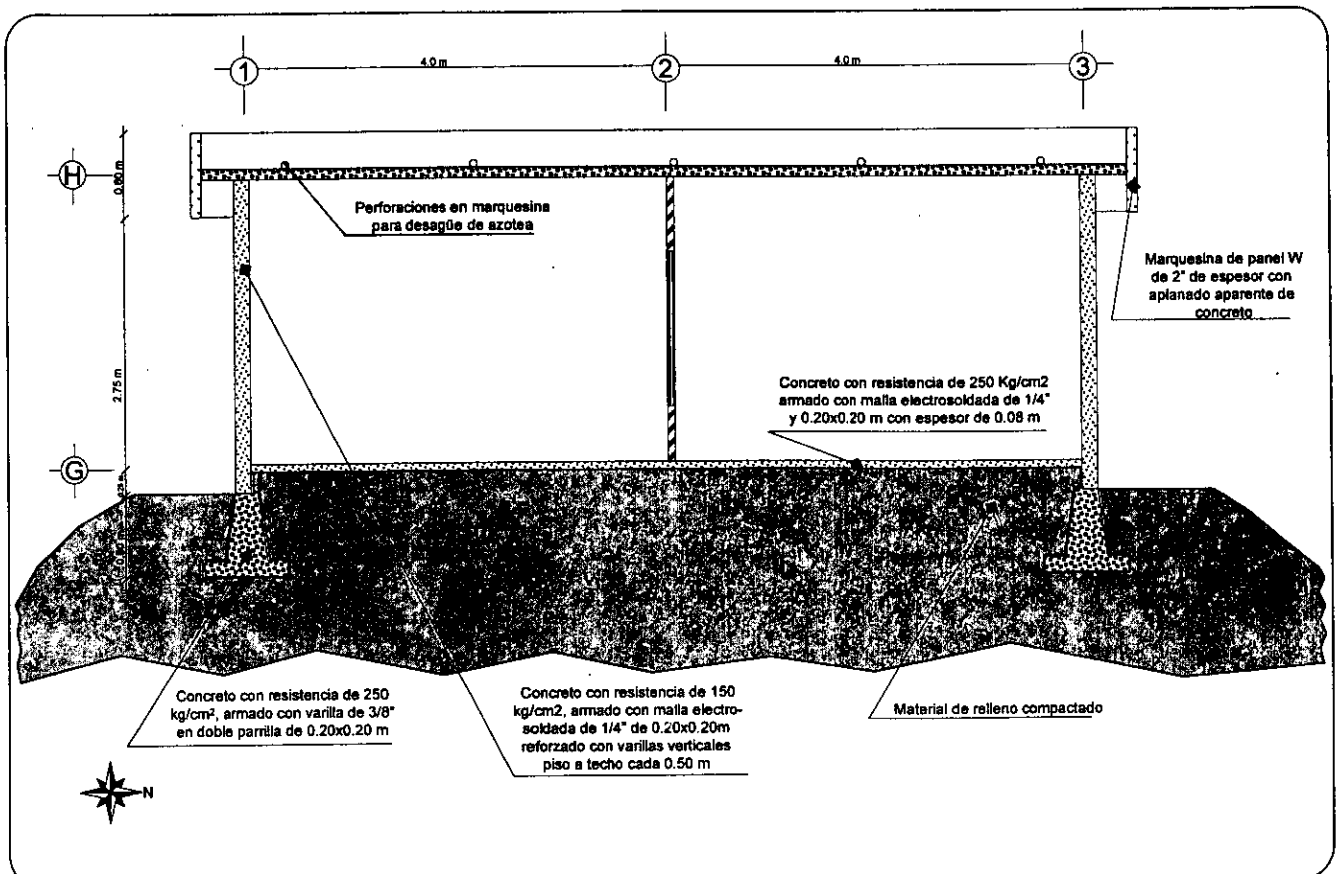
Capacidad requerida: 6220 W

La mayoría del equipo a conectar es de tipo electrónico por lo que no se ve afectado el factor de potencia y prácticamente la totalidad del consumo es de potencia real.

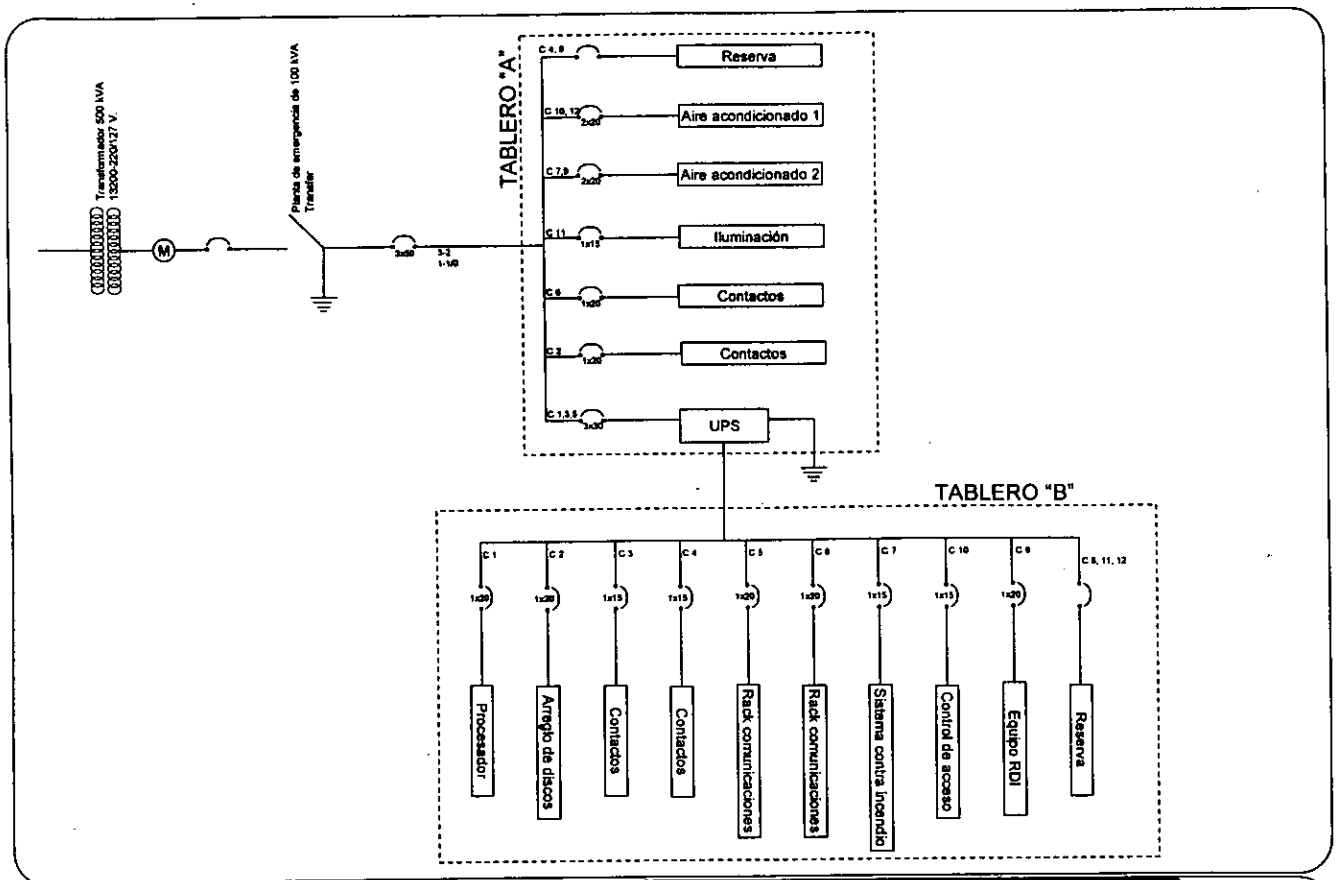
Una UPS de 10 kVA está diseñado para cargas hasta con un 0.8 de factor de potencia, por lo que en realidad su capacidad es de aproximadamente 8000 Watts, con lo que ya se incluye el 25 % de capacidad extra de la que se habló en el párrafo anterior.

Seguridad física – planta de emergencia

Como se mencionó en los antecedentes, ya existe una planta de emergencia de 100 kVA que actualmente se utiliza aproximadamente al 50% de su capacidad (según diagramas eléctricos existentes), considerando que el centro de cómputo tendrá un consumo menor a los 15 kVA, entonces se tomó la decisión de conectar a esta planta las nuevas instalaciones. Las únicas recomendaciones son: la de efectuar un mantenimiento preventivo mayor con el fin de asegurar la confiabilidad de la operación de este equipo, y reforzar el control de acceso al local por medio de la instalación de una cerradura de seguridad, ya que actualmente es prácticamente libre el paso hacia esta área.



Logotipo de la empresa	Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.				Logotipo del cliente
	Nombre del plano: Detalle del corte aa'	Ubicación: Cd. Acuña, Coah.	Clave del plano: Plano 5.3		
	Visto Bueno:	Aprobó:	Fecha:	Revisó:	Fecha: Escala: 1:50



Logotipo de la empresa	Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.			Logotipo del cliente
	Nombre del plano: Instalación eléctrica Diagrama unifilar	Ubicación: Cd. Acuña, Coah.	Clave del plano: Plano 5.4	
	Visto Bueno: Aprobó: Fecha:	Revisó: Fecha:	Escala: 1:50	

CUADRO DE CARGAS

TABLERO: "A" | TIPO: QO | FASES: 3 | HILOS: 5

Circuito	Contactos 180 W	Lámparas 2x70	Aire acondicionado 2000 W	UPS 8000 w		Cables [cal]	Interruptor termomagnético	Fase A	Fase B	Fase C
C 1,3,5				1		6	3X50	2800	2800	2800
C 2	4					10	1X15	720		
C 4									reserva	
C 6	4					10	1X15			720
C 7,9			1			6	2X20	1000	1000	
C 8								reserva		
C 10,12			1			6	2X20		1000	1000
C 11		2				10	1X15			280
							TOTALES:	4320	4600	4600

CUADRO DE CARGAS

TABLERO: "B" | TIPO: QO | FASES: 2 | HILOS: 4

Circuito	Procesador 900 W	Arreglo de discos 1100 W	Control de Acceso 300 W	Sistema contra incendio 400 W	Rack comunicaciones 1000 W	RDI 500 W	Contactos 180 W	Cables [cal]	Interruptor termomagnético	Fase A	Fase B
C 1	1							10	1x20	900	
C 2		1						10	1x20		1100
C 3							2	10	1x15	360	
C 4							2	10	1x15		360
C 5					1			10	1x20	1000	
C 6					1			10	1x20		1000
C 7				1				10	1x15	400	
C 8											Reserva
C 9						1		10	1x20	500	
C 10			2					10	1x15		600
C 11										Reserva	
C 12											Reserva
									TOTALES:	3160	3060

Logotipo de la empresa

Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.

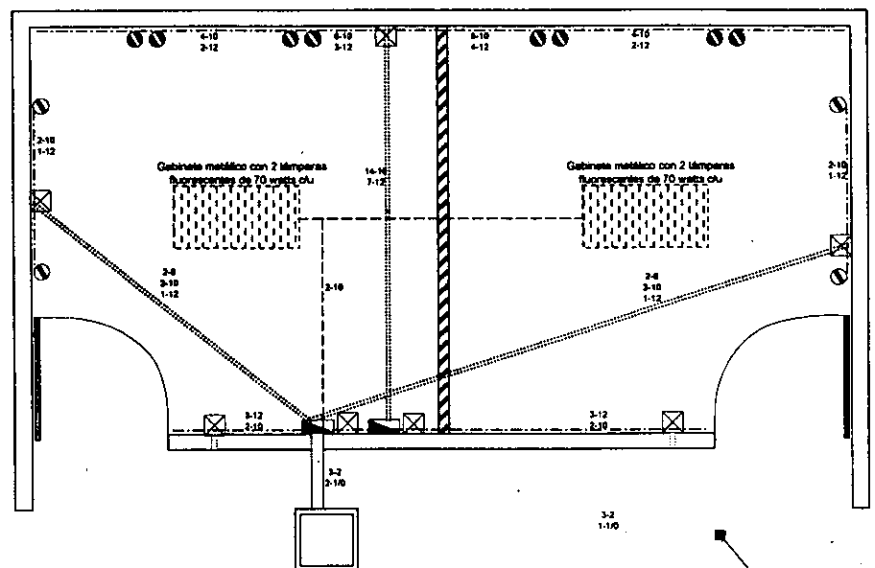
Nombre del plano: Instalación eléctrica Cuadros de carga

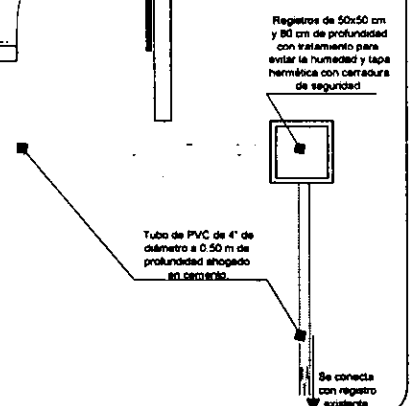
Ubicación: Cd. Acuña, Coah.

Clave del plano: Plano 5.5

Proyectó: Revisó: Fecha: Aprobó: Fecha: Escala: 1:50

Logotipo del cliente





Simbología

- Tablero eléctrico tipo QO de sobreponer con interruptores termomagnéticos.
- Tubo conduit pared delgada de 3/4" sobrepuesto en el techo y pared.
- Tubería PVC de 2" ahogada en el piso de concreto.
- Canaleta plástica de 103x46 mm de 3 vías sobrepuesta en la pared.
- Contacto doble polarizado color ambar con servicio normal.
- Contacto doble polarizado color rojo con servicio de UPS.
- Caja de conexiones de 10x10 cm galvanizada.

N

Logotipo de la empresa	Nombre del proyecto: Nuevo centro de cómputo en la aduana de Ciudad Acuña, Coahuila.			Logotipo del cliente
	Nombre del plano: Instalación eléctrica Distribución de contactos	Ubicación: Cd. Acuña, Coah.	Clave del plano: Plano 5.6	
	Visto Bueno: Aprobó: Fecha:	Revisó: Fecha:	Escala: 1:50	

Seguridad física – aire acondicionado

Para calcular la capacidad requerida en base volumen del espacio a acondicionar, se sabe que una tonelada de refrigeración (12000 BTU/hr) es suficiente para mantener la temperatura y humedad de hasta 50 m^3 de aire, incluyendo equipamiento de oficina y personal trabajando ahí dentro. Por lo que, dadas las dimensiones del centro de cómputo (7.85x3.85x3 metros), la capacidad requerida para acondicionar el espacio interior del centro de cómputo es de 24000 BTU/hr, que equivale aproximadamente a 2 toneladas de refrigeración.

Por otro lado, el cálculo a partir de las cargas individuales de los equipos que se conectarán según datos del fabricante y las personas que ahí laborarán es el siguiente:

Equipo	Consumo [BTU/hr]
Procesador	2000
Arreglo de discos	2000
Consola	1500
UPS	3000
RDI	2500
Rack de comunicaciones	3000 (promedio c/u)
Personas	1200 (promedio c/u)
Control de acceso	500
Sistema contra incendio	500
Otros equipos menores	2000 (todos)
TOTAL:	**21200**

Por lo que para fines de diseño, se recomienda tomar la cantidad que resulte mayor que en este caso es de 24000 BTU/hr como resultado del cálculo por espacio, con lo que aseguramos que con esta capacidad es suficiente para la operación de la sala informática; sin embargo, se adquirirán dos equipos de 18000 BTU/hr (1.5 toneladas de refrigeración cada uno) en base a las recomendaciones de las sección 2.4.3., es decir, para prevenir que alguno de los dos se dañe y el otro pueda soportar la carga total; lo cual es posible tan sólo con evitar que en caso de daño a algún equipo accese solo una

persona a la vez al local protegido y se saquen de operación algunos equipos de menor importancia, ya sea de comunicaciones o del concepto "otros" en el que se incluye, por ejemplo, PC's para monitoreo de red o iluminación.

Seguridad física – Sistema contra incendio

En base al diagrama de la sección 2.4.4., únicamente se describirá aquí la manera de calcular la cantidad de agente extintor que se necesita en el centro de cómputo que se está analizando.

Los datos que se requieren son los siguientes:

Porcentaje de concentración (recomendado para no causar daño a humanos): 7%
Altura sobre el nivel del mar (de la ciudad donde se instalará): 570 metros
Rango de temperaturas (de operación óptima): 18 – 22 °C

Con estos tres valores se encuentra en una tabla del fabricante la cantidad, en libras, de agente extintor que se requieren por metro cúbico de espacio a proteger. De la tabla se obtiene que en este lugar en particular se requieren 0.463 libras de extintor por cada metro cúbico.

El centro de cómputo tiene 90.66 m3, dada sus dimensiones interiores (7.85x3.85x3 metros), por lo que requieren 42 lbs. de agente extintor a presión dentro del contenedor cilíndrico.

El agente extintor seleccionado para ser utilizado en este centro de cómputo, es el gas FM-200 por sus características de ser un agente limpio y no dañar la capa de ozono cuando ocurre su descarga para la extinción de un incendio. Otra razón de esta selección es el hecho de que en México aún no se cuenta con distribuidores de otros agentes como el inergen que tengan una infraestructura de atención a clientes instalada, lo cual es muy importante para el soporte de servicio y refacciones que se requiere en caso de fallas posteriores a la instalación.

Seguridad física – piso falso

Debido a que ningún equipo instalado en el centro de proceso tiene entre sus requerimientos de operación algún parámetro que obligue a la instalación del piso falso, se toma la decisión de no instalarlo, por lo que el centro de computo tendrá piso firme acabado en loseta cerámica de alta resistencia para evitar acumulación de cargas estáticas y que pueda soportar el peso de los equipos instalados.

5.4. Seguridad lógica

Debido a que éste es un proyecto que permitirá renovar al centro de cómputo existente, la parte de aplicación más fuerte es la de seguridad física; sin embargo, todas las consideraciones estudiadas en referencia a la protección de los sistemas se aplican ya en el centro de cómputo actual. Por lo que, con el propósito de hacer una aplicación didáctica de lo estudiado en la sección de seguridad lógica se presentará una descripción de la manera en que se hace uso actualmente de los conceptos incluidos, y así tener un caso práctico que ilustre completamente esta tesis.

Seguridad lógica – control de acceso

Actualmente se encuentra operando un minicomputador de plataforma abierta Hewlett Packard serie 800 modelo D-270, con un sistema operativo HP-UX 10.20 y un manejador de base de datos informix versión 7.22.

Este sistema se encuentra operando bajo un control estricto de acceso, ya que tanto la cuenta denominada "root" (o superusuario), como la cuenta de superusuario del DBMS, "informix", se encuentran controladas por el área de seguridad de la organización y sólo son accesadas en casos de contingencia en el sistema, aplicando un proceso que permite el control para la entrega de las mismas. Este control que es autenticado por medio de un número de identificación personal (NIP), el cual se mantiene bajo el conocimiento y responsabilidad del personal de cada localidad.

El control de las contraseñas está basado en las políticas que vienen implícitas en el sistema operativo y que están activas para todas y cada una de la cuentas que residen en el sistema. Por otro lado, existen en el centro de procesamiento políticas y normas para que la generación de las contraseñas sea aplicada de acuerdo a los estándares de la industria. Existen controles propietarios aplicados para el control de accesos por cuentas de soporte a sistema operativo y al DBMS, además de los controles de acceso que autentican al usuario por medio de una clave o número de identificación personal.

Además se cuenta con un esquema de personalización de claves, personalización que es utilizada por las aplicaciones que residen en el sistema; y con un software para control de accesos activo, que permite monitorear aquellos accesos y la ejecución de comandos que toman la identidad de usuarios poderosos o privilegiados (root e informix).

Es importante señalar que el acceso al computador está restringido en su totalidad y aquellos accesos no autorizados son fácilmente detectados en base a los controles físicos y lógicos establecidos en dicho equipo.

Seguridad lógica – Criptografía

Actualmente se tiene establecido un esquema de actualizaciones a las aplicaciones. Dicho esquema se basa en la generación de paquetes de información encriptados, los cuales son generados con el método de encripción RSA, el cual ya es conocido por el manejo de dos llaves, una pública y otra privada.

Una vez que las áreas de desarrollo liberan actualizaciones a los sistemas de información de cada centro de cómputo, éstas son armadas en paquetes de información encriptados en los que se incluye una llave pública. Una vez que se transmite la información encriptada, el personal de la Aduana procede a instalar la actualización a las aplicaciones por medio de un esquema de actualizaciones controlado que permite instalar en base a la llave privada, que es responsabilidad del personal de la localidad.

Dicho esquema de actualizaciones apoyado en la utilización del esquema de encripción de llave pública y llave privada a su vez mantiene un registro de actividades apoyado en bitácoras de instalación y ejecución del programa del sistema operativo para la instalación de software.

Seguridad lógica – Clasificación de los datos

En el ambiente operativo descrito se tiene un control sobre los diferentes niveles de acceso a la información, implementados tanto a nivel de las aplicaciones como al nivel de acceso a la información contenida en los sistemas.

La información es accesada en base a los diferentes perfiles y características de los datos, ya que actualmente la información contenida en el sistema de cada localidad es considerada muy sensible.

De igual forma, y como una preocupación constante por parte de las áreas de seguridad informática y auditoría de la organización, existe el compromiso de mantener y conservar la integridad de la información, de tal hecho se derivan los esfuerzos para que los controles actuales sean mejorados, en apoyo a las políticas, normas y procedimientos establecidos para salvaguardar los datos, que en su totalidad tiene un grado de sensibilidad y confidencialidad bastante alto.

Seguridad lógica – seguridad en computadoras y sistemas

Una parte primordial en los sistemas de información es la seguridad que nos pueda brindar, como valor agregado, el sistema operativo, considerando la plataforma del equipo de la aduana en cuestión.

Actualmente en dicho sistema operativo se cuenta con una base de cómputo confiable (TCB) a nivel C2, dicha plataforma nos ofrece la garantía que las contraseñas se encuentran encriptadas y el acceso a los archivos está restringido. De igual forma se

encuentran activas las políticas del manejo de contraseñas y reintentos por penetraciones no autorizadas. Cuando alguna cuenta ha realizado repetidos intentos para accesar, ésta se deshabilita automáticamente y se solicita al área de seguridad de la organización su activación correspondiente.

El equipo posee, también, la facilidad de obtener soporte remoto por parte del proveedor vía línea telefónica; sin embargo, esta facilidad de equipo ha sido deshabilitada para evitar posibles conexiones no autorizadas por el personal de la Aduana.

Actualmente en dicho equipo no se realizan impresiones, ya que éstas han sido sustituidas por la generación del reporte a áreas de disco y su vez son consultadas en línea únicamente por el personal autorizado.

Asimismo, las aplicaciones que residen en dicho sistema son probadas y verificadas a nivel central, esto con la finalidad de que los desarrollos no contemplen salidas a sistema operativo, para realizar funciones inapropiadas y que las aplicaciones realicen sólo aquellas tareas para las que fueron diseñadas. Todo esto con el objetivo de evitar que se presenten las llamadas puertas traseras, caballos de Troya o cualquier otro método de alteración de información, que puede ser implementado en las aplicaciones.

Una parte muy importante y a la cual se le ha dado mucha importancia, es que en las aplicaciones que residen en el equipo de dicha localidad se lleva a cabo la generación de bitácoras y pistas de auditoría para el análisis respectivo, en caso de que se presente cualquier posible intrusión al sistema, alteración a la información o eliminación de la misma.

Algo que se ha implementado es el cambio de programación para la ejecución de comandos que permiten tomar la identidad de usuarios privilegiados, tales como un comando conocido como "*su*" , en donde la ejecución de éste se ha modificado para que en el caso que sea ejecutado lleve a cabo la solicitud de una llave, llave que es controlada por el área de seguridad de la organización. En lo que respecta al DBMS, de igual forma se tomó el control de la utilería "*dbaccess*", la cual es utilizada para accesar

al manejador de la base de datos y es controlada a través de un llave, llave que también es controlada a nivel central por el área de seguridad de la organización.

En los que respecta a controles para evitar posibles contagios de virus en las microcomputadoras que son utilizadas en dicha localidad, la organización lleva a cabo una campaña de seguridad corporativa antivirus, apoyada en un software comercial activo que protege toda la red.

Una vez que fue retirado el control de las claves privilegiadas (root e informix) de dicho equipo, fue implementada una aplicación que llevará a cabo la correcta administración del equipo (tanto a nivel de sistema operativo como de base de datos) sin la necesidad de tener acceso directo al sistema. Dicha implementación permite el control interno para realizar actividades de monitoreo de la base de datos (verificación de espacios), de acceso de usuarios, monitoreo de procesos, ejecución de comandos autorizados para el control de servicios, etc.

Otro de los aspectos básicos es el control de herramientas de desarrollo y compiladores, en donde el control radica principalmente en garantizar que no estén presentes en el equipo de producción, eliminando tambien el software sensible que pudiese afectar la integridad y confidencialidad de la información.

Adicionalmente, se han tomado una serie de medidas por parte de las áreas administrativas para evitar que la información que es procesada en dicha localidad, sea difundida a terceros y de esta forma evitar posibles fugas de información.

Seguridad lógica – telecomunicaciones

En esta parte, que es primordial para la organización debido a la posibilidad tan grande que existe de que la información que transmite dicha Aduana a nivel central sea interceptada, se están realizando los esfuerzos necesarios para sustituir el medio de comunicación actual (enlace vía X.25 en forma satelital), para contar con un medio más seguro (como RDI). Aunque la información que se transmite a la Aduana, llega

encriptada (como se había mencionado con anterioridad) para realizar las actualizaciones a las aplicaciones, con lo que se impide que la información sea alterada.

Por el momento se están controlando los equipos de comunicaciones (ruteador), para evitar posibles alteraciones a las configuración y la posible caída del enlace, lo cual repercutiría en la operación diaria de la Aduana.

Seguridad lógica – programas de aplicación

En lo que ha software de desarrollo se refiere y como se ha mencionado a lo largo del caso práctico, una vez que se ha realizado una nueva aplicación ésta es verificada por un área de laboratorio y diseño de pruebas, que tiene como función primordial el probar todas y cada una de las modificaciones, actualizaciones o nuevos desarrollos que se hagan a la aplicación que reside en el equipo de la Aduana.

De igual forma se lleva un control de todas y cada una de las versiones así como el control de los cambios a las aplicaciones. En lo que respecta a la seguridad implementada en dicha aplicación se tiene diferentes niveles de acceso a los diferentes módulos o subsistemas que la integran.

Con esta descripción de control en las aplicaciones se concluye el caso práctico que sirve para ejemplificar la teoría de seguridad informática desarrollada en este trabajo. Dando paso a los resultados y conclusiones del trabajo desarrollado, en donde se hablará de la manera en que este trabajo cumplió con el objetivo planteado y de las lecciones aprendidas en el desarrollo del mismo.

RESULTADOS Y CONCLUSIONES

Cuando decidimos elaborar este documento en el que se reflejan cuatro años de experiencia en el área de la seguridad informática, sabíamos de la importancia que tiene el hecho de conjuntar en un solo manual toda la información relacionada con la protección y la seguridad de los datos que se procesan en un centro de cómputo. Sin embargo, no teníamos idea de lo difícil que es encontrar información accesible debido a lo actual del tema y a su naturaleza confidencial; por lo que fue necesario idear una estrategia de recopilación basada en boletines especializados, conferencias, internet y la poca bibliografía disponible para lograr el objetivo planteado, mismo que establece la necesidad de contar en todos los centros de cómputo con un esquema integral de seguridad que, en base a controles físicos y lógicos, pueda garantizar una operación continua, la protección de los recursos y la preservación de las tres propiedades básicas de la información.

Una vez analizados los fundamentos y principios básicos tanto en seguridad física y lógica como parte del esquema planteado, se espera que el personal capacitado para llevar a cabo el liderazgo en la construcción y operación de un centro de procesamiento de información considere todos los requerimientos técnicos apoyándose en el personal especializado para la implementación, tanto de dispositivos de control como de aquellas medidas preventivas o de seguridad que permiten una adecuada administración de sistemas de información. Deben comprender, también, que la protección de la integridad y confidencialidad de la información que se procesa o guarda en un centro de cómputo, generalmente es considerada como la principal preocupación para una empresa, ya que la información es uno de sus más importantes recursos.

Un resultado difícil de evaluar en este momento es precisamente el grado de utilidad o la aceptación de este documento como un manual de referencia para el líder de proyecto, ya que implica prescindir inicialmente del apoyo de las áreas involucradas y prácticamente generar un anteproyecto, para presentarlo al cliente, sin más ayuda que la información recopilada en este manual.

A través del desarrollo de este documento, se han destacado las características del esquema que se desea implantar, partiendo de un conocimiento más exacto de todos aquellos requerimientos indispensables y de los controles que apoyen a una mejor administración, tanto de los recursos de los sistemas como de las aplicaciones que residen en los equipos.

Se ha determinado que es necesario contar con áreas perfectamente acondicionadas y con un mínimo de riesgo para la operación de equipos de procesamiento, en base a estándares y principios básicos que permitan mantenerlo a salvo en caso de cualquier contingencia y/o siniestro. De igual forma existirán controles internos para mantener un cierto grado de acceso controlado y que cumpla con las características definidas; esto en función de las necesidades de cada organización.

Por otro lado y como parte medular para la salvaguarda de la información, se establecieron aquellos controles lógicos que nos permitirán administrar de una mejor manera los accesos a los sistemas de información así como a las aplicaciones; dichos controles y medidas preventivas/correctivas establecerán el grado de seguridad y las herramientas necesarias para determinar cuándo, dónde y cómo se ha intentado violar la seguridad.

Por último, es importante señalar que la aplicación del esquema integral de seguridad implica la participación, los esfuerzos y la disponibilidad de todo personal de la organización a partir del desarrollo de una conciencia y/o cultura de seguridad informática a nivel general, empezando desde los altos directivos para la mejora continua de medidas y controles con un grado mayor de protección y funcionalidad con lo que se logrará garantizar la integridad, confidencialidad y disponibilidad de la información.

BIBLIOGRAFÍA

- Dirección General de Normas, *Normas Técnicas de Instalaciones Electricas (NTIE),* Ediciones Andrade, S.A., México, 1993.
- Linda Walsh, *Computer Security Basics*, Editorial O'Reilly, U.S.A., 1995.
- Computer Security Institute, *23th Annual Conference Proceedings about Computer Security,* U.S.A., 1996.
- Autores varios, *Manager's Guide to Information Protection,* Computer Security Institute, U.S.A., 1997.
- Carlos A. Soriano y Fernando Navarro, *Instalaciones de Salas Informáticas,* Editorial Parainfo, S.A., España, 1989.
- Philip Fites & Martin P. J. Kratz, *Information System Security,* International Thomson Publishing, U.S.A., 1996.
- Marc Farley, Tom Stearns & Jeffrey Hsu, *Seguridad e Integridad de Datos*, Editorial Mc. Graw Hill, México, 1997

A

GLOSARIO DE TÉRMINOS

Texto encriptado.- Datos producidos a través del uso de encripción, en donde el contenido semántico de los datos resultantes no está disponible.

Texto Claro.- Dato comprensible, el contenido de la semántica la cual está disponible.

Sistema de codificación.- Cualquier sistema de comunicación en la que se usan grupos de símbolos para representar elementos del texto plano de longitud variante. En el sentido más amplio, una manera de convertir información de forma satisfactoria para comunicaciones o encripción, por ejemplo, lenguaje codificado, clave Morse, códigos de teletipos. Un sistema criptográfico en el cual los equivalentes criptográficos (usualmente llamados grupos de codificación) típicamente consisten de letras, dígitos o ambas, en combinaciones sin sentido son sustituidos por elementos de texto claro, los cuales pueden ser palabras, frases o sentencias.

Criptografía.- El arte o ciencia en lo que se refiere a los principios, formas y métodos para interpretar texto plano incomprensible y para convertir mensajes encriptados en

forma comprensible. La disciplina la cual incorpora principios, formas y métodos para la transformación en orden de los datos y ocultar el contenido de su información, para esconder su información, previniendo su modificación no detectada y/o prevenir su uso no autorizado.

Nota: La criptografía determina los métodos usados en la encripción y desencripción.

Llave de encripción de datos.- Una llave criptográfica usada para encriptamiento (y desencriptamiento) de datos.

Estándar de encripción de datos.- Un algoritmo de encripción libre adoptado por el Instituto Nacional de Estándares y Tecnología para uso público.

Integridad de los datos.- La propiedad que tienen los datos de que no se han alterado o destruido en una manera no autorizada.

Desencripción o desencriptamiento.- La inversión de una encripción reversible correspondiente.

Desencriptor.- Convertir, por el uso de la llave apropiada, texto encriptado en su equivalente texto plano.

Firma Digital.- Datos añadidos a, o una transformación criptográfica de, una unidad de datos que permite a un receptor de la unidad de datos y protege contra la falsificación por el receptor.

Encriptador.- Convertir texto plano en una forma no comprensible por métodos de un sistema de cifras.

Encriptamiento.- La transformación criptográfica de datos para producir texto encriptado.

Nota: La encripción puede ser irreversible, en cuyo caso el proceso de desencripción correspondiente no puede realizarse factiblemente.

Codificar.- Convertir texto plano en una forma no comprensible por medio de un sistema de códigos.

Encriptor.- Convertir texto plano en forma no comprensible por medio de un criptosistema.

Encripción.- El proceso de transformación de datos a una forma no comprensible, de tal forma que los datos originales no pueden obtenerse (primera forma de encripción) o no pueden obtenerse sin usar el proceso inverso de desencripción (segunda forma de encripción).

Key.- Una secuencia de símbolos que controlan las operaciones de encripción y desencripción.

Manejo de llaves.- La generación, almacenamiento, distribución, eliminación y aplicación de llaves de acuerdo con una política de seguridad.

Encripción fin a fin.- Encripción de datos dentro de o en el sistema fuente final, con el desciframiento correspondiente que sólo ocurre dentro de o en el sistema de destino final.

Encripición de enlace.- La aplicación de operaciones de encripción en línea a un enlace de un sistema de comunicaciones para que toda la información que pasa sobre el enlace sea encriptada en su totalidad. La encripción fin a fin dentro de cada enlace en una red de comunicaciones.

Encripción enlace por enlace.- La aplicación individual de encripción de datos en cada enlace de un sistema de comunicaciones.

Texto plano.- Texto comprensible o señales que tienen significado y el cual puede leerse o representarse sin la aplicación de cualquier desencripción.

Repudiación.- Rechazo de una de las entidades involucradas en una comunicación habiendo participado en todo o parte de ella.

Análisis de tráfico.- La deducción de información de la observación de flujos de tráfico (presencia, ausencia, cantidad, dirección y frecuencia).

Relleno de tráfico.- La generación de instancias falsas de comunicación, unidades de datos falsas y/ o datos falsos dentro de las unidades de datos.

Nivel de acceso.- La porción jerárquica del nivel de seguridad usado para identificar la sensibilidad de los datos y el margen de autorización de usuarios. El nivel de acceso, junto con las categorías no-jerárquicas, forman la etiqueta de sensibilidad de un objeto.

Tipo de acceso.- La naturaleza de un acceso correcto a un dispositivo, programa o archivo en particular (como leer, escribir, ejecutar, añadir, modificar, borrar y crear).

Agregación.- Pueden determinarse los sistemas de datos individuales y elementos de los datos ser no clasificados y ser de una categoría de sensibilidad específica. Cuando esos datos se combinan con otro datos, la totalidad de la información puede ser clasificada o en una categoría de sensibilidad más alta, con los requisitos de protección más altos.

Recurso de Granularidad.- El grado al que los recursos son considerados como recursos individuales o como una clase.

Autorización.- El otorgar a un usuario, programa o proceso el derecho de acceso. El privilegio concedido a un individuo por un oficial designado para accesar información.

Clasificación.- Una determinación que la información requiere, en el interés de seguridad nacional, un grado específico de protección contra el descubrimiento desautorizado junto con una designación que significa que semejante determinación se ha hecho.

Criticalidad.- Un concepto relacionado a la misión que soporta el sistema automatizado y el grado que la misión es dependiente en el sistema. Este grado de dependencia corresponde al efecto en la misión en caso del rechazo del servicio, modificación, o

destrucción de datos o software. Un parámetro indicando el grado de dependencia de la organización en un recurso.

Custodio de los datos.- El grupo o individuo que ha sido confiada la posesión de, y responsabilidad para, la seguridad de los datos especificados.

Dato.- Una representación de hechos, conceptos, información o instrucciones de una manera conveniente para la comunicación, interpretación o proceso por humanos. Una categoría del recurso que consiste en la información manejada por la organización.

Propietario de los datos.- La autoridad reglamentaria responsable para un tipo particular o categoría de información, o el individuo o organización responsable para los datos actuales ahí contenidos.

Base de datos.- Un conjunto de datos coleccionados y organizados en una manera significativa para un propósito en particular.

Clasificación predefinida.- Una clasificación temporal, reflejando la clasificación más alta a procesarse en un sistema automatizado. La clasificación predefinida está incluida en la declaración del resguardo añadida al producto.

Documentación.- Una categoría del recurso consistente de manuales, listados, etc. Debe también incluir planes de recuperación y el resultado del análisis de la amenaza.

Granularidad.- La fineza relativa o tosquedad por las que un mecanismo puede ajustarse, la frase " la granularidad de un solo usuario " significa que el mecanismo de control de acceso puede ajustarse para incluir o excluir a cualquier simple usuario.

Información.- Los términos, dato, información, material, documentos y temas son considerados sinónimos y se usan intercambiablemente en este orden.

Etiqueta.- Una pieza de información que representa el nivel de seguridad de un objeto y que describe la sensibilidad de la información en el objeto. La marca de un elemento de

información para reflejar su clasificación y su conjunto de categorías que representan la sensibilidad de la información.

a) *Etiqueta interna.*- El marcado de un elemento de información para reflejar la clasificación y sensibilidad de la información dentro de los confines del medio que contiene la información.

b) *Etiqueta externa.*- La marca visible por fuera del medio o la cubierta del medio que refleja la clasificación y sensibilidad de la información residente dentro del medio.

Dato privilegiado.- Datos no sujetos a las reglas usuales debido a algunas circunstancias especiales.

Datos sensibles.- Datos que requieren protección debido al riesgo y magnitud de pérdida o daño que podrían ser el resultado del descubrimiento inadvertido o deliberado, causando alteración y/o destrucción de los datos .

Información sensible.- Información que, determinado por una autoridad competente, debe protegerse porque su descubrimiento no autorizado, alteración, pérdida o destrucción causarán daños perceptibles por lo menos a alguien o algo. Cualquier información la cuál requiere un grado de protección y la cuál no debe hacerse generalmente disponible.

Sensibilidad.- La característica de un recurso que implica su valor o importancia, y puede incluir su vulnerabilidad.

Datos técnicos.- Información clasificada o no clasificada de cualquier tipo que puede usarse o adaptarse para usar en el diseño, producción, fabricación, restauración, reparación, procesamiento, ingeniería, desarrollo, operación o reconstrucción de productos.

Prueba de datos.- Una categoría del recurso que consiste de información usada para determinar la aplicabilidad, eficiencia o precisión de los sistemas.

Aceptancia.- La condición que existe cuando una facilidad o sistema generalmente reúnen los estándares de desempeño técnicos y requisitos de seguridad

Aplicación.- Esas partes de un sistema, incluyendo partes del sistema operativo que no son responsables para reforzar la política de seguridad.

Software de aplicación.- Las rutinas y programas diseñados por, o para los usuarios del sistema y clientes.

Administración de la configuración.- La administración de cambios hechos al h*ardware* del sistema, *software*, *firmware* y documentación a lo largo del desarrollo y la vida operacional del sistema.

Canal secreto.- Un canal de comunicación que permite dos procesos cooperando para transferir información de una manera que viole la política de seguridad del sistema.

Canal de almacenaje secreto.- Un canal secreto que involucra la escritura directa o indirecta de una localidad de almacenamiento por un proceso y la lectura directa o indirecta de la localidad de almacenamiento por otro proceso.

Contaminación de los datos.- Un proceso deliberado o accidental o acto que produce un cambio en la integridad del dato original. El proceso por el cual los errores de los elementos de datos almacenados en sistemas de información automatizados se propagan durante su uso repetido, llevando a base de datos inestables.

Verificación de diseño.- El uso de técnicas de verificación usualmente asistidas por computadora, para demostrar una correspondencia matemática entre un modelo abstracto y una especificación formal del sistema.

Protección del archivo.- El agregado de todos los procesos y procedimientos establecidos en un sistema automatizado y diseñado para inhibir el acceso no autorizado, contaminación o eliminación de un archivo.

Seguridad del archivo.- Los medios por los cuales el acceso a los archivos de la computadora únicamente está limitado a los usuarios autorizados.

Controles internos.- El plan de organización y todo de los métodos y medidas adoptadas dentro de una agencia para salvaguardar sus recursos, asegurar la exactitud y fiabilidad de su información, asegurar el apego a las leyes aplicables, regulaciones y políticas, y promover la economía operacional y eficiencia.

Privacidad.- El derecho de individuos y organizaciones para controlar la colección, almacenamiento y diseminación de su información o información sobre ellos.

Puerta trasera.- Un mecanismo oculto de *software* o *hardware* que permite engañar a los mecanismos de protección del sistema. Desarrolladores de *software* frecuentemente introducen puertas traseras en su código que les permite ingresar al sistema y realizar ciertas funciones.

Caballo de Troya.- Un programa de computadora con una aparente o función realmente útil que contiene funciones adicionales que clandestinamente explotan las autorizaciones legítimas del proceso evocado para el perjuicio de la seguridad.

B

CONVENIO DE RESPALDO

CONVENIO DE RESPALDO ENTRE CENTROS DE CÓMPUTO PARA EL PLAN DE CONTINGENCIA

Convenio que celebran por una parte el **Centro de cómputo A**, que en lo sucesivo se denominará "**CCA**" representado por el **Nombre del responsable del centro de cómputo A**, y por otra parte el **Centro de cómputo B**, que en lo sucesivo se denominará "**CCB**" representado por el **Nombre del responsable del centro de cómputo B** de acuerdo con las siguientes declaraciones y cláusulas:

DECLARACIONES

1.- Declara el "**CCA**" a través de su representante el **Nombre del responsable del centro de cómputo A** que tiene facultades para celebrar el presente convenio, con la autorización de **Nombre de la empresa**, y que tiene su domicilio en **Domicilio en donde se encuentra ubicado el centro de cómputo A.**

2.- Declara "**CCB**" a través de su representante el **Nombre del responsable del centro de cómputo B** que tiene facultades para celebrar el presente convenio, con la autorización de **Nombre de la empresa**, y que tiene su domicilio en **Domicilio en donde se encuentra ubicado el centro de cómputo B.**

3.- Declaran ambas partes que desean celebrar el presente convenio para brindarse mutuamente soporte o respaldo en caso de contingencia, denominando **Instalación Huésped** a la que solicite apoyo e **Instalación Anfitriona** a la que lo otorgue.

4.- Declaran las partes que cuentan con la infraestructura informática necesaria en equipos, programas, personal e instalaciones para otorgar soporte a la otra parte, según anexos "A" y "B" y dar formal cumplimiento a las siguientes:

CLÁUSULAS

1.- "**CCA**" se obliga por éste convenio a:

1.1 Dar apoyo al "**CCB**" en caso de existir alguna falla en sus equipos de cómputo ó debido a cargas de trabajo excesivas a través de la utilización de sus instalaciones, equipos y periféricos, siguiendo el procedimiento establecido y apegándose a las condiciones de soporte detalladas en el anexo "D".
1.2 Proteger y almacenar en su cintoteca cintas, DAT's, Diskettes, o algún otro tipo de Almacenamiento Magnético que haya sido dejado bajo su tutela por "**CCB**"
1.3 Custodiar los elementos y dispositivos citados en el anexo "C".

2.- "**CCB**" se obliga por este convenio a:

2.1 Dar apoyo al "**CCA**" en caso de existir alguna falla en sus equipos de cómputo ó debido a cargas de trabajo excesivas a través de la utilización de sus instalaciones, equipos y periféricos, siguiendo el procedimiento establecido y apegándose a las condiciones de soporte detalladas en el anexo "D".
2.2 Proteger y almacenar en su cintoteca cintas, DAT's, Diskettes, o algún otro tipo de Almacenamiento Magnético que haya sido dejado bajo su tutela por "**CCA**".
2.3 Custodiar los elementos y dispositivos citados en el anexo "C".

3.- La Instalación Huésped será responsable tanto de las actividades realizadas por su personal en la instalación anfitriona, como de los resultados obtenidos durante el tiempo que se haga uso de las instalaciones y equipos. Asimismo será responsable de apegarse a los procedimientos y normas de seguridad de la Instalación Anfitriona.

4.- La vigencia de este convenio es indefinida, pudiendo cualquiera de las partes darlo por concluido por medio de un escrito con 30 días de anticipación.

5.- Para todo aquello no previsto en el cuerpo de éste convenio, las partes convienen en resolverlo de mutuo acuerdo.

6.- Las partes convienen en crear una comisión formada por dos representantes de cada una de las partes, y que empezará a funcionar dentro de los diez días hábiles siguientes a la firma del presente convenio. Esta comisión se abocará a determinar:

6.1 Como garantizar la seguridad y confidencialidad de la información para evitar su destrucción accidental o su acceso no autorizado.
6.2 El soporte que otorgará cada una de las partes.
6.3 Todos los aspectos técnicos que en una u otra medida deban ser considerados.

6.4 La forma en que deberán comunicarse cada uno de los Centros de Cómputo respecto a los cambios en equipo y software que afecten la aplicación del convenio.

6.5 La comisión se podrá abocar a enriquecer el contenido de este convenio a través de uno o más adendums, dándolos a conocer al área de Seguridad.

7.- El personal responsable de realizar el objeto de este Convenio es: por parte del "**CCA**", el **Nombre del responsable del CCA** y por el "**CCB**" el **Nombre del responsable del CCB**.

8.- Si durante la prestación del respaldo, el personal huésped hiciera mal uso del equipo, las partes acuerdan, que será responsabilidad del Responsable del centro de cómputo o su equivalente huésped, restituir los daños que del mismo resultaran.

9.- En caso de que sobrevenga alguna controversia que no pueda resolver la comisión, las partes se someterán a la decisión tomada por los directivos de la empresa.

Este convenio se firma por las partes en original y cuatro copias el día __ de _____de 199_.

RESPONSABLES DE LAS INSTALACIONES

POR "CCA" **POR "CCB"**

Nombre del responsable del CCA

Nombre del responsable del CCB

TESTIGOS

POR "CCA" **POR "CCB"**

Nombre del Responsable de Procesos de Datos del CCA

Nombre del Responsable de Procesos de Datos del CCB

ANEXO "A"

INFRAESTRUCTURA REQUERIDA POR EL CENTRO DE CÓMPUTO A ("CCA") EN CASO DE CONTINGENCIA

INSTALACIONES "CCA"

Ubicación del Inmueble: **Calle y número.**
Col.
C.P.
Ciudad
Tel. **Directo**
Conmutador:
Extensiones:

Responsable del centro de cómputo: _____

Suplente : _____

CONFIGURACIÓN DE LOS EQUIPOS REQUERIDOS:

CANTIDAD	DESCRIPCIÓN	CAPACIDAD MÍNIMA
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

SOFTWARE:

SISTEMA OPERATIVO: _____
VERSIÓN _____

PROGRAMAS: _____
_____
_____
_____

ANEXO "B"

INFRAESTRUCTURA REQUERIDA POR EL CENTRO DE CÓMPUTO B ("CCB") EN CASO DE CONTINGENCIA

INSTALACIONES "CCB"

Ubicación del Inmueble: **Calle y número.**
Col.
C.P.
Ciudad
Tel. **Directo**
Conmutador:
Extensiones:

Responsable del centro de cómputo: _____

Suplente: _____

CONFIGURACIÓN DE LOS EQUIPOS REQUERIDOS:

CANTIDAD	DESCRIPCIÓN	CAPACIDAD MÍNIMA
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

SOFTWARE:

SISTEMA OPERATIVO: _____
VERSIÓN _____

PROGRAMAS: _____
_____
_____
_____

ANEXO "C"

CARTA DE SOLICITUD DE APOYO

Ciudad de _____, a __de _____ de 199_.

Responsable del Centro de Cómputo
Domicilio Instalación Anfitriona
P r e s e n t e

Con base en el Convenio de Soporte de fecha dd/mm/aa, solicito a usted apoyo para nuestro Centro de Cómputo, a partir del día _____ del mes de _____, a las _____ hrs. con una duración estimada hasta el día ___del mes de _____.a las _____ hrs.

Lo anterior en virtud de que _____(Explicación de la Causa)_____.

Anexo encontrará la lista del personal autorizado para efectuar la operación de nuestras aplicaciones, el inventario de suministros que ingresarán a sus instalaciones y el inventario de dispositivos que utilizaremos de su cintoteca. Asimismo le informo que la coordinación de actividades del mismo estará a cargo del Sr. _____.

Agradeciendo de antemano sus finas atenciones, me es grato reiterarme a sus ordenes para cualquier aclaración.

A T E N T A M E N T E,

(El Responsable del Centro de Cómputo Huésped.)

CC: Director General

LISTA DEL PERSONAL QUE ASISTIRÁ A LAS INSTALACIONES

NOMBRE	CARGO
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

INVENTARIO DE ELEMENTOS Y SUMINISTROS DEL CENTRO HUÉSPED, QUE INGRESARAN AL CENTRO ANFITRIÓN

CANTIDAD	DESCRIPCIÓN DEL CONTENIDO

INVENTARIO DE ELEMENTOS Y DISPOSITIVOS QUE SERÁN UTILIZADOS DE LA CINTOTECA ANFITRIONA

No. DE CINTA	FECHA	CONTENIDO

ANEXO "D"

CONDICIONES DE SOPORTE

La Normatividad a la que deberá someterse el personal huésped que requiera apoyo en caso de contingencia y el personal anfitrión que lo proporcione es la siguiente, como mínimo indispensable:

a) Toda persona que tenga necesidad de acceso al edificio del centro de cómputo anfitrión, deberá identificarse e indicar el motivo de su visita.

b) En el área de recepción deberá registrarse en el control de visitantes anotando lo siguiente:

- Nombre completo
- Persona ó Departamento a contactar
- Motivo
- Hora de entrada/salida
- Tipo de usuario

c) Los usuarios del área de producción tendrán acceso únicamente al mostrador de la mesa de control, para la entrega de documentos, recepción de reportes y/o dispositivos magnéticos.

Sistema Operativo

El Sistema Operativo debe ser estándar en las instalaciones suscritas al convenio, persiguiéndose con ello, que al requerirse el respaldo de equipo, sea transparente para su utilización inmediata, comprometiéndose a mantener actualizada la documentación de programas, de equipo auxiliar y de Cómputo detallado en los anexos "A" y "B".