INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIDAD CULHUACÁN

PROPUESTA DEL DISEÑO DE UN PLAN DE RECUPERACION DE DESASTRES (DRP) PARA CONTROL ESCOLAR DE LA E.S.I.M.E. UNIDAD CULHUACAN

TESINA

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

INGENIERO EN COMUNICACIONES Y ELECTRONICA

P R E S E N T A N

HERNÁNDEZ VARGAS IRVING OMAR

MARTINEZ ARCINIEGA ARMANDO

MARTINEZ GUZMAN JOSE LUIS

REYES ALONSO DIANA GABRIELA

ASESOR:

M. EN C. RAYMUNDO SANTANA ALQUICIRA

INDICE

INTRODUCCIÓN

Durante varias décadas, los japoneses han desarrollado diversos programas para enfrentar los terremotos que permanentemente tienen lugar en su país. Su trabajo de preparación y contingencias no sólo ha consistido en construir infraestructura capaz de resistir los movimientos telúricos, sino que también ha contemplado un amplio proceso de educación a la población. Este es un ejemplo destacable de cómo un programa para enfrentar emergencias puede ayudar a salvar muchas vidas y a reducir los daños causados por los desastres naturales a los que se enfrenten.

Con el transcurso del tiempo la tecnología avanza a pasos agigantados, y con ello las empresas y las instituciones se hacen dependientes de esta, ello con lleva que muchas se vean afectadas en sus labores si su tecnología informática ha sido afectada por algún tipo de contingencia.

Es por ello que dichas empresas e Instituciones buscan alta disponibilidad de servicios a sus clientes, utilizando técnicas basadas en los Planes de recuperación de desastres (DRP *Disaster Recovery Plan).*

La Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culiacán no es la excepción, ella no cuenta con un plan adecuado el cual garantice una recuperación de sus actividades en un tiempo menor al crítico.

El propósito de este proyecto es el de entregar la propuesta del diseño, un plan de recuperación de desastres el cual presentará la situación actual de la Escuela con relación a su capacidad de recuperación de operaciones en caso de sufrir una contingencia que afecte a la tecnología informática de la misma.

OBJETIVO:

El propósito de este proyecto es el de entregar el análisis del ambiente tecnológico que presentará la situación actual de la escuela con relación a su capacidad de recuperación de operación en caso de sufrir una contingencia.

PLANTEAMIENTO DEL PROBLEMA.

Existen varias empresas que con el paso del tiempo han visto como se pierde su información por diferentes causas, que al no contemplar respaldos alternos pierden varios días de productividad y sus clientes se ven afectados en los servicios que ofrece al no tener una alta disponibilidad.

ALCANCE

Se realizará el análisis de la situación actual de la red en ESIME Culhuacán para la recuperación de de los servicios en el caso de una contingencia; así como la propuesta de equipos para una posible aplicación.

JUSTIFICACION

Mantener disponible la información de la institución así como diversos usos que se requieren teniendo así una solución alternativa.

CAPITULO I

INTRODUCCIÓN A LAS REDES

1.1 Antecedentes de las redes

Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras, así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte, almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

El viejo modelo de tener una sola computadora para satisfacer todas las necesidades de una organización se está reemplazando con rapidez por otro que considera un número grande de computadoras separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computadoras, se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones, son ejemplo de esto.

Considerando que conectar una red de computadoras era hasta hace poco, un lujo para muchas empresas y organizaciones, el auge en la popularidad de Internet y la necesidad competitiva para acceder a la información de forma instantánea, lo ha hecho obligatorio. Adicionalmente, la madurez de la tecnología de las redes, le ha convertido ahora en un medio más fidedigno y por consiguiente más deseable como un reemplazo para otros mecanismos propietarios o para tecnologías de comunicaciones más lentas en los entornos corporativos.

1.1.1 Objetivos de las redes

Las redes en general, se utilizan para "compartir recursos", y uno de sus objetivo es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a varios kilómetros de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además, la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo / rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor.

1.1.2 Aplicación de las redes

Para dar una idea sobre algunos de los usos importantes de redes de computadoras, tenemos tres ejemplos: el acceso a programas remotos, el acceso a bases de datos remotas y facilidades de comunicación.

La posibilidad de tener un precio mas bajo se debe a que el enlace de una llamada telefónica normal utiliza un circuito caro y en exclusiva durante todo el tiempo que dura la llamada, en tanto que el acceso a través de una red, hace que solo se ocupen los enlaces de larga distancia cuado se están transmitiendo los datos.

Otra forma que muestra el amplio potencial del uso de redes, es su empleo como medio de comunicación (INTERNET). Como por ejemplo, el tan conocido por todos, correo electrónico (e-mail), que se envía desde una terminal, a cualquier persona situada en cualquier parte del mundo que disfrute de este servicio. Además de texto, se pueden enviar fotografías e imágenes.

1.2 Clasificación de las redes

Un número muy grande de redes se encuentran funcionando, actualmente, en todo el mundo, algunas de ellas son redes públicas operadas por proveedores de servicios portadores comunes o PTT, otras están dedicadas a la investigación, también hay redes en cooperativas operadas por los mismos usuarios y redes de tipo comercial o corporativo.

Las redes, por lo general, difieren en cuanto a su historia, administración, servicios que ofrecen, diseño técnico y usuarios. La historia y la administración pueden variar desde una red cuidadosamente elaborada por una sola organización, con un objetivo muy bien definido, hasta una colección específica de máquinas, cuya conexión se fue realizando con el paso del tiempo, sin ningún plan maestro o administración central que la supervisara.

1.2.1 Redes de comunicación

La posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas; cargar aplicaciones desde puntos de ultramar; enviar mensajes a otros países y compartir ficheros todo ello desde una computadora personal de las últimas décadas.

1.2.2 Redes de área local (LAN)

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN) como forma de normalizar las conexiones entre las máquinas que se utilizan como sistemas. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable coaxial al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio.

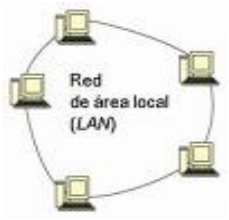


Fig. 1 Red Lan

La LAN más difundida, la Ethernet, utiliza un mecanismo denominado ***Call Sense Multiple Access-Collision Detect*** (CSMA-CD). Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando. Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante.

Hay topologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios, y el control de los recursos de la red.

Ethernet. Es la tecnología más popular para redes LAN usada actualmente, es popular porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación.

Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría los usuarios de la informática actual. La norma de Ethernet fue definida por el Instituto para los Ingenieros Eléctricos y Electrónicos (IEEE) como IEEE Standard 802.3. Adhiriéndose a la norma de IEEE, los equipos y protocolos de red pueden ínter operar eficazmente.

Fastethernet. Para redes Ethernet que necesitan mayores velocidades, se estableció la norma Fast Ethernet (IEEE 802.3u). Esta norma elevó los límites de 10 Megabits por segundo (Mbps.) de Ethernet a 100 Mbps. con cambios mínimos a la estructura del cableado existente.

Hay tres tipos de Fast Ethernet: 100BASE-TX para el uso con cable UTP de categoría 5, 100BASE-FX para el uso con cable de fibra óptica, y 100BASE-T4 que utiliza un par de cables más para permitir el uso con cables UTP de categoría 3.

La norma 100BASE-TX se ha convertido en la más popular debido a su íntima compatibilidad con la norma Ethernet 10BASE-T. En cada punto de la red se debe determinar el número de usuarios que realmente necesitan las prestaciones más altas, para decidir que segmentos del troncal necesitan ser específicamente reconfigurados para 100BASE-T y seleccionar el hardware necesario para conectar dichos segmentos "rápidos" con los segmentos 10BASE-T existentes.

1.2.3 Redes de área extensa (WAN)

Cuando se llega a un cierto punto deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos.

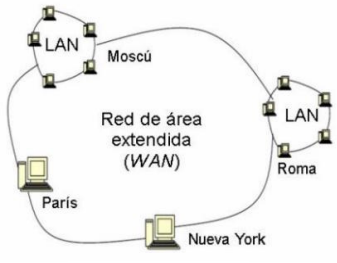


Fig. 2 Red Wan

Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extensa (WAN). Casi todos los operadores de redes

nacionales ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad adecuados para la interconexión de las LAN.

Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevee que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

1.3 Capas del modelo OSI

El modelo de referencia OSI es el modelo principal para las comunicaciones por red. Aunque existen otros modelos, en la actualidad la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI, especialmente cuando desean enseñar a los usuarios cómo utilizar sus productos. Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

El modelo de referencia OSI permite que los usuarios vean las funciones de red que se producen en cada capa. Más importante aún, el modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. Además, puede usar el modelo de referencia OSI para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación (por ej., hojas de cálculo, documentos, etc.), a través de un medio de red hasta otro programa de aplicación ubicado en otra computadora de la red, aún cuando el transmisor y el receptor tengan distintos tipos de medios de transmisión.

Fig. 3 Capas del modelo OSi

1.3.1 Capa física

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y

la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Así como de transmitir los bits de información a través del medio, se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uní o bidireccional (simplex, dúplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); o electromagnéticos.

Estos últimos, dependiendo de la frecuencia /longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión

1.3.1.1 Medios de transmisión

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

Par trenzado (*UTP, unshielded twisted pair*) Es el medio guiado más barato y más usado. Consiste en un par de cables, embutidos para su aislamiento, para cada enlace de comunicación. Debido a que puede haber acoples entre pares, estos se trenza con pasos diferentes. La utilización del trenzado tiende a disminuir la interferencia electromagnética.

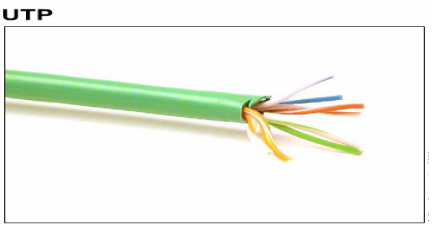


Fig. 4 Cable de par trenzado

Este tipo de medio es el más utilizado debido a su bajo coste (se utiliza mucho en telefonía) pero su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance.

Con estos cables, se pueden transmitir señales analógicas o digitales. Es un medio muy susceptible a ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas.

Par trenzado apantallado y sin apantallar. Los pares sin apantallar son los más baratos aunque los menos resistentes a interferencias aunque se usan con éxito en telefonía y en redes de área local. A velocidades de transmisión bajas, los pares apantallados son menos susceptibles a interferencias, aunque son más caros y más difíciles de instalar.

Cable coaxial. Consiste en un cable conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre por otra capa aislante que es la funda del cable.

Fig. 5 Cable coaxial

Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, poca interferencia y permite conectar más estaciones.

Se suele utilizar para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc... Se utiliza para transmitir señales analógicas o digitales.

Sus inconvenientes principales son: atenuación, ruido térmico, ruido de ínter modulación. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

Fibra óptica. Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica. Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta.

El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etc.

Fig. 6 Fibra óptica

Es un medio muy apropiado para largas distancias e incluso últimamente para LAN's . Sus beneficios frente a cables coaxiales y pares trenzados son:

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

El método de transmisión es: los rayos de luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable, entonces sólo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo. Son precisamente esos rayos que inciden en un cierto rango de ángulos los que irán rebotando a lo largo del cable hasta llegar a su destino. A este tipo de propagación se le llama multimodal. Si se reduce el radio del núcleo, el rango de ángulos disminuye hasta que sólo sea posible la transmisión de un rayo, el rayo axial, y a este método de transmisión se le llama monomodal.

Los inconvenientes del modo multimodal es que debido a que dependiendo al ángulo de incidencia de los rayos, estos tomarán caminos diferentes y tardarán más o menos tiempo en llegar al destino, con lo que se puede producir una distorsión (rayos que salen antes pueden llegar después), con lo que se limita la velocidad de transmisión posible .

Hay un tercer modo de transmisión que es un paso intermedio entre los anteriormente comentados y que consiste en cambiar el índice de refracción del núcleo. A este modo se le llama multimodo de índice gradual.

Los emisores de luz utilizados son: LED (de bajo coste, con utilización en un amplio rango de temperaturas y con larga vida media) y ILD (más caro, pero más eficaz y permite una mayor velocidad de transmisión).

Medios de transmisión no guiados. Se utilizan medios no guiados, principalmente el aire. Se radia energía electromagnética por medio de una antena y luego se recibe esta energía con otra antena.

Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional. En la direccional, toda la energía se concentra en un haz que es emitido en una cierta dirección, por lo que tanto el emisor como el receptor deben estar alineados. En el método omnidireccional, la energía es dispersada en múltiples direcciones, por lo que varias antenas pueden captarla. Cuanto mayor es la frecuencia de la señal a transmitir, más factible es la transmisión unidireccional. Por tanto, para enlaces punto a punto se suelen utilizar microondas (altas frecuencias). Para enlaces con varios receptores posibles se utilizan las ondas de radio (bajas frecuencias). Los infrarrojos se utilizan para transmisiones a muy corta distancia (en una misma habitación).

Microondas terrestre. Suelen utilizarse antenas parabólicas. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

Fig.7 Antenas de Microondas Terrestres

La principales causas de pérdida son: la atenuación que aumenta con el la distancia, las lluvia; las interferencias es otro inconveniente de las microondas, estos sistemas, pude haber más solapamientos de señales.

Microondas por satélite. El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.

Fig. 8 Antenas de microondas por satélite

Se suele utilizar este sistema para:

- Difusión de televisión.
- Transmisión telefónica a larga distancia.
- Redes privadas.

El rango de frecuencias para la recepción del satélite debe ser diferente del rango al que este emite, para que no haya interferencias entre las señales que ascienden y las que descienden.

Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores, ha de tenerse cuidado con el control de errores y de flujo de la señal.

Las diferencias entre las ondas de radio y las microondas son:

- Las microondas son unidireccionales y las ondas de radio omnidireccionales.
- Las microondas son más sensibles a la atenuación producida por la lluvia.
- En las ondas de radio, al poder reflejarse estas ondas en el mar u otros objetos, pueden aparecer múltiples señales "hermanas".

1.3.2 Capa de enlace de datos

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

1.3.3 Capa de red

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sea necesario, para hacer llegar los datos al destino. Los equipos encargados de realizar este encaminamiento se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés ***routers*** y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande). La PDU de la capa de red es Paquetes.

1.3.4 Capa de transporte

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación.

En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte.

Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice.

De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas anteriores, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.

Para finalizar, podemos definir a la capa de transporte como: capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independiente del tipo de red física que utilice. La PDU de la capa de transportes son segmentos.

1.3.5 Capa de sesión

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).
- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión entre dos máquinas, se pueda efectuar para las operaciones de principio a fin, reanudándolas en caso de interrupción.

1.3.6 Capa de presentación

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres, números, sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos. Esta capa también permite cifrar los datos y comprimirlos.

1.3.7 Capa de aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (HyperText Transfer Protocol) el protocolo bajo la WWW
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros
- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de TCP/IP) envío y distribución de correo electrónico
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final
- SSH (Secure Shell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

1.4 Seguridad en las redes

1.4.1 Características en las redes

Seguridad. Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder datos de carácter confidencial. La norma Data Encryption System (DES) para protección de datos informáticos, implantada a finales de los años setenta, se ha visto complementada recientemente por los sistemas de clave pública que permiten a los usuarios codificar y decodificar con facilidad los mensajes sin intervención de terceras personas.

Privacidad. Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

Integridad. Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

Disponibilidad. Se refiere a la continuidad operativa de la entidad, la perdida de disponibilidad puede implicar, la perdida de productividad o credibilidad de la institución. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar perdidas importantes.

Confidencialidad. Se refiere a la protección de datos frente a la difusión no autorizada, la perdida de confidencialidad puede resultar en problemas legales. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal, etc.

1.4.2 Información en las redes

Datos. Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

Bases de datos. Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

- Las características que presenta un DBMS son las siguientes:
- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.

Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

Sistema de información. Un sistema informático utiliza computadoras para almacenar los datos de una organización y ponerlos a disposición de su personal. Pueden ser tan simples como en el que una persona tiene una computadora y le introduce datos, los datos pueden ser registros simples como ventas diarias, se produce una entrada por cada venta.

Sin embargo la mayor parte de los sistemas son más complejos que el enunciado anteriormente. Normalmente una organización tiene más de un sistema de computadoras para soportar las diferentes funciones de la organización, ya sean de venta, recursos humanos, contabilidad, producción, inventario, etc.

Los sistemas de información tienen muchas cosas en común. La mayoría de ellos están formados por personas, equipos y procedimientos. Al conjugar una serie de elementos como hombres y computadoras se hace imprescindible tomar medidas que nos permitan una continuidad en la operatividad de los sistemas para no ver afectados los objetivos de las mismas y no perder la inversión de costos y tiempo.

La figura 9 nos muestra en un sentido amplio lo que se puede considerar un Sistema de Información (SI) como un conjunto de componentes que interactúan para que la empresa pueda alcanzar sus objetivos satisfactoriamente.

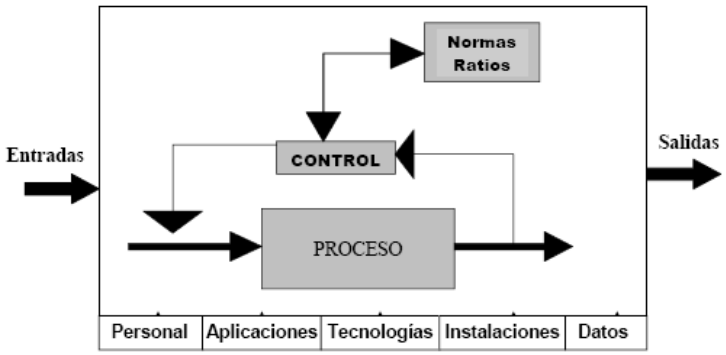


Fig. 9 Sistema de Información

Los componentes o recursos de un Sistema de Información son los siguientes:

- Datos: En general se consideran datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- Aplicaciones: Se incluyen los manuales y las aplicaciones informáticas.
- Tecnología: El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- Instalaciones: En ellas se ubican y se mantienen los sistemas de información.
- Personal: Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos.

CAPITULO II

ASPECTOS GENERALES DE SEGURIDAD EN INFORMACIÓN

2.1 Ataques

Ataque. Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

2.1.2 Ataques activos

Ataque activo. Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

Ingeniería social. Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele tolo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente (generalmente es así), puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y contraseñas.

Ataques de modificación-daño. Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aún así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Amenaza. Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

Incidente. Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.

Golpe. Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

2.1.3 Ataques pasivos

Ataque pasivo. Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

Ataques de monitorización. Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de establecer sus vulnerabilidades y posibles formas de acceso futuro.

Errores de diseño, implementación y operación. Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, Internet, correo electrónico y todas clase de servicios informático disponible.

2.2 Contingencia

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones habituales y reste productividad. El plan se sigue si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos. Debe haber un plan para cada tipo de ataque y tipo de amenaza.

Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre pasar las directivas de seguridad.

Cuando hay la posibilidad de que algún problema se presente en forma imprevista se tendrá la interrupción prolongada de los recursos informáticos y de comunicación de una organización, que no puede remediarse dentro de un periodo predeterminado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Estos pueden ser de dos tipos:

- Eventos naturales: Huracanes, incendios, terremotos, etc.
- Evento desatado por personas: Sabotaje, huelga, accidentes, errores, etc.

Un plan de contingencias como una estrategia planificada con una serie de procedimientos que nos faciliten o nos orienten a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización ante la eventualidad de todo lo que lo pueda paralizar, ya sea de forma parcial o total.

El plan de contingencia es una herramienta que le ayudará a que los procesos críticos de su empresa u organización continúen funcionando a pesar de una

posible falla en los sistemas computarizados. Es decir, un plan que le permite a su negocio u organización, seguir operando aunque sea al mínimo.

Las empresas y/o instituciones deben estar preparadas para manejar una crisis, tanto en el aspecto operacional, como de comunicación. Deben reflexionar sobre las amenazas y su vulnerabilidad. Esto para diseñar y preparar un Plan de Contingencia destinado a superar las crisis que se les presente.

Figura 10 Plan de Contingencias

En la actualidad existen varias empresas que se dedican a la implementación de un plan de contingencia, así como también manuales y libros especializados en este tema.

Generalmente los objetivos de un plan de contingencia son garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y definir acciones y los procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

2.2.1 Aspectos del plan de contingencia

- Plan de Reducción de Riesgos (Plan de Seguridad).
- Plan de Recuperación de Desastres.
- Actividades Previas al Desastre.
- Establecimiento del Plan de Acción.
- Formación de Equipos de Evaluación (auditoria de cumplimiento de procedimientos de Seguridad).
- Actividades durante el Desastre.
- Plan de Emergencias.
- Formación de Equipos.
- Entrenamiento.
- Actividades después del Desastre.

- Evaluación de Daños.
- Prioridad de Actividades.
- Ejecución de Actividades
- Evaluación de Resultados.
- Retroalimentación del Plan de Acción.
- Realizar un análisis de riesgos de sistemas críticos que determine la tolerancia de los sistemas.
- Establecer un periodo crítico de recuperación, en la cual los procesos debe de ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por que se establecerán las prioridades del proceso.
- Asegurar la capacidad de las comunicaciones
- Asegurar la capacidad de los servidores de respaldo.

2.3 Seguridad física antes del desastre

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos. El nivel adecuado de seguridad física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el fallo o, en su caso, aminorar las consecuencias que de el se puedan derivar.

Esta consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial, se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Para que una empresa tenga seguridad física se debe considerar lo siguiente:

- Ubicación del edificio.
- Ubicación del Centro de Procesamiento de Datos dentro del edificio.
- Compartimentación.
- Elementos de la construcción.
- Potencia eléctrica.
- Sistemas contra Incendios.

- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

2.3.1 Tipos de desastres

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se preveen en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

2.3.2 Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

1. Utilización de Guardias
2. Utilización de Detectores de Metales
3. Utilización de Sistemas Biométricos
4. Verificación Automática de Firmas
5. Protección Electrónica

2.4 Seguridad física después del desastre

Se debe implementar una estrategia cuando ha ocurrido un desastre o un ataque. Esto ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, determinar porque tuvo lugar, a reparar el daño que causo y a implementar un plan de contingencia si existe. El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de el.

La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización. Por otra parte, no es común que un negocio responda por sí mismo ante un acontecimiento como este, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que junto con el sitio alterno de proceso de datos,

constituye el plan de contingencia que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

2.4.1 Acciones realizadas durante un desastre

Evaluación del daño. Determinar el daño causado durante el ataque o la contingencia. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que pueda proseguir las operaciones y la productividad normal.

Determinar la causa del daño. Para determinar la causa del daño, es necesario saber a que recursos iba dirigido el ataque y que puntos vulnerables se explotaron para obtener acceso o perturbar los servicios durante el ataque o contingencia.

Reparar el daño. Es muy importante que el daño se repare lo antes posible para restaurar las operaciones normales y los datos perdidos durante la contingencia, los planes y procedimientos para la recuperación de desastres de la organización deben cubrir la estrategia de restauración.

CAPITULO III

ANÁLISIS DE RIESGOS EN LOS SISTEMAS DE INFORMACIÓN

3.1 Análisis de riesgos

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección de la Información en análisis, versus el costo de volverla a producir (reproducir).

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que suceda cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

El análisis de riesgos supone responder a preguntas del tipo:

- ¿Qué puede ir mal?
- ¿Con qué frecuencia puede ocurrir?
- ¿Cuáles serían sus consecuencias?
- ¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?
- En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:
- ¿Qué se intenta proteger?
- ¿Cuál es su valor para uno o para la organización?
- ¿Frente a qué se intenta proteger?
- ¿Cuál es la probabilidad de un ataque?

3.2 Valoración de riesgos

La valoración de riesgo es el primer proceso en la metodología del Análisis de Riesgos. En las organizaciones se usa valoración de riesgos para determinar el grado de la amenaza potencial y asociar el riesgo a un sistema de IT.

El riesgo es una función de la probabilidad de las amenazas-fuentes dadas que ejercitan una vulnerabilidad potencial particular, y el impacto que resulta de ese acontecimiento adverso en la organización.

Para determinar la probabilidad de un futuro acontecimiento adverso, se debe analizar conjuntamente con las vulnerabilidades potenciales y los controles en el lugar para el sistema IT. El impacto refiere a la magnitud de daño que se podría causar por un ejercicio de las amenazas de una vulnerabilidad.

El nivel del impacto es gobernado por los impactos potenciales de la misión y alternadamente produce un valor relativo para los activos y los recursos de IT afectados (e.g., la Criticidad y la sensibilidad de los componentes y de los datos del sistema de IT).

3.3 Metodología de valoración de riesgos

3.3.1 Caracterización del sistema

En la determinación de los riesgos para un sistema de IT, el primer paso es definir el alcance del esfuerzo. En este paso, los límites del sistema de IT son identificados, junto con los recursos y la información que constituye el sistema.

Caracterizando un sistema IT establece el alcance del esfuerzo de valoración de riesgo, delinea los límites operacionales de la autorización (o acreditación), y proporciona la información (e.g., hardware, software, conectividad del sistema, y división responsable o personal de la ayuda) esencial para definir el riesgo. Ver Figura 11

3.3.1.1 Información relacionada al sistema. Identificar el riesgo para un sistema requiere una comprensión afilada del proceso del sistema en el ambiente. La persona o personas que conducen la valoración de riesgo debe por lo tanto recoger primero la información relacionada al sistema, que generalmente se clasifica como sigue:

- Hardware.
- Software.
- Interfaces del Sistema (e.g., conectividad interna y externa).
- Datos e información.
- Personas quienes dan soporte y usan el sistema IT.
- Misión del sistema (e.g., Los procesos realizados por el sistema IT).
- Criticidad del Sistema y los datos (e.g., Valor o importancia del sistema para una organización).
- Sensibilidad del Sistema y los datos

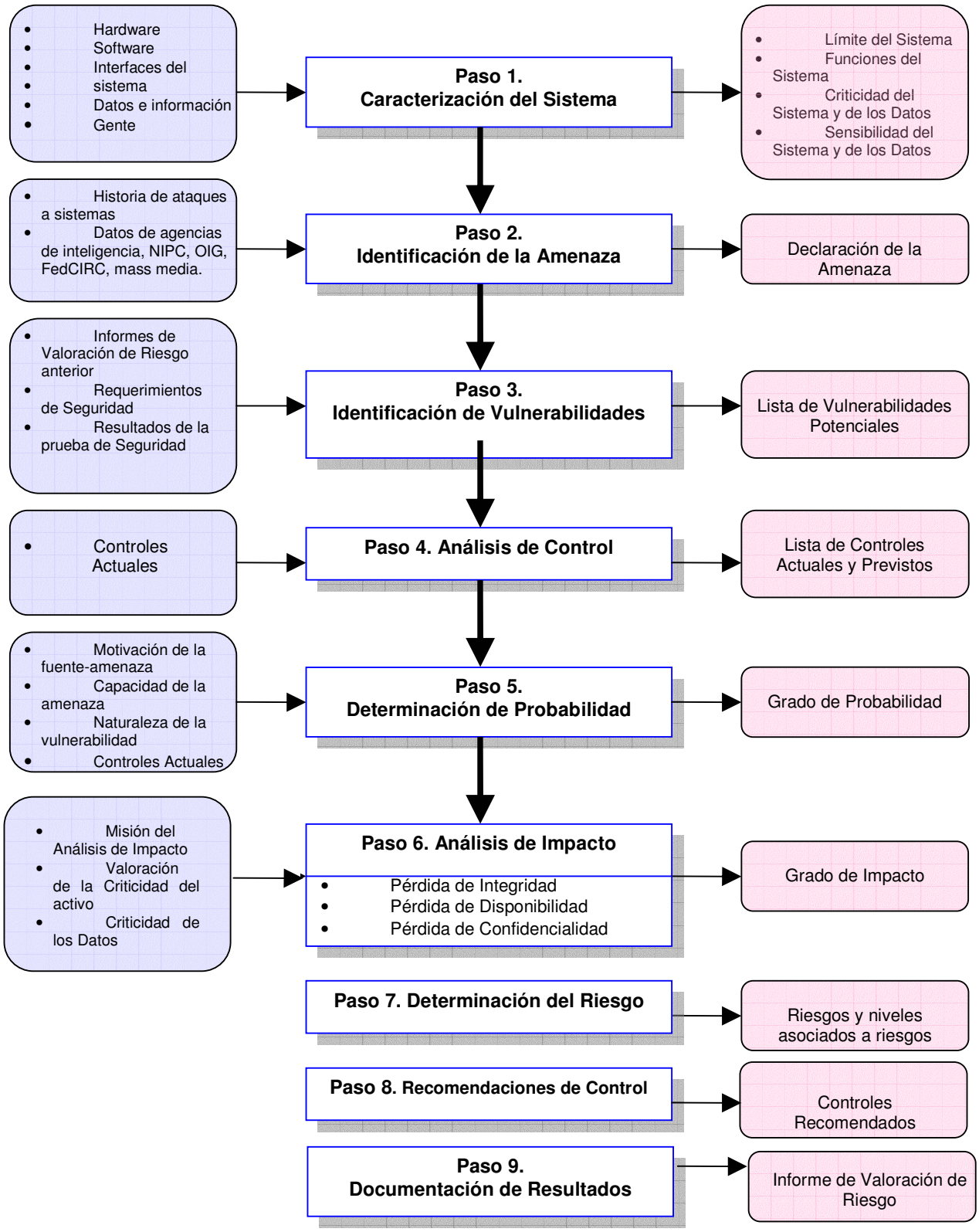


Fig. 11 Metodología de la Valoración de Riesgo

La información adicional relacionada con el ambiental operacional del sistema de IT y de sus datos incluye, pero no se limita al siguiente:

- Los requerimientos funcionales para el sistema.
- Usuarios del sistema (e.g., usurarios del sistema que proporcionan la ayuda técnica, usuarios de aplicaciones que utilizan el sistema para realizar funciones del negocio).
- Políticas de seguridad que gobiernan el sistema (políticas organizacionales, requerimientos federales, leyes, prácticas industriales).
- Arquitectura de Seguridad del sistema
- Topología actual de la red (e.g., diagrama de red).
- Protección de almacenaje de la información que salvaguarda el sistema y disponibilidad de los datos, integridad, y confidencialidad.
- Flujo de información que pertenece al sistema (e.g., interfaces de sistema, entrada del sistema y organigrama de la salida).
- Controles técnicos usados para el sistema (e.g., producto de seguridad incorporada o adicionada que apoya la identificación y de la autentificación, discrecional o control de acceso obligatorio, intervención, protección residual de la información, métodos del cifrado).
- Controles de gerencia usados para el sistema (e.g., reglas de comportamiento, planeamiento de seguridad).
- Controles operacionales usados para el sistema I(e.g., seguridad personal, respaldos, contingencia, y recuperación de la operación; mantenimiento del sistema; almacenamiento fuera de sitio; procedimientos del establecimiento y cancelación de la cuenta del usuario; controles para la segregación de funciones de usuarios, por ejemplo el acceso de usuario privilegiado contra el acceso de usuario estándar).
- Seguridad física en el ambiente del sistema (e.g., seguridad de facilidad, políticas del centro de datos).
- Seguridad ambiental implementada por el sistema procesado en el ambiente (e.g., controles por humedad, agua, energía, contaminación, temperatura, y productos químicos).

Para un sistema que esté en iniciación o fase de diseño, la información del sistema se puede derivar del diseño o del documento de requerimientos. Para un sistema en desarrollo, es necesario que defina las reglas clave de seguridad y las cualidades previstas para el futuro del sistema.

Los documentos del diseño del sistema y el plan de seguridad del sistema pueden proporcionar la información útil sobre la seguridad de un sistema que esté en desarrollo.

3.3.1.2. Técnicas de acopio de Información- Cualquiera, o una combinación, de las técnicas siguientes pueden ser utilizadas en recopilar la información relevante para el sistema dentro de su límite operacional:

- **Cuestionarios.** Para colectar información relevante, el personal de valoración de riesgo puede desarrollar un cuestionario referente a la gerencia y a los controles operacionales previstos o usados para el sistema. Este cuestionario se debe distribuir al personal de gerencia técnico y no técnico aplicable que es el que diseña o da soporte del sistema. El cuestionario también se podría utilizar durante visitas y entrevistas en sitio.

- **Entrevistas en sitio.** Las entrevistas con ayuda de los cuestionarios pueden permitir a personal de valoración de riesgo recoger la información útil sobre el sistema (e.g., cómo el sistema es operado y manejado). Las visitas en sitio también permiten que el personal de valoración de riesgo observe y recopile la información sobre la seguridad física, ambiental, y operacional del sistema. El Apéndice A contiene una muestra de preguntas de la entrevista hechas durante entrevistas con personal del sitio para alcanzar una mejor comprensión de las características operacionales de una organización. Para los sistemas todavía en la fase del diseño, la visita en sitio sería datos cara-a-cara que recolectan ejercicios y podría proporcionar la oportunidad de evaluar el ambiente físico en el cual el sistema IT funcionará.

- **Revisión del documento.** Documentos de políticas (e.g., documentación legislativa, directorios), documentación del sistema (e.g., guía de usuario del sistema, manual administrativo del sistema, diseño del sistema y documento de requisito, documento de la adquisición), y documentación seguridad-relacionada (e.g., el informe de intervención anterior, informe de valoración de riesgo, resultados de prueba del sistema, plan de seguridad del sistema, políticas de la seguridad) pueden proporcionar buena información sobre los controles de seguridad usados y previstos para el sistema. El análisis de impacto de la misión de una organización o la valoración de la Criticidad del activo proporciona la información con respecto a sistema y Criticidad y sensibilidad de los datos.

- **Uso de la herramienta de exploración automatizada.** Los métodos técnicos proactive se pueden utilizar para recoger la información del sistema eficientemente. Por ejemplo, una red tras la herramienta puede identificar los servicios que funcionan en un grupo grande de anfitriones y proporcionan una manera rápida de construir los perfiles individuales del sistema(s) de IT de la meta.

3.3.2 Identificación de la Amenaza

Una amenaza es el potencial para que una amenaza-fuente particular ejercite con éxito una vulnerabilidad particular. Una vulnerabilidad es una debilidad que puede ser accidentalmente accionado o explotado intencionalmente. Una fuente-amenaza no presenta un riesgo cuando no hay vulnerabilidad que no puede ser ejercitada.

En la determinación de la probabilidad de una amenaza, uno debe considerar amenaza fuentes, las vulnerabilidades potenciales y los controles existentes.

Identificación Amenaza-Fuente

La meta de este paso es identificar las amenaza-fuentes potenciales y compilar una declaración de amenaza de un listado de amenaza-fuente potenciales que son aplicables al sistema IT que está siendo evaluado.

Una amenaza-fuente es definida como cualquier circunstancia o evento con el potencial de causar daño a un sistema IT. Las amenaza-fuentes comunes pueden ser naturales, humanas, o ambientales.

En la determinación de amenaza-fuentes, es importante considerar todas las amenaza-fuentes potenciales que podrían causar daño a un sistema IT y a su ambiente de proceso. Por ejemplo, aunque la declaración de la amenaza para un sistema IT situado en un desierto puede no incluir una “inundación natural” debido a la probabilidad baja de tal acontecimiento que ocurre, las amenazas ambientales tales como una pipa que estalla puede inundar rápidamente una sala de computadoras y causar daño a los activos y a los recursos de IT de una organización.

Los seres humanos pueden ser amenaza-fuentes con actos intencionales, tales como ataques deliberados de las personas malévolas o de las contrariedades de los empleados, o actos in intencionales, tales como negligencia y errores. Un ataque deliberado puede ser (1) una tentativa malévola de tener el acceso desautorizado a un sistema IT (e.g., conjeturar vía contraseña) para comprometer integridad del sistema y de datos, disponibilidad, o confidencialidad o (2) un benigno, pero no obstante útil, tentativa de evitar seguridad del sistema.

Un ejemplo del último tipo de ataque deliberado es la escritura de un programador al programa Trojan Horse para puentear seguridad del sistema en orden para "conseguir el trabajo hecho."

Motivación y Acciones de la Amenaza

La motivación y los recursos para realizar un ataque hecho por humanos es una amenaza-fuente potencialmente peligrosa. La Tabla 1 presenta una descripción de muchas amenazas humanas comunes de hoy, de sus motivaciones posibles, y de los métodos o de las acciones de la amenaza por las cuales puede ser que realicen un ataque. Esta información será útil a las

organizaciones que estudian sus ambientes humanos de la amenaza y que modifican sus declaraciones humanas de la amenaza.

Además, revisiones de la historia de robos del sistema; informes de la violación de la seguridad; informes de incidente; y las entrevistas con los administradores de sistema, el personal del escritorio de ayuda, y la comunidad de usuario durante la reunión de información ayudarán a identificar las amenaza-fuentes humanas que tienen el potencial de dañar un sistema de IT y sus datos y que pueden ser una preocupación donde existe una vulnerabilidad.

Amenazas Humanas: Amenaza-Fuente, Motivación, y Acciones de la Amenaza.

Amenaza-Fuente	Motivación		Acciones de la Amenaza
Hacker, cracker	Desafío Ego Rebelión	4 5 6 7	Hacheando Ingeniería Social Intrusión al sistema, robo Acceso al sistema desautorizado
Criminal Computacional	Destrucción de información Acceso ilegal a la información Aumento monetario Alteración desautorizada de datos	8 9 10 11 12	Delito informático (e.g., cyber asecho) Actos fraudulentos (e.g., reinicio, personificación, intercepción) Soborno de información Spoofing Intrusión al sistema
Terrorista	Chantaje Destrucción Explotación Venganza	13 14 15 16 17	Bomba/terrorismo Guerra de información Ataque de sistema (e.g., negación del servicio distribuida) Penetración al sistema Forzar al sistema
Espionaje industrial (compañías, gobiernos extranjeros, otros intereses del gobierno)	Ventaja competitiva Espionaje económico	18 19 20 21 22 23	Explotación económica Hurto de información Intrusión en la privacidad del personal Ingeniería Social Penetración al Sistema Acceso desautorizado al sistema (acceso clasificado, propietario, y/o información tecnológica-relacionada)
iniciados (entrenados mal, contrariedades, malévolos, negligentes, deshonestos o empleados terminados)	Curiosidad Ego Inteligencia Aumento monetario Venganza Errores in intencionales y omisiones (e.g., error de entrada de datos, error de programación)	24 25 26 27 28 29 30 31 32 33 34 35 36 37	Asalto de un empleado Chantaje Hojeo de información propietaria Abuso de la computadora Fraude y hurto Soborno de información Entrada falsificada, corrupción de datos Intercepción Código malicioso (e.g., virus, bomba lógica, caballo de Troya) Venta de información personal Insectos del sistema Intrusión del sistema Sabotaje del sistema Acceso desautorizado al sistema

Tabla 1 Amenazas Humanas: Amenaza-Fuente, Motivación, y Acciones de la Amenaza.

Una estimación de la motivación, recursos, y capacidades que se pueden requerir para realizar un ataque acertado debe desarrollarse después de que se hayan identificado las amenaza-fuentes potenciales, en orden para

determinar la probabilidad de una amenaza que ejercita una vulnerabilidad del sistema.

La declaración de una amenaza, o la lista de amenaza-fuente potenciales, se debe adaptar a la organización individual y a su ambiente de proceso (e.g., hábitos que computa el usuario final). En general, la información sobre las amenazas naturales (e.g., inundaciones, terremotos, tormentas) debe estar fácilmente disponible.

Las amenazas sabidas han sido identificadas por las organizaciones del gobierno y del sector privado. Las herramientas de detección de intrusión también están llegando a ser más frecuentes, y las organizaciones del gobierno y de la industria recogen continuamente datos sobre los acontecimientos de la seguridad, de tal modo mejorando la capacidad de determinar las amenazas realistas.

Una amenaza contenida en una lista de amenaza-fuente que podrían explotar vulnerabilidades del sistema.

3.3.3 Identificación de vulnerabilidades

El análisis de la amenaza para un sistema IT debe incluir un análisis de las vulnerabilidades asociadas al ambiente de sistema. La meta de este paso es para desarrollar una lista de las vulnerabilidades del sistema (defectos o debilidades) que se podrían explotar por las amenaza-fuentes potenciales.

Vulnerabilidad: Un defecto o una debilidad en procedimientos de la seguridad del sistema, diseño, implementación, o los controles internos que se podrían ejercitar (accionado accidentalmente o explotado intencionalmente) y resultado en una abertura de la seguridad o una violación de la política de la seguridad del sistema.

Los métodos recomendados para identificar las vulnerabilidades del sistema son el uso de fuentes de vulnerabilidades, el funcionamiento de la prueba de seguridad del sistema, y el desarrollo de una lista de comprobación de los requisitos de la seguridad.

Debe ser observado que los tipos de vulnerabilidades que existirán, y la metodología necesaria para determinar si las vulnerabilidades estén presentes, (ver tabla 2) variarán generalmente dependiendo de la naturaleza del sistema IT y de la fase en que está, en el SDLC:

- Si el sistema IT todavía no se ha diseñado, la búsqueda para las vulnerabilidades debe centrarse en las políticas de la seguridad de la organización, los procedimientos previstos de la seguridad, las definiciones del requisito del sistema, y los análisis de producto de la seguridad.

- Si el sistema IT se está implementando, la identificación de vulnerabilidades se debe ampliar para incluir una información más

específica, tal como las características previstas de seguridad descritas en la documentación del diseño de la seguridad y los resultados de la prueba y de la evaluación de la certificación del sistema.

- Si el sistema IT es operacional, el proceso de identificar vulnerabilidades debe incluir un análisis de características de seguridad del sistema IT y de los controles de la seguridad, técnico y procesal, usados para proteger el sistema.

Pares de Vulnerabilidades/Amenazas

Vulnerabilidad	Amenaza-Fuente	Acción de la Amenaza
Los identificadores del sistema de empleados terminados (identificación) no se quitan del sistema.	Empleados terminados	Marcar en la red de la compañía y accesar los datos del propietario de la compañía
Los Firewall de la compañía permite de entrada al telnet, y el huésped ID es permitido en XYZ servidor.	Usuarios no autorizados (e.g., hackers, empleados terminados, criminales informáticos, terroristas)	Usando el telnet para XYZ servidor y hojeando los archivos con el huésped ID
El vendedor ha identificado defectos en el diseño de la seguridad del sistema; sin embargo, los remiendos nuevos no se han aplicado al sistema	Usuarios no autorizados (e.g., hackers, empleados disgustados, criminales computacionales, terroristas)	Obteniendo el acceso no autorizado a los ficheros del sistema sensibles basados en vulnerabilidades sabidas del sistema
El centro de datos utiliza las regaderas del agua para suprimir el fuego; los encerados para proteger el hardware y el equipo contra daño del agua no están en lugar	Fuego, personas negligentes	Riegue las regaderas que son giradas en el centro de datos

Tabla 2 Pares de Vulnerabilidades/Amenazas

Fuentes de vulnerabilidades. Las vulnerabilidades técnicas y no técnicas lo asociaron a que el ambiente de proceso del sistema IT se puede identificar vía las técnicas de información-acopio. Una revisión de otras fuentes de la industrial será útil en la preparación para las entrevistas y en desarrollar los cuestionarios eficaces para identificar las vulnerabilidades que pueden ser aplicables a los sistemas IT específicos (e.g., una versión específica de un sistema operativo específico).

El Internet es otra fuente de información sobre las vulnerabilidades sabidas del sistema fijadas por los vendedores, junto con arreglos calientes, paquetes del servicio (service packs), parches, y otras medidas remediadoras que se puedan

aplicar para eliminar o para atenuar vulnerabilidades. Las fuentes documentadas de vulnerabilidades que se deben considerar en un análisis cuidadoso de la vulnerabilidad incluyen, pero no se limitan a, el siguiente:

- Documentación previa de la valoración de riesgo del sistema IT determinado.
- Los informes de intervención de los sistemas IT, informes de anomalía del sistema, informes de revisión de seguridad, y pruebas del sistema e informes de evaluación.
- Equipos de respuesta incidente/emergencia de computación comercial y listas de poste (e.g., correos del foro de SecurityFocus.com)
- Alarmas y boletines de vulnerabilidades del Aseguramiento de la Información para los sistemas militares.
- Análisis de seguridad del software del sistema

Prueba de seguridad al sistema.

Los métodos preactivos, empleo de pruebas del sistema, pueden ser usados para identificar eficientemente las vulnerabilidades en el sistema, dependiendo de la Criticidad del sistema IT y recursos disponibles Los métodos de la prueba incluyen:

- Herramienta de Escaneo Automatizado de vulnerabilidades
- Prueba y Evaluación de Seguridad
- Prueba de penetración.

La herramienta de escaneo automatizado de vulnerabilidades es usada para escasear un grupo de host o una red para saber los servicios. Sin embargo, debe ser notado que algunas de las vulnerabilidades potenciales identificadas por la herramienta de escaneo automatizado pueden no representar vulnerabilidades verdaderas en el contexto del ambiente de sistema.

Por ejemplo, algunas de estas herramientas de escaneo filtran vulnerabilidades potenciales sin la consideración del ambiente y requerimientos del sitio. Algunas de las “vulnerabilidades” señaladas por medio de una bandera por el software de escaneo automatizado pueden realmente no ser vulnerables para un sitio particular pero pueden ser configuradas a tal manera que su ambiente lo requiera. Así, este método de prueba puede producir positivos falsos.

ST&E es otra técnica que puede ser usada para identificar vulnerabilidades del sistema IT durante el proceso de la valoración del riesgo. Esto incluye el desarrollo y ejecución de un plan de prueba (e.g., prueba de escritura, prueba de procedimientos, y resultados de la prueba previstos). El propósito de la

prueba de seguridad del sistema es probar la eficacia de los controles de la seguridad de un sistema IT pues se han aplicado en un ambiente operacional.

El objetivo es asegurarse que los controles aplicados resuelvan la especificación aprobada de seguridad para el software y hardware e implementar la política de seguridad de la organización o resolver estándares industriales.

La prueba penetrada puede ser usada para complementar la revisión de controles de seguridad y asegurarse que las diferentes facetas del sistema IT estén seguras. La prueba de penetración, cuando está empleada en el proceso de valoración de riesgo, puede ser utilizada para determinar la capacidad de un sistema IT de soportar tentativas intencionales para evitar seguridad del sistema. Este objetivo es para probar el sistema IT del punto de vista de una amenaza-fuente y para identificar fallas potenciales en los esquemas de protección del sistema IT.

Los resultados de este tipo de pruebas opcionales de seguridad ayudarán a identificar vulnerabilidades de un sistema.

Desarrollo de la lista de comprobación de requisitos de seguridad.

Durante este paso, el personal de valoración de riesgo se determina si los requisitos de la seguridad estipulados para el sistema IT y recogidos durante la caracterización del sistema están siendo resueltos por controles de seguridad existentes o previstos.

Típicamente, los requisitos de seguridad del sistema se pueden presentar en forma de tabla, con cada requisito acompañado por una explicación de cómo el diseño o la implementación del sistema hace o no satisface ese requisito del control de seguridad.

Una lista de comprobación de requisitos de seguridad contiene los estándares básicos de seguridad que se pueden utilizar para evaluar y para identificar sistemáticamente las vulnerabilidades de los activos (personal, hardware, software, información), procedimientos no automatizados, procesos, y las transmisiones informativas asociadas a un sistema IT dado en las áreas siguientes de seguridad:

- Gerencia
- Operacional
- Técnica

La tabla 3. Enlista los criterios de seguridad sugeridos para el uso en identificar las vulnerabilidades de un sistema IT en cada área de la seguridad.

Criterios de Seguridad

Área de Seguridad	Criterio de Seguridad
Seguridad Gerencial	• Asignación de responsabilidades • Continuidad de ayuda • Capacidad de respuesta del incidente • Revisión periódica de Controles de seguridad • investigaciones de la separación del personal y del fondo • Valoración de riesgo • Seguridad y entrenamiento técnico • Separación de deberes • Autorización del sistema y reautorización • Sistema o aplicación del plan de seguridad
Seguridad Operacional	• Control de contaminantes aerotransportados (humo, polvo, productos químicos) • Controles para asegurar la calidad de la fuente de corriente eléctrica • Acceso y disposición de medios de datos • Distribución y etiquetado de datos externos • Facilidad de protección (e.g., sala de ordenadores, centro de datos, oficina) • Control de humedad • Control de temperatura • Estación de trabajo, laptops, y ordenadores personales independientes
Seguridad Técnica	• Comunicaciones (e.g., dial-in, interconexión el sistema, routers) • Criptografía • Control de acceso discrecional • Identificación y autentificación • Detección de intrusión • Reuso de objeto • Auditoria de sistema

Tabla 3 Criterios de Seguridad

El resultado de este proceso es la lista de comprobación de los requisitos de seguridad. Las fuentes que pueden ser utilizadas en la compilación de tal lista de comprobación incluyen, pero no se limitan al gobierno regulador y directorios y las fuentes de seguridad aplicables al sistema IT que procesa el ambiente:

- CSA de 1987.
- Publicaciones Federales de Información Procesada de Estándares.

- OMB Noviembre 2000 Circular A-130.
- Acto de Privacidad de 1974.
- Sistema de Plan de seguridad del sistema IT trazado.
- Las políticas de seguridad de la organización, pautas, y estándares.
- Prácticas industriales.

El NIST SP 800-26, Guía Identidad-Valoración de Seguridad para Sistemas de Tecnología de Información, provee un cuestionario extensivo que contiene los objetivos de control específicos contra los que un sistema o grupo de sistemas interconectados pueden ser evaluados y medidos. Los objetivos de control son resumidos directamente de requisitos de mucho tiempo encontrados en la ley parlamentaria, política, y la orientación sobre seguridad y privacidad.

Los resultados de la lista de verificación (o cuestionario) pueden ser usados como la entrada para una evaluación del acatamiento y el incumplimiento. Este proceso identifica el sistema, proceso, y defectos de procedimiento que representan las vulnerabilidades potenciales.

3.3.4 Análisis de control

El objetivo de este paso es para analizar los controles que han sido implementados, o son planeados para la implementación, por la organización para minimizar o eliminar la probabilidad (o probabilidad) de ejercitar amenazas a una vulnerabilidad del sistema.

Para obtener una clasificación de probabilidad en general que indica la probabilidad de que una vulnerabilidad potencial puede ser ejercida dentro de la construcción del entorno de amenaza asociado (Paso 5 Abajo), la implementación de controles actuales o planeados deben ser considerados.

Por ejemplo, una vulnerabilidad (e.g., sistema o defecto de procedimiento) probablemente no es para ser ejercido o la probabilidad es baja cuando es un nivel bajo de interés o capacidad de amenaza-fuente o si hay controles de seguridad eficaces que pueden eliminarse, o reducir la magnitud de daño.

Métodos de Control. Los controles de seguridad abarcan el uso de los métodos técnicos y no técnicos. Los controles técnicos son garantías que son incorporadas en hardware, software, o microprograma (e.g., mecanismos de control de acceso, identificación y mecanismos de autentificación, métodos de encriptación, software de detección de intrusión). Los controles no técnicos son controles de dirección y operacionales, como las políticas de seguridad; procedimientos operacionales; y personal, físico, y seguridad ambiental.

Categorías de Control. Las categorías de control para los métodos tanto técnicos como no técnicos pueden ser clasificadas más a fondo como

preventivo o detectivo. Estas dos subcategorías son explicadas de la siguiente manera:

- Los controles preventivos impiden los intentos de infringir la política de seguridad e incluyen tales controles como la ejecución de control de acceso, encriptación, y autentificación.

- Los controles detectivos advierten de las infracciones o intento de infracciones de la política de seguridad e incluyen tales controles como rastros de intervención, métodos de detección de intrusión, y sumas de comprobación.

La implementación de tales controles en curso o planeados durante el proceso de mitigación del riesgo es el resultado directo de la identificación de deficiencias de controles en curso o planeados durante el proceso de valoración de riesgo (e.g., los controles no están en lugar o los controles no se ponen en ejecución correctamente).

Técnicas de Análisis de Control. El desarrollo de una lista de comprobación de los requisitos de seguridad o el uso de una lista disponible será provechoso analizar controles de una manera eficiente y sistemática.
La lista de comprobación de los requisitos de seguridad se puede utilizar para validar no conformidad de la seguridad así como conformidad. Por lo tanto, es esencial poner al día tales listas de comprobación para reflejar cambios en el ambiente del control de una organización (e.g., cambios en políticas, métodos, y requisitos de la seguridad) para asegurar la validez de la lista de comprobación.

3.3.5 Determinación de probabilidad

Para derivar un grado total de la probabilidad que indique la probabilidad que una vulnerabilidad potencial se puede ejercitar dentro de la construcción del ambiente asociado de la amenaza, los siguientes factores que gobiernan deben ser considerados:

- Motivación y capacidad de Amenaza-Fuente.

- Naturaleza de la vulnerabilidad.

- Existencia y eficacia de controles actuales.

La probabilidad que una vulnerabilidad potencial se podría ejercitar por una amenaza-fuente dada se puede describir como alta, media, o baja. La Tabla 4 describe estos tres niveles de probabilidad.

Definiciones de Probabilidad

Nivel de Probabilidad	Definición de Probabilidad
Alto (High)	La amenaza-fuente es altamente motivada y suficientemente capaz, y los controles para evitar que la vulnerabilidad sea ejercitada son ineficaces.
Medio (Médium)	La amenaza-fuente es motivada y capaz, pero los controles están en el lugar que puede impedir el ejercicio acertado de la vulnerabilidad.
Bajo (Low)	La amenaza-fuente carece de motivación o capacidad, o los controles están en el lugar para prevenir, o impedir significativamente por lo menos, la vulnerabilidad de ser ejercitada.

Tabla 4 Definiciones de Probabilidad

3.3. 6 Análisis de impacto

El siguiente paso principal en medir el nivel del riesgo es determinar el impacto adverso resultando de un ejercicio acertado de la amenaza de una vulnerabilidad. Antes de comenzar el análisis del impacto, es necesario obtener la información necesaria:

- Misión del sistema (e.g., el proceso desarrollado por el sistema IT).
- Criticidad del sistema y datos (e.g., valor o importancia del sistema para una organización).
- Sensitividad del sistema y datos.

Esta información se puede obtener de la documentación de organización existente, tal como el informe de análisis del impacto de la misión o de valoración de la Criticidad del activo. Un análisis del impacto de la misión (también conocido como análisis del impacto del negocio da la prioridad a los niveles del impacto asociados al compromiso de los activos de la información de una organización basados en una valoración cualitativa o cuantitativa de la sensibilidad y criticidad de esos activos.

Una valoración de Criticidad del activo identifica y da prioridad a los activos de información sensible y crítica de la organización (e.g., hardware, software, sistemas, servicios, y activos relacionados de tecnología) esos ayudan a las misiones críticas de la organización.

Si no existe esta documentación o tales valoraciones para los activos de IT de la organización no se han realizado, la sensibilidad del sistema y datos se puede determinar basado en el nivel de protección requerido para mantener la disponibilidad del sistema y datos, integridad, y confidencialidad.

Sin importar el método usado para determinar cómo es sensible un sistema IT y sus datos, el sistema y los dueños de la información son los responsables de determinar el nivel del impacto para su propio sistema e información. Por lo

tanto, en analizar el impacto, el acercamiento apropiado consiste en entrevistarse con el dueño del sistema de la información.

Por lo tanto, el impacto adverso de un acontecimiento de seguridad se puede describir en términos de la pérdida o de la degradación de cualesquiera, o una combinación de cualesquiera, de las tres metas siguientes de la seguridad: integridad, disponibilidad, y confidencialidad. La lista siguiente proporciona una breve descripción de cada meta de seguridad y la consecuencia (o impacto) que no es satisfecho:

Pérdida de Integridad. La integridad del sistema y datos se refiere al requisito de que la información se proteja contra la modificación incorrecta. Se pierde la integridad si los cambios desautorizados son realizados a datos del sistema IT por actos intencionales o accidentales. Si la pérdida de integridad del sistema o datos no se corrige, el uso continuado del sistema contaminado o los datos corrompidos podría dar lugar a inexactitud, fraude, o decisiones erróneas. También, la violación de integridad puede ser el primer paso en un ataque acertado contra disponibilidad o confidencialidad de sistema. Por todas estas razones, la pérdida de integridad reduce el aseguramiento de un sistema IT.

Pérdida de Disponibilidad. Si una misión-crítica del sistema IT es inasequible a sus usuarios finales, la misión de la organización puede ser afectada. La pérdida de funcionalidad del sistema y de eficacia operacional, por ejemplo, puede dar lugar a pérdida de tiempo productivo, así impidiendo el funcionamiento de los usuarios finales de sus funciones en el soporte de la misión de la organización.

Pérdida de Confidencialidad. La confidencialidad del sistema y datos se refiere a la protección de información del acceso no autorizado. El impacto del acceso no autorizado de información confidencial puede extenderse del compromiso de seguridad nacional al acceso de datos del Acto de Privacidad.

El acceso desautorizado, inesperado, o no intencional podía dar lugar a pérdida de confianza pública, vergüenza, o acción legal contra la organización.

Algunos impactos tangibles pueden ser medidos cuantitativamente en rédito perdido, el costo de reparación del sistema, o el nivel del esfuerzo requerido para corregir los problemas causados por una acción acertada de la amenaza. Otros impactos (e.g., pérdida de confianza pública, pérdida de credibilidad, daños a los intereses de la organización) no pueden ser medidos en unidades específicas sino puede ser calificado o descrito en términos de impactos altos, medios, y bajos. Debido a la naturaleza genérica de esta discusión, esta guía señala y describe solamente las categorías cualitativas – impacto alto medio, y bajo (ver Tabla 5).

Definiciones de Magnitud de Impacto

Magnitud de Impacto	Definición de Impacto
Alto (High)	El ejercicio de la vulnerabilidad (1) puede dar lugar a la pérdida altamente costosa de activos tangibles o de recursos importantes; (2) puede violar, dañar, o impedir perceptiblemente la misión de una organización, la reputación, o el interés; o (3) puede dar lugar a muerte humana o a lesión seria.
Medio (Médium)	El ejercicio de la vulnerabilidad (1) puede dar lugar a la pérdida costosa de activos tangibles o de recursos; (2) puede violar, dañar, o impedir la misión de una organización, la reputación, o el interés; o (3) puede dar lugar a lesión humana.
Bajo (Low)	El ejercicio de la vulnerabilidad (1) puede dar lugar a pérdida de algunos activos tangibles o de recursos o (2) pueden perceptiblemente afectar la misión, reputación, o interés de una organización.

Tabla 3.5 Definiciones de Magnitud de Impacto

Cualitativo o Valoración Cualitativo

En conducir el análisis del impacto, la consideración se debe dar a las ventajas y a las desventajas de cuantitativo contra valoraciones cualitativos. La ventaja principal del análisis cualitativo del impacto es que da la prioridad a los riesgos e identifica las áreas para la mejora inmediata en la dirección de las vulnerabilidades. La desventaja del análisis cualitativo es que no proporciona las medidas cuantificables específicas de la magnitud de los impactos, por lo tanto está haciendo un análisis de costes y beneficios de cualquier control recomendado de dificultad.

La ventaja principal de un análisis cuantitativo del impacto es que proporciona una medida de la magnitud de los impactos, que se puede utilizar en el análisis de costes y beneficios de controles recomendados. La desventaja es que, dependiendo de las gamas numéricas usadas para expresar la medida, el significado del análisis cuantitativo del impacto puede ser confuso, requiriendo ser interpretado el resultado de una manera cualitativa. Los factores adicionales se deben considerar a menudo para determinar la magnitud de impacto. Éstos pueden incluirse, pero no son limitados a:

- Una valoración de la frecuencia del ejercicio de la amenaza-fuente del excedente de la vulnerabilidad al período especificado (e.g., 1 año).

- Un coste aproximado por cada ocurrencia del ejercicio de la amenaza-fuente de la vulnerabilidad.

- Un factor cargado basado en un análisis subjetivo del impacto relativo del ejercicio de una amenaza específica de una vulnerabilidad específica.

3.3.7 Determinación de riesgo

El propósito de este paso es trazar el nivel de riesgo de activos del sistema IT. La determinación de riesgo para un par amenaza/vulnerabilidad puede ser expresado como una función de:

- La probabilidad de una amenaza-fuente dada que procura ejercitar una vulnerabilidad dada.

- La magnitud del impacto si una amenaza-fuente ejercita con éxito la vulnerabilidad.

- La suficiencia de los controles planeados o existentes de seguridad para reducir o eliminar riesgo.

Para medir el riesgo, una escala de riesgo y una matriz de riesgo-nivel debe ser desarrollado.

Matriz Riesgo-Nivel

La determinación final del riesgo de misión es obtenida multiplicando las clasificaciones asignadas para la probabilidad de amenaza (e.g., probabilidad) e impacto de amenaza. La tabla 6 da demostraciones de cómo los grados de riesgo totales pudieron ser determinados basado en entradas de probabilidad de la amenaza y de categorías del impacto de la amenaza. La matriz abajo es una matriz 3 x 3 de la probabilidad de la amenaza (alto, medio, y bajo) y del impacto de la amenaza (alto, medio, y bajo). Dependiendo de los requerimientos del sitio y la gradualidad de valoración de riesgo deseada, algunos sitios pueden utilizar una matriz de 4 x 4 o 5 x 5. La última incluye una muy Baja/Alta probabilidad de amenaza y un muy Bajo/Alto impacto de amenaza para generar un muy Bajo/Alto nivel de riesgo. Un "muy Alto" nivel de riesgo puede requerir un posible paro del sistema o paro de toda la integración del sistema IT y prueba de esfuerzos.

Matriz Nivel-Riesgo

Probabilidad de amenaza	**Impacto**		
	Bajo (Low) (10)	**Medio (Medium)** (50)	**Alto (High)** (100)
Alto (1.0)	**Bajo** 10 X 1.0 = 10	**Medio** 50 X 1.0 = 50	**Alto** 100 X 1.0 = 100
Medio (0.5)	**Bajo** 10 X 0.5 = 5	**Medio** 50 X 0.5 = 25	**Medio** 100 X 0.5 = 50
Bajo (0.1)	**Bajo** 10 X 0.1 = 1	**Bajo** 50 X 0.1 = 5	**Bajo** 100 X 0.1 = 10

Escala de Riesgo: Alto (>50 a 100); Medio (>10 a 50); Bajo (1 a 10)

Tabla.6 Matriz Nivel-Riesgo

La matriz da la demostración de cómo los niveles de riesgo Alto, Medio, y Bajo son derivados. La determinación de estos niveles o grados del riesgo puede ser subjetiva. El análisis razonado para esta justificación se puede explicar en los términos de la probabilidad asignada para cada nivel de la probabilidad de amenaza y un valor asignado para cada nivel del impacto. Por ejemplo,

- La probabilidad asignada para cada probabilidad de nivel de amenaza es 1.0 para Alto, 0.5 para Medio, 0.1 para Bajo.

- El valor asignado para cada nivel de impacto es 100 para Alto, 50 para Medio, y 10 para Bajo.

Descripción de Nivel de Riesgo

La tabla 7 describe los niveles del riesgo demostrados en la matriz antedicha. Esta escala del riesgo, con sus grados de alto, de medio, y de bajo, representa el grado o el nivel del riesgo a el cual un sistema IT, facilidad, o procedimiento pudieron ser expuestos si una vulnerabilidad dada fue ejercitada. La escala del riesgo también presenta las acciones que la gerencia mayor, los dueños de la misión, debe tomar para cada nivel del riesgo.

Escala de Riesgo y Acciones necesarias

Nivel de Riesgo	Descripción de riesgo y acciones necesarias
Alto (High)	Si una observación o la búsqueda se evalúa como alto riesgo, hay una necesidad fuerte de medidas correctivas. Un sistema existente puede continuar funcionando, pero un plan de acción correctiva se debe poner en lugar cuanto antes.
Medio (Médium)	Si una observación se clasifica como riesgo medio, las acciones correctivas son necesarias y un plan se debe desarrollar para incorporar estas acciones dentro de un período del tiempo razonable.
Bajo (Low)	Si una observación se describe como riesgo bajo, el DAA del sistema debe determinarse si las acciones correctivas todavía están requeridas o decidir a aceptar el riesgo.

Tabla 7 Escala de Riesgo y Acciones necesarias

3.3.8 Recomendaciones de control

Durante este paso del proceso, los controles que podrían atenuar o eliminan los riesgos identificados, como apropiado a las operaciones de la organización, se proporcionan. La meta de los controles recomendados es reducir el nivel de riesgo al sistema IT y a sus datos a un nivel aceptable. Los factores siguientes se deben considerar en controles de recomendación y soluciones alternativas para reducir al mínimo o para eliminar riesgos identificados:

- Eficacia de opciones recomendadas (e.g., compatibilidad del sistema).

- Legislación y regulación.
- Políticas organizacional.
- Impacto operacional.
- Seguridad y confiabilidad.

Las recomendaciones de control son los resultados del proceso de valoración de riesgo y proporcionan la entrada al proceso de mitigación del riesgo, durante cuál los controles de seguridad procesal y técnica recomendada se evalúan, dan prioridad, y se implementan.

Debe ser observado que no todos los controles recomendados posibles se pueden implementar para reducir pérdida. Para determinar que se requiere y que es apropiado para una organización específica, un análisis de costos y beneficios, debe ser conducido por los controles recomendados propuestos, para demostrar que los costes implementados se pueden justificar por la reducción en el nivel del riesgo. En adición, el impacto operacional (e.g., efecto sobre funcionamiento del sistema) y viabilidad (e.g., requerimientos técnicos, aceptación de usuario) de introducir las opción recomendada se debe evaluar cuidadosamente durante el proceso de mitigación del riesgo.

3.3.9 DOCUMENTACIÓN DE RESULTADOS

Una vez que se haya terminado la valoración de riesgo (las amenaza-fuentes y las vulnerabilidades identificadas, los riesgos determinados, y los controles recomendados proporcionados), los resultados se deben documentar en un informe oficial o un sesión informativa.

Un informe de valoración del riesgo es un informe que ayuda a la gerencia mayor, los dueños de la misión, toma de decisiones en la política, procesal, presupuesto, y sistema operacional y cambios de la gerencia. Diferente de un informe de intervención o investigación, que busca fechoría, un informe de valoración de riesgo no se debe presentar de una manera acusatoria sino como un acercamiento sistemático y analítico a determinar riesgo de modo que la gerencia mayor entienda los riesgos y asigne recursos a reducir y pérdidas potenciales correctas.

Por esta razón, alguna gente prefiere tratar los pares de amenaza/vulnerabilidad como observaciones en vez de resultados en valoración de riesgo. El Apéndice B proporciona una idea general sugerida para el informe de valoración de riesgo.

Reporte de Valoración de Riesgo que describe las amenazas y vulnerabilidades, medidas de riesgo, y provee las recomendaciones de la implementación de control.

CAPITULO IV

PLAN DE RECUPERACIÓN DE DESASTRES (DRP)

4.1 Antecedentes de los DRP

En la actualidad existen varias empresas que han realizado inversiones importantes en la **TI**, es por ello que estas empresas necesitan de una DRP que cumplan con sus exigencias y poder así tener alta disponibilidad hacia sus clientes.

Existen empresas que se dedican a la planeación de estrategias de recuperación, entre ellas podemos mencionar a **IBM de México**, el cual en sus servicios identifica las vulnerabilidades del negocio, evaluando el impacto de una interrupción de información, desarrollando una estrategia para administrar los riesgos e implementando un programa de continuidad de negocios integrado.

IBM de México ofrece una estrategia de continuidad utilizable, de bajo costo, que prepare a la empresa para tratar interrupciones imprevistas de la mejor manera.

Identifica las vulnerabilidades del negocio, evaluando el impacto de una interrupción de información, desarrollando una estrategia para administrar los riesgos e implementando un programa de continuidad de negocios integrado.

IBM se a caracterizado a lo largo de los años por ser una compañía que ha ido avanzando en conjunto con la tecnología, es por eso que al entrar al ambiente de los DRP´s nos da una muestra de satisfacción, contempla los puntos importantes que debe de contener un DRP, que son los siguientes:

- **Identificar la Vulnerabilidad.** Dentro de una empresa se realizara un estudio el cual nos indicara donde estarán las posibles fallas que puedan poner en riesgo todo el sistema informático.

- **Evaluar el impacto de una interrupción**. Cuando haya sucedido un desastre y nuestro sistema informático sea dañado nos permitirá saber que información no esta disponible y así agilizar el levantamiento de nuestro sistema para que esté de nuevo disponible a nuestros usuarios.

- **Desarrollar una estrategia.** En este punto se tomaran en cuenta todas las reglas y normatividades que llevara nuestro método científico para hacerle frente a un desastre.

- **Implementar un programa de continuidad.** En el momento que llegue a suceder el desastre nosotros deberemos contar con un plan de emergencia en el cual tengamos un sistema informático B que

llegue a reemplazar al titular con al menos los requerimientos mínimos que solicite la empresa.

- **Bajo costo.** En este punto, las empresas creen que al tener un servicio como este llegue a ser demasiado costoso y que muy pocas veces llegue a ser utilizado y optan por hacerlo en forma de back up.

DRP Consultores. En **DRP Consultores** apoyan a sus clientes a recuperar y reanudar la operación normal de su Empresa en situaciones de contingencia, en el menor tiempo y costos factibles, mediante el análisis, desarrollo, implantación y mantenimiento de Planes de Recuperación de Desastres (DRP, Disaster Recovery Plan) y/o Planes de Continuidad del Negocios (BCP, Business Continuity Plan).

Sus talleres de trabajo están diseñados para aquellas empresas que realizarán su desarrollo con personal interno pero que necesitan apoyo de consultores expertos.

Generalmente los talleres se manejan como sesiones de trabajo en los que se les explica la metodología y los consultores internos de la empresa la desarrollan con supervisión de resultados por parte de DRP Consultores.

Profit. Otra empresa es Profit el cual ofrece servicios, consiste en la realización de consultoría especializada en la creación de medidas que permitan la continuación de la operación del negocio en caso de desastre.

Integridata. Es una empresa que desde 1998 está especializada únicamente en el Resguardo de Medios. Actualmente resguardan aproximadamente 1,200 TB de información, de empresas líderes en el ramo automotriz, bancario, construcción, manufactura, seguros y servicios financieros

Como aliados de SunGard proporcionan servicios complementarios al DRP. InteGridata menciona los siguientes puntos importantes de porque es importante de por que es tener una Bóveda externa:

- La Seguridad Física para la información es un concepto binario, es decir, los Medios están seguros (SAFE) o los Medios NO están seguros (UNSAFE).

- Es importante que los Medios sean almacenados por personal especializado y dedicado al almacenamiento y resguardo.

- La bóveda debe ser un espacio que cumpla con las normas internacionales, asegurando la Confidencialidad, Integridad y Seguridad de los Medios.

- Sin una política de Respaldo de Información se deja sin efecto la inversión realizada para el Plan de Recuperación en caso de Desastre, dado que sin Respaldo de Información: NO HAY RECUPERACIÓN.

4.2 Análisis de fallas en la seguridad

Esto supone estudiar las computadoras, su software, localización y utilización con el objeto de identificar los resquicios en la seguridad que pudieran suponer un peligro.

Por ejemplo, si se instala una computadora personal nueva, para recibir informes de inventario desde otras PC´s vía MODEM situados en lugares remotos, y debido a que el MODEM se ha de configurar para que pueda recibir datos, se ha abierto una vía de acceso al sistema informático. Habrá que tomar medidas de seguridad para protegerlo, como puede ser la validación de la clave de acceso.

4.3 Actividades previas al desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.

Podemos detallar las siguientes Actividades Generales:

- Establecimiento del Plan de Acción.
- Formación de Equipos Operativos.
- Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad).
- Establecimiento de Plan de Acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

a) Sistemas e Información.

b) Equipos de Cómputo.

c) Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

d) Políticas (Normas y Procedimientos de Backups).

4.3.1 Sistemas e Información. La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombré del Sistema.

- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).

- La Dirección (Gerencia, Departamento, etc.) que genera la información base (él «dueño» del Sistema).

- Las unidades o departamentos (internos/externos) que usan la información del Sistema.

- El volumen de los archivos que trabaja el Sistema.

- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.

- El equipamiento necesario para un manejo óptimo del Sistema.

- El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema).

- Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).

- Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

4.3.2 Equipos de Cómputo. Hay que tener en cuenta:

- Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

- Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

- Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC's con

Información importante o estratégica y color verde a las PC's de contenidos normales.

- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

4.3.3 Obtención y almacenamiento de los Respaldos de Información (BACKUPS).

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

1) Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

2) Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

3) Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

4) Backups de los Datos (Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

5) Backups del Hardware. Se puede implementar bajo dos modalidades:

- **Modalidad Externa.** Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

- **Modalidad Interna.** Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

4.4 Plan de recuperación de desastres

4.4.1 Términos y definiciones para un DRP

Copia de seguridad: Una copia de seguridad es una copia de archivos almacenados originalmente en el disco duro. Las copias de seguridad permiten volver a crear archivos perdidos o dañados, o restaurar sistemas que no funcionan.

Almacenamiento: Un archivo es un sistema de almacenamiento a largo plazo organizado y accesible.

Imagen del sistema: Una imagen del sistema es una instantánea de todo el sistema. Las imágenes del sistema incluyen el sistema operativo, la configuración del sistema y todos los archivos de datos. En el software también recibe el nombre de Copia de seguridad de todo el sistema.

Recuperación de desastres: La recuperación de desastres es el proceso de restauración del sistema tras un "desastre". Un desastre es cualquier situación en la que hay que volver a crear un sistema después de un fallo en el disco duro. Si sólo hay que recuperar un grupo de archivos o carpetas, no se puede hablar de recuperación de desastres.

Rotación de discos: Una rotación de discos significa utilizar varios discos para realizar una copia de seguridad de los datos y del sistema. Permite guardar el historial de todo el sistema o de los datos en varios discos y brinda la opción de almacenar discos en un lugar externo, lo que aumenta la seguridad de los datos.

Revisiones de archivos: Las revisiones de archivos son versiones diferentes de un archivo o una carpeta. Ésta es la cantidad de historial que se mantiene de los datos en un solo disco. Cuantas más revisiones de archivos se conserven, más protección se tiene contra problemas del sistema que son graduales y que tardan un tiempo en detectarse. Guardar un periodo largo de revisiones de archivos proporciona la flexibilidad necesaria para ver cómo eran las cosas en el pasado.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento

El proceso de recuperación en caso de contingencia consiste en la identificación, planeación, definición y prueba de procedimientos y planes requeridos para restaurar los servicios regulares de IT, en la eventualidad de sufrir una falla o caída de los servicios. Las acciones deberán incluir el regreso de las operaciones normales.

El principal objetivo del proceso es anticiparse a la contingencia para minimizar el impacto en la ESIME Culhuacán.

Las metas del proceso son:

- Proporcionar capacidad de recuperación que permita satisfacer la necesidad de la escuela.
- Asegurar la integridad de la información vital para la ESIME Culhuacán y su disponibilidad diaria en caso de una contingencia.
- Estar preparados para recuperar los sistemas en caso de falla.

El proceso involucra, entre otras cosas, el desarrollo de una serie de subprocesos y procedimientos predefinidos tales como la identificación de recursos de la IT, programas e información aplicativa requeridos para reanudar los servicios en su totalidad.

4.5 Documentación de la recuperación

El proceso de recuperación en caso de contingencia requiere que se mantenga disponible la información del mismo y un alto nivel de capacitación de la organización participante, en las distintas actividades del proceso.

Para lo cual se recomienda:

- Documentar y formalizar la interacción entre los grupos involucrados en el plan de recuperación. Cada grupo debe

entender su participación y como se relaciona esta con la recuperación global del ambiente de IT.

- Capacitar y mantener entrenado el personal de recuperación mediante la realización de ejercicios de recuperación no anunciados, en los cuales el personal clave no se encuentre disponible ni sea localizable, de la misma manera en lo que sucedería en caso de una contingencia real.

- Motivar al personal a utilizar la documentación y las listas de verificación para comunicar el estatus de la ejecución del plan a otro personal interesado.

- Documentar y mantener autorizados los elementos mínimos requeridos para recuperar la operación de la Escuela en caso de contingencia, mediante los cuales se puede mencionar:

- Inventarios y configuración del Hardware y Software de comunicaciones.

- Inventarios de proveedores y sus contactos.

- Procedimientos de operación de todas las plataformas de operación.

- Procedimientos de respaldo y restauración de todas las plataformas.

- Niveles de servicios para contingencia.

- Procedimiento de acceso y uso del área, incluyendo listas del personal autorizado para declarar oficialmente una contingencia.

- Directorio de contactos en caso de una contingencia.

- Información de puntos de reunión (centro de comando) para contingencia.

4.6 Obtención y almacenamiento de los respaldos (back ups)

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto «c», debiéndose incluir:

- Periodicidad de cada Tipo de Backup.

- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales).

- Uso obligatorio de un formulario estándar para el registro y control de los Backups.

- Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa (mencionado en el punto «a»), y los backups efectuados.

- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.

- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).

- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida sí el desastre alcanzo todo el edificio o local estudiado).

- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

CAPITULO V

PROPUESTA DEL DISEÑO DEL DRP PARA EL CENTRO ESCOLAR DE ESIME CULHUACÁN

5.1 ESTADO ACTUAL DE LA RED DE CONTROL ESCOLAR DE ESIME CULHUACAN

Dentro de la ESIME Unidad Culhuacán se llevo a cabo una serie de exámenes, los cuales se aplicaron al área de **Control Escolar,** ya que es la que maneja información valiosa para la comunidad estudiantil, con lo que se detecto que el personal no esta capacitado para hacerle frente a un desastre y tampoco cuenta con el equipo necesario para resolver una contingencia.

Se realizó un estudio en base a la información obtenida de las siguientes fuentes:

- Listas de verificación.
- Entrevistas realizadas al personal gerencial y profesional del área de Control Escolar de la ESIME Unidad Culhuacán.
- Visitas al área de Control Escolar de la ESIME Unidad Culhuacán.

5.1.1 Lista de Verificación (Checklist)

La lista de verificación que se aplicó se puede observar en el anexo A. Es la forma de realizar un inventario, el cual nos arrojo el siguiente resultado:

- *Numero de personal en el área:* Aproximadamente 6 personas por turno.
- *Grado académico:* La mayoría son secretarios (as).
- *Numero de equipos:* Aproximadamente 6 equipos.

Estos equipos son:

Hardware [1]

- Pentium uno (64 Ram, 80 GB disco duro, 16 MB en video, lectora de CD-Rom, lectora de Disquete).
- 5 impresoras láser monocromo de la marca HP los cuales dan servicios a toda el área de control escolar.
- Cuentan con un Nobreak para todos los equipos de la marca **ISB Sola Basic** modelo **Mini Sei** el cual da soporte de energía on-line [2]

[1] Es el substrato físico en el cual existe el software. El hardware abarca todas las piezas físicas de un ordenador (CPU, placa base, etc).

[2] La energía en la salida nunca se interrumpe, ideal para proteger equipos delicados y muy sensibles a las perturbaciones de la línea.

Software [3]

- El sistema operativo que tienen es Windows 98 y una que usa Windows Millenium.
- Cuenta con paquetería de oficina (Microsoft Office)
- El antivirus que manejan es el **ViRobot Sauri** el cual va más allá de detectar y limpiar los virus informáticos; determinar su procedencia, recuperar archivos y erradicar el problema.

La Unidad ESIME Culhuacán cuenta con una infraestructura de varios equipos de cómputo para el área de Control Escolar, la cual por razones de seguridad no se nos permitió observar, pero se nos indico de manera gráfica como se encontraba estructurada y distribuida. Ver anexo B, figura 1.

La red en la Unidad ESIME Culhuacán esta estructurada de manera que el área de Control Escolar, dentro del Edificio de ICE, cuenta con un Hub y una red tipo estrella, al que llegan todas las terminales de este departamento como son: estaciones de trabajo, impresoras, el servidor.

A través de un enlace de fibra óptica se conecta el Hub a un Switch (A) ubicado en el edifico de IC (Ingeniería en Computación), este se enlaza por medio de fibra óptica a un Switch (B), ubicado en el edificio IM (Ingeniería Mecánica), por ultimo se conecta a un Router que se encuentra en el mismo edificio.

El Router se conecta a un Modem (Transciver) para enviarlo a través de microondas terrestres, esta antena se encuentra en el techo del edificio, se realiza una transferencia de datos a UPIICSA, esta recibe los datos y los retransmite a Zacatenco, en donde se almacenan toda la base de datos que se tiene en ESIME Culhuacán.

El área de control escolar cuenta con un equipo de seguridad básico. Esta compuesto por dos extinguidores, una salida de emergencia, letreros de evacuación, letreros en caso de sismo o incendio, su área de trabajo esta ubicado en un lugar estratégico ya que cuentan con espacio para poder circular ampliamente.

Es importante decir, que los respaldos que se realizan en ESIME Culhuacán son periódicos y de forma manual, oscilando de 3 a 15 días para realizarlos por personal de Zacatenco; las instalaciones en donde se encuentran ubicados los equipos, tiene muchas vulnerabilidades entre las que se pueden mencionar:

- Las instalaciones solo cuentan con un velador.
- Las ventanas no están protegidas.
- No hay un sistema de alarma.

[3] Se refiere a los programas y datos almacenados en un ordenador

- Tienen demasiados privilegios los equipos de trabajo.
- No se cuenta con respaldo de la información.
- El servidor no se encuentra en un lugar adecuado.
- El personal de prevención no esta capacitado adecuadamente.

5.2 Análisis de posibles riesgos del área de control escolar.

A continuación se muestran los posibles riesgos que la escuela puede tener en base a la información que se menciono en el tema Estado Actual de la Red de Control Escolar:

Riesgos Humanos

- Acto Hostil como pueden ser:
- Agresión física o moral
- Robo
- Incendios.

Riesgos Naturales:

- Inundaciones
- Sismos
- Tormentas eléctricas

Riesgos Tecnológicos:

- Incendios
- Acceso al centro de cómputo

5.2.1 Tabla de probabilidad y vulnerabilidad en las instalaciones.

Después de identificar los posibles riesgos a los que se enfrenta la escuela, se elaboro una tabla de probabilidad y vulnerabilidad que se puede observar en el Anexo C, tabla 1. La cual cuenta con una lista de posibles amenazas las cuales se les registro la probabilidad y vulnerabilidad clasificándolas como: No Aplicable (NA), Bajo (B), Medio (M) y Alto (A). Así como los ya detectados.

Posteriormente se analizaron las probabilidades y vulnerabilidades de cada riesgo identificado y se presentó a la escuela un informe acerca del impacto

que pudieran tener en la operación, y de esta manera la misma decidiera que hacer con ellos (reducir, eliminar, transferir o aceptar).

Las decisiones tomadas fueron las siguientes:

Sismos. La ESIME Unidad Culhuacán, debe reducir el riesgo de un siniestro, capacitando a su personal, y a su vez implementar un sistema de alarma que ayude a agilizar la evacuación del edificio.

Incendios. Reducir el riesgo de este siniestro, ya que no cuenta con un sistema de alarma contra incendios, señalamientos en las rutas de evacuación, sistemas de irrigación, detectores de humo, mantenimiento de extintores y personal capacitado.

Agresión física o moral. Se debe reducir el riesgo debido a que la ubicación de la Escuela no se encuentra en una zona favorable para el resguardo de la integridad física y moral de sus empleados, así como la disponibilidad de números de emergencia a los cuales se pueda acudir en caso de la agresión.

Robo. Se debe reducir el riesgo, tomando en cuenta que no se tiene suficiente personal de vigilancia, alarmas, sistemas de circuito cerrado y el entorno social de inseguridad actual en el país no favorece al desarrollo de las operaciones diarias que se llevan a cabo.

5.2.2 Recomendaciones sobre el análisis de riesgo

A continuación se hará un análisis de cada uno de los riesgos identificados:

Sismos:

- Ubicar su sitio de trabajo a distancia de archivos, libreros, mobiliario y objetos que pudieran caerse.
- No apilar en exceso papelería, ni mobiliario que pueda causar fallas en las losas o pisos de su área
- Mantener los pasillos y áreas de circulación limpios y libres de obstáculos.
- Conocer en donde está ubicado el encargado de área.
- Identificar en su piso en donde están las rutas de evacuación, las salidas normales y de emergencias, así como escaleras de servicios y de emergencia.
- Estar capacitado para responder a este tipo de siniestros.

Incendios:

- Contar con extintores en buenas condiciones y en lugares estratégicos

- Contar con salidas de emergencias.
- Contar con número telefónicos donde se pueda reportar cualquier emergencia.
- Evitar sobrecargar las líneas eléctricas, llevando un control de cargas de las instalaciones.
- Desconectar los aparatos y equipos electrónicos al término de su jornada.
- No utilizar para la limpieza productos inflamables como gasolina.
- Reportar cualquier olor a quemado, gas, gasolina o productos aromáticos inflamables.
- No arrojar cerillos ni cigarros encendidos a los cestos de basura.
- No fumar en áreas restringidas.
- Identificar las posibles fuentes de incendio de su centro de trabajo.
- Familiarizarse con la ubicación y el uso de los extinguidores de su área de trabajo.
- Reportar las obstrucciones a los accesos de extinguidores y de gabinetes de concentración al encargado de piso.

Tormenta eléctrica:

Las tormentas eléctricas pueden producir lluvias intensas (que a su vez pueden provocar inundaciones repentinas), vientos fuertes, granizadas, rayos y tornados.

Los rayos constituyen una importante amenaza durante una tormenta eléctrica. Por este motivo es recomendable que todos los equipos que se encuentren en uso sean correctamente aterrizados a un sistema de tierras, para evitar cualquier daño en los mismos.

Acto Hostil

AGRESIÓN FÍSICA Y MORAL:
Conocer en donde está ubicado el encargado de área.
Tener capacitación sobre, cómo, actuar en esta situación.
Contar con el suficiente personal de vigilancia apto para responder ante este suceso.
Tener al alcance números telefónicos de emergencias.

ROBO:
Tener capacitación sobre, cómo, actuar en caso de este tipo de atentado.
Tener al alcance números telefónicos de emergencias

Situar alarmas en lugares estratégicos y que solo el personal conozca su ubicación.
Contar con el suficiente personal de vigilancia apto para responder ante este suceso.

5.3 PROPUESTA PARA LA APLICACIÓN DE UN PLAN DE RECUPERACIÓN DE DESASTRES (DRP)

Cada negocio y organización pueden experimentar un incidente serio, que puede impedir la continuación de las operaciones.

Es importante que los encargados de cada área demuestren una visión clara para mantener un proceso eficaz del planteamiento de recuperación en caso de un desastre.

Es vital que la ESIME Unidad Culhuacán tome el desarrollo y el mantenimiento del plan de recuperación de desastre seriamente. No es una tarea que puede ser tomada a la ligera hasta que alguien se ocupe en realizar el DRP. Un incidente serio puede por supuesto ocurrir en cualquier momento.

Toda el personal debe ser informado acerca del Plan de Recuperación de Desastre que se requiere para asegurarse de que las funciones esenciales de la organización puedan continuar en el acontecimiento de alguna contingencia.

Para la realización de nuestra propuesta llevaremos acabo la siguiente metodología:

- Conocer la infraestructura actual del centro de cómputo: Instalaciones, hardware, software y comunicaciones.
- Establecer rutinas aleatorias de comprobación de integridad de los respaldos.
- Documentar los elementos claves para la operación de los sistemas y mantener copia de éstos en bóveda externa.
- Evaluar la capacidad de recuperación de la Escuela Superior De Ingeniería Mecánica y Eléctrica Unidad Culhuacán, revisando sus procesos de recuperación, respaldo/ restauración y administración de sistemas
- Identificar las fortalezas y áreas de riesgo existentes
- Dar pautas para eliminar o minimizar riesgos y establecer alineamientos para implantar una disciplina de recuperación de operación de operaciones
- Determinar la necesidad de establecer y formalizar procesos y procedimientos funcionales que permitan fortalecer la infraestructura de sistemas de la Escuela Superior De Ingeniería Mecánica y Eléctrica

Unidad Culhuacán en caso de continencia y obtener una recuperación efectiva de su ambiente de tecnología de información.

Se propone el diseño de una DRP (Plan de Recuperación contra Desastres), debido a que la información que se esta manejando en la institución día con día es de vital importancia para el alumnado, egresados, docentes y el mismo Instituto Politécnico Nacional. Entre la información que se maneja cada ciclo escolar se puede mencionar calificaciones, boletas, tramites de documentos, etc. Los cuales si se llegaran a perder, pondrían a la escuela en una crisis que tendría un alto costo en recursos.

5.3.1 Ubicación del equipo.

La ubicación de la red alterna (DRP), se encontrará en el edificio de laboratorios en el primer piso. El cual cuenta con un cuarto de energía, sistema de seguridad, almacén, monitores del circuito cerrado, ubicación de los equipos (host, servidor e impresora), un panel de parcheo, switches, Rack`s y área telefónica. Ver Anexo D, figura 1.

Remodelaciones en el á*rea del Site*. (Ver Anexo D, figura 2)

- Se hará la introducción del sistema de aire acondicionado, para evitar el calentamiento de los equipos, como pueden ser servidores, routers, switches, firewalls, etc., que se encuentren el cuarto y con esto optimizar el desempeño de los equipos.
- Se colocara en toda el área piso falso, esto con la finalidad de que el cuarto tenga una buena ventilación, se pueda meter parte del cableado de manera organizada debajo del piso, entre otras.
- Se pondrá un cableado por la parte superior del cuarto, por medio de estructuras metálicas o en algunos casos utilizando tubos de PVC, por las cuales pase el cable que así lo requiera.
- Se instalará un sistema contra incendios en todo el cuarto.
- Se colocara un sistema de circuito cerrado de cámaras, para la vigilancia del lugar.
- Se colocará en la entrada principal del Cuarto de Comunicaciones, un sistema de seguridad, el cual identificará al personal autorizado para entrar al mismo, por medio de las huellas digitales.
- Se acondicionara un cuarto para monitoreo del cuarto (circuito cerrado) el cual se encontrara debidamente protegido, para evitar cualquier acceso de personas ajenas al mismo. Este cuarto se llamara “Monitores del Circuito Cerrado”.
- Habrá un área en la cual se encontrará todo el equipo que alimenta la red y evitara cualquier descarga eléctrica, así como alguna falla en el suministro de energía eléctrica. Estos equipos pueden ser una planta de emergencia, un regulador contra descargas, una batería de pilas UPS, etc. Esta área se llamara “Cuarto de Energía”.

5.3.2 Enlace y topología.

La conexión de la red del edificio ICE (Control Escolar), se realizara con fibra óptica en ambos extremos por medio de Switches que manejan velocidades de 100BaseTX y 1000BaseSX bajo el estándar IEEE 802.3, al Server del Site del

DRP, el cual recibirá y procesara toda la información a copiar. La información a copiar de Control Escolar será de 5 computadoras de las cuales, cada una con todo y sistema operativo no superan los 3Gb por maquina, por lo tanto la información a copiar será de 15Gb como máximo al día. Ver Anexo E.

El diseño de la red se formará con una topología estrella bajo el estándar IEEE 802.3 *(FastEthernet y GigaEthernet)*, por medio de un switch (A) que conecta a un servidor, 5 computadoras y una impresora. Haciendo uso de cable UTP-C5, además estará conectado por fibra óptica al switch (P) y este último se conectará al switch (S) bajo el estándar 1000BaseSX. El switch (S) se conectará al Router bajo el estándar 100BaseSX y, de ese punto la señal pasará por un modem para salir por la Microonda que se encuentra en el techo del edificio de IM y, de esta manera la señal dará dos saltos de microonda pasando por la microonda de UPIICSA para después llegar a la de Zacatenco en donde se respaldará la información de Control Escolar.

Sin embargo, es importante decir que el enlace de microonda puede fallar y, es por ello que en el diseño se propone contratar un servicio de enlace E1 dedicado, con un ISP, que llegará de forma directa hasta Zacatenco.

El Site del DRP se interconectara a los switches (A y S) con el switch R por medio de fibra óptica bajo el estándar 1000BaseSX.

Ahora bien, el Site del DRP que se esta proponiendo, siempre estará en funcionamiento, recibiendo la información con que se este trabajando en el área de Control Escolar (edificio ICE) de manera que si en algún momento llegara a haber una contingencia en esa parte de la red, el Site del DRP (edificio de Laboratorios) entraría en funcionamiento en una forma activa dejando la forma pasiva como comúnmente se encuentra trabajando.

5.3.3 Descripción del equipo propuesto.

Cableado

Cable UTP-C5 (Unshielded Twisted Pair). Este tipo de cable se propuso para el cableado a los equipos como son: terminales, impresoras y otros, bajo la tecnología Fast Ethernet (bajo el estándar IEEE 802.3), debido a las características que posee. Ver anexo E, tabla 1

Fibra Óptica multimodo

La fibra óptica se propuso para el backbone, el cual es el circuito interno de la red, por el cual viajan todos los datos. Todos los switches se interconectan por medio de este material que nos brinda una red más ágil en la transferencia de información. La tecnología que se esta usando es la Gigabit Ethernet (bajo el estándar IEEE 802.3). Ver Anexo E, tabla 2

La NIC (Tarjetas de Red)
PLACA RED C-NET 10/100 PCI PRO-200, Ver anexo E, figura 1

Características:

- Chip sencillo PCI 100BaseTX Fast Ethernet
- Estándares Soportados IEEE 802.3u u IEEE 802.3
- Modo Full-duplex hasta 200 Mbps.
- Función de auto Negociación
- Conector UTP RJ-45 soporta 100BaseTX y 10Base-T
- Es Plug and Play, se configura automáticamente

Equipo de Interconexión

Switch Fast Ethernet 24 puertos 2 puertos Gb. Ver Anexo E, figura 2

Características

- (24) Puertos 100/10Mbps
- Cada Puerto crea un segmento independiente en la red
- 2 puertos Gigabit Ethernet, 10/100/1000 Mbps
- Con soluciones Ethernet, FastEthernet y Gigabit Ethernet
- Plug & Play

Host

5 computadoras con las siguientes características , Ver anexo E, figura 3

- Motherboard Intel : ABIT-SD7-533(Chipset SIS, Sonido, DDR333, Bus 400)
- Procesador: 2.4Ghz Bus 533 1Mb Cache.
- Memoria RAM: 128Mb 266Mhz
- Disco duro: 40Gb 7200 R.P.M. SEGATE
- Unidad lectora: Floppy 31/2
- Unidad CD-DVD: 16X LG
- Mouse y Teclado Plug and play
- Monitor LCD: 15” LG (para menor consumo de energía)
- Bocinas AOPEN

Impresora

Laserjet 1020 a 600 puntos por pulgada, Anexo E, figura 4

PC como Servidor (Ver Anexo E, figura 5

- Motherboard Intel : P4S800D-X (Chip SIS, AGP 8x, DDR 400 Dual Chanel, Sonido y Red, SATA, Bus 800)
- Procesador: 3.2Ghz Bus 800 1Mb Cache.
- Memoria RAM: 512Mb 400Mhz
- Disco duro interno: 300Gb Serial ATA 7200 R.P.M. SEGATE
- Disco duro externo: 300Gb USB 2.0 MAXTOR
- Unidad lectora: Floppy 31/2
- Unidad CD-DVD: 16X LG
- Mouse y Teclado Plug and play
- Monitor LCD: 15” LG (para menor consumo de energía)

Software de los Host

- Microsoft Windows XP Sp2
- Norton antivirus Symantec 2005
- Programas y aplicaciones Para control escolar

SOFTWARE (Servidor)

Para la realización de el sistema de recuperación ante desastres es necesario llevar acabo la selección del software a utilizar, entre los mas destacados y fiables en el mercado utilizaremos el que nos proporciona la compañía Iomega Corp. La versión a utilizar es Automatic Backup (ver Figura 6.0) compatible con las versiones de Windows Server; la instalación se realiza en el servidor de la red, alterna a control escolar.

Tras instalar Iomega® Automatic Backup Pro, Puede utilizarse para hacer una copia total del sistema (sistema operativo, aplicaciones, configuración y datos), así como solamente archivos y datos. En este caso usaremos la copia total del sistema (llamada también imagen para recuperación de desastres), se selecciona la ruta origen. Ver Figura 6.1

Por medio de este software se realiza copias de seguridad del sistema operativo, de todas las aplicaciones, de la configuración del sistema y de todos los archivos de datos que se encuentran en la red de control escolar hacia la red alterna. Este tipo de copia de seguridad en disco duro contiene todo lo necesario para restaurar el sistema en caso de fallo.

Las copias de seguridad se realizan en forma total a la red de control escolar en un principio, luego solo se actualizaran en forma automática solo aquellos archivos que sean nuevos o modificados. Figura 6.2

Se realizara un numero de dos copias, para ello se realiza la primer copia de sistema en el disco duro interno del servidor, luego así una copia externa en un dispositivo de disco duro externo. Se etiquetaran con un nombre: Seguridad Interna y Seguridad Externa.

El disco duro externo se guardara sin compresión ya que los datos no superan los 3Gb por cada computadora de control escolar. De manera predeterminada, el software crea una imagen para la recuperación de desastres nueva cada vez que se ejecuta una copia de seguridad de todo el sistema.

Se realizaran 20 copias del sistema en forma de historial, una independiente de la otra, de tal forma que podamos seleccionar un punto de restauración de las 20 disponibles; se realizara de esta forma ya que la copia total del sistema incluye cualquier archivo que estuviese en la red de control escolar, para el caso de que existiese una amenaza de infección por Virus se pueden descartar del historial copias de seguridad que estuviesen infectados.

Esto nos proporciona mayor seguridad en la integración de los datos a disponer. Entonces se selecciona el destino de la copia haciendo uso de ventanas de Windows en el podemos ubicar el destino utilizando una ubicación de red. Ver figura 6.3

El software realiza copias de seguridad de todo el sistema a intervalos regulares de horas o días; si como realiza copias de seguridad de todo el sistema a una hora marcada, ciertos días de la semana.

Entonces se realizaran copias de seguridad interna a una hora marcada de los día hábiles en los que labora control escolar, para ello es recomendable hacer la copia justo al termino de labores por día, para que no afecte el rendimiento de la red de control escolar y no se genere trafico en este, además se realiza una copia del disco duro interno en uno externo cada 2 días, etiquetándolo como seguridad externa. Ver Figura 6.4

A la imagen de copia de seguridad realizada estarán cifradas y protegidas mediante contraseña, disponibles solo para el Administrador de la red tanto ESIME Culhuacán como Zacatenco. Ver Figura 6.5

Para restaurar una copia de seguridad de todo el sistema, debe iniciar el Asistente de restauración del sistema de Iomega Automatic Backup Pro. Puede arrancar Iomega Automatic Backup Por mediante el CD de inicio del sistema el cual puede crearse para la restauración del los host de la red.

Determinación de una estrategia de copias de seguridad

A la hora de planificar una estrategia de copias de seguridad, se deben tener en cuenta las siguientes recomendaciones y problemas:

- Se determina cuántos datos puede permitirse perder. Como el costo nos es crítico se realiza una copia de seguridad de los datos al día.
- Utilizar discos duros, ya que transfieren la información más rápidamente que las cintas. No hay que buscar a través de diferentes cintas o esperar para avanzar a la mitad de la cinta para encontrar un archivo.
- Utilizar por lo menos un disco de seguridad en forma de rotación. Para generar un historial más completo.
- Guardar una copia de seguridad del sistema completo fuera de las instalaciones (disco extraíble). Esto protegerá al sistema en caso de un desastre en las instalaciones.
- Hacer una copia de seguridad de todo el sistema antes de actualizar el hardware o el software. Así se protegerá de posibles problemas del sistema introducidos al actualizarlo.
- Guardar varias revisiones de archivos. Así aumentará el historial de datos guardando varias versiones de archivos en un único disco de copia de seguridad.
- Guardar y manipular los discos de copias de seguridad de manera adecuada para garantizar una larga duración del disco. Evitar la exposición de los discos a la luz solar directa, las temperaturas

extremas, la humedad o los campos magnéticos (como los procedentes de monitores o altavoces).

- Almacenar el disco de inicio o cualquier otro medio de inicio en un lugar seguro, con el fin de asegurarse que se podrá acceder a ellos si se produce un desastre del sistema alterno.

Ventajas: Varias copias de largo plazo (cada mes) de todo el sistema se almacenan en el interior y exterior.

Desventajas: Guardar grandes cantidades de historial (revisiones de archivos e imágenes del sistema) ocupa más espacio en el disco.

Distribución de personal encargado de Administrar la Red

Es necesario que el sistema a implementar cuente con personal capacitado para su mantenimiento y puesta en funcionamiento; para ello se requiere del siguiente personal:

Administrador de la red. Será el mismo administrador de red de control escolar quien configure el sistema y, este a su vez se encargará de ambas redes.

Técnico. Nos ayudará con respecto a fallos y necesidades para mantener la red en buen estado, como energía eléctrica, cambiar el cable dañado, instalar ó manipular equipos eléctricos y electrónicos.

Encargado del personal de Control Escolar. Nos ayudara a distribuir correctamente al personal de acuerdo a sus funciones de oficina cuando suceda una contingencia.

CONCLUSIONES

Evaluar y controlar permanentemente la seguridad física del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros.
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

Si se crea la atmósfera organizacional adecuada para propiciar una buena comunicación se podrá elaborar con mucha mayor facilidad y agilidad un plan de contingencia, el cual será de gran utilidad para responder mejor ante situaciones no previstas y fortalecer los puntos débiles de la institución, cualquiera que esta sea, adicionalmente las mejoras que posteriormente se le harán al plan se llevarán a cabo con mayor participación y consenso de la gente involucrada, teniendo como resultado una mejor respuesta ante las eventualidades y menor resistencia a la prueba del plan cuando se requiera.

Por tal motivo, el objetivo primordial de este plan de recuperación de desastres es preservar la integridad física del personal, las instalaciones y la seguridad del equipo de cómputo, así como recuperar las operaciones de la institución en el menor tiempo.

Esto se puede lograr, por medio de un lugar alterno instalado dentro de la misma escuela, en el cual se encuentre un equipo similar con las características recomendadas al de control escolar y se realicen copias de seguridad con el software Iomega para enfrentar cualquier contingencia y obtener el resultado deseado.

ANEXO A

Nombre de la escuela

1. Talento Humano asignado a la Función de Sistemas de Información.

1.1 Cantidad de personas en el área de Sistemas: _____

1.2 Perfil del personal de sistemas.

Perfil	Cantidad
Tecnólogos en Sistemas	
Ingenieros de Sistemas	
Especialistas en Telecomunicaciones.	
Otros (Indique)	

2. Plataformas de Hardware y Software utilizadas.

Plataforma	Descripción
Sistemas Operacionales	
Motores de Bases de Datos	
Otras Herramientas de Desarrollo	
Software de Red.	
Equipos Activos de la Red	
Internet	
Intranet	
Extranet	
Firewalls	
Servidores de Archivo	
Mainframes	
Minicomputares	
Microcomputadores	
Otras (indique)	

3. Las actividades de procesamiento de datos que se realizan en la empresa.

o	***Descripción***	**Marque con X**
1	Grabación (captura de Datos)	( )
2	Control de Entradas y Salidas.	( )
3	Producción de información (Procesamiento y actualización de archivos).	( )
4	Help Desk.	( )
5	Soporte a usuarios de microcomputadores y LANs.	( )
6	Mantenimiento de hardware.	( )
7	Administración de bases de datos (DBA)	( )
8	Administración de la Seguridad lógica (controles de acceso)	( )

9	Planeación estratégica de sistemas.	( )
10	Administración de contratos de terceras partes.	( )
11	Definición e implementación de políticas de seguridad corporativas.	( )
12	Análisis y Diseño de Sistemas.	( )
13	Construcción de Programas (Elaboración de programas de computador).	( )
14	***Mantenimiento de Software Aplicativo***	( )
15	Administración de Telecomunicaciones.	( )
16	Otras.	( )

4. Servicios de procesamiento de datos que son contratados con terceros.

o	***Descripción***	**Marque con X**
1	Mantenimiento de hardware.	2 ( )
2	Administración de los Centros de Procesamiento de Datos	2 ( )
3	Grabación de Datos	2 ( )
4	Planeación estratégica de sistemas.	2 ( )
5	Planeación de Contingencias en Sistemas de Información.	2 ( )
6	Análisis y Diseño de Sistemas.	2 ( )
7	Programación de aplicaciones.	2 ( )
8	***Mantenimiento de Software Aplicativo***	2 ( )
19	Seguridad en Sistemas de Información.	
10	Otras (indíquelas).0	2 ( )

Nombre del funcionario encuestado:_____

Cargo: _____

Tel: _____

Fecha: _____.

ANEXO B

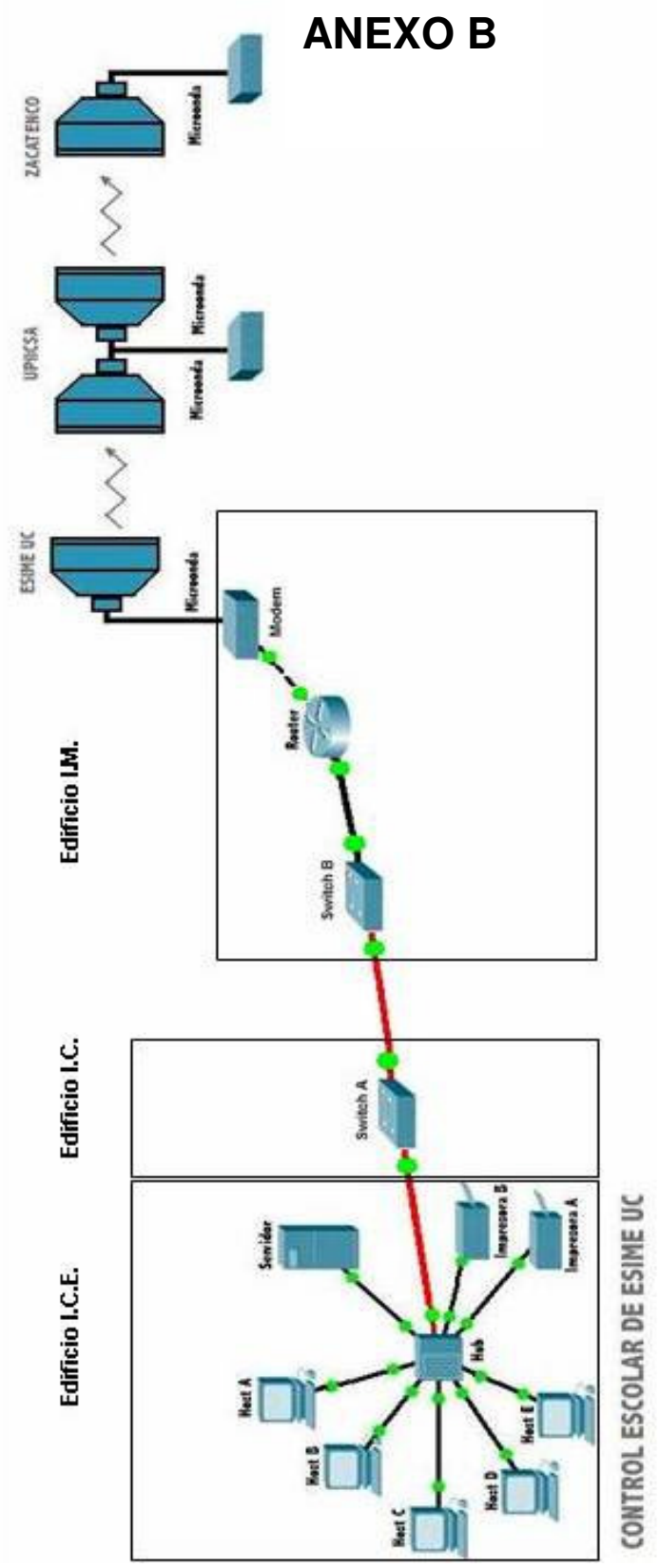


Figura 1 Estado Actual de la red de control escolar

ANEXO C

Posibles Amenazas	Probabilidad				Vulnerabilidad				Riesgos detectados
	NA	B	M	A	NA	B	M	A	
Inundaciones	✔				✔				
Sismos				✔				✔	✔
Tormenta Eléctrica			✔				✔		✔
Incendios			✔					✔	✔
Artefactos explosivos		✔				✔			
Agresión física o moral			✔				✔		✔
Robo				✔				✔	✔
Acceso a las instalaciones				✔				✔	✔
Sabotaje computacional				✔			✔		✔

NA: No Aplica; **B:** Bajo; **M:** Medio; **A:** Alto

Tabla 1 Probabilidad y vulnerabilidad en las instalaciones

ANEXO D

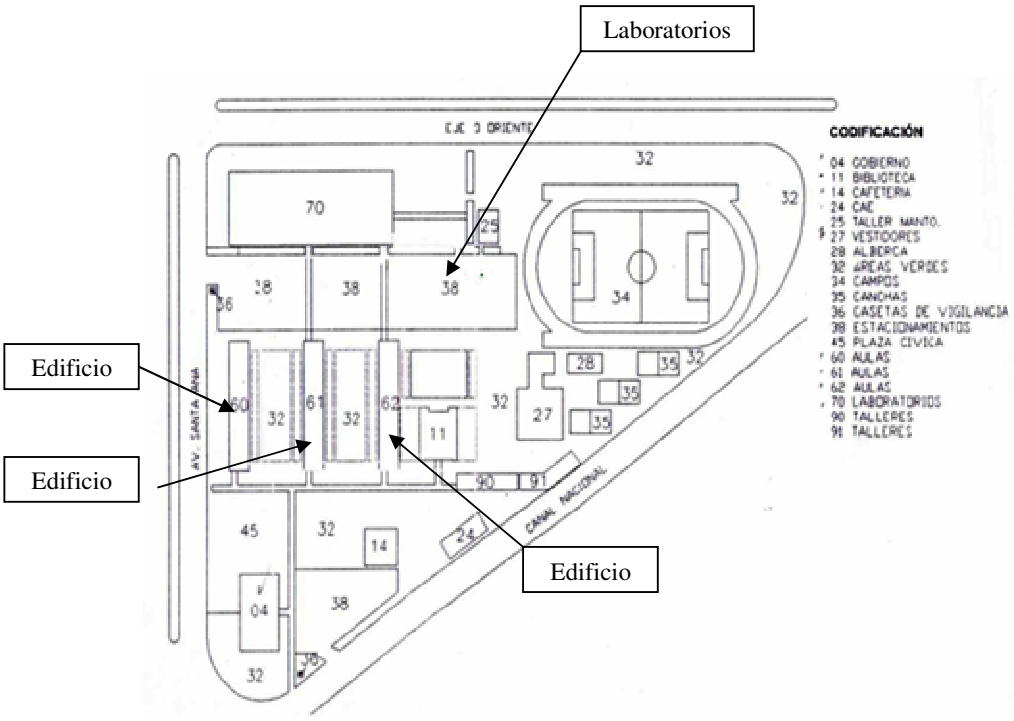


Figura 1 Ubicación del site

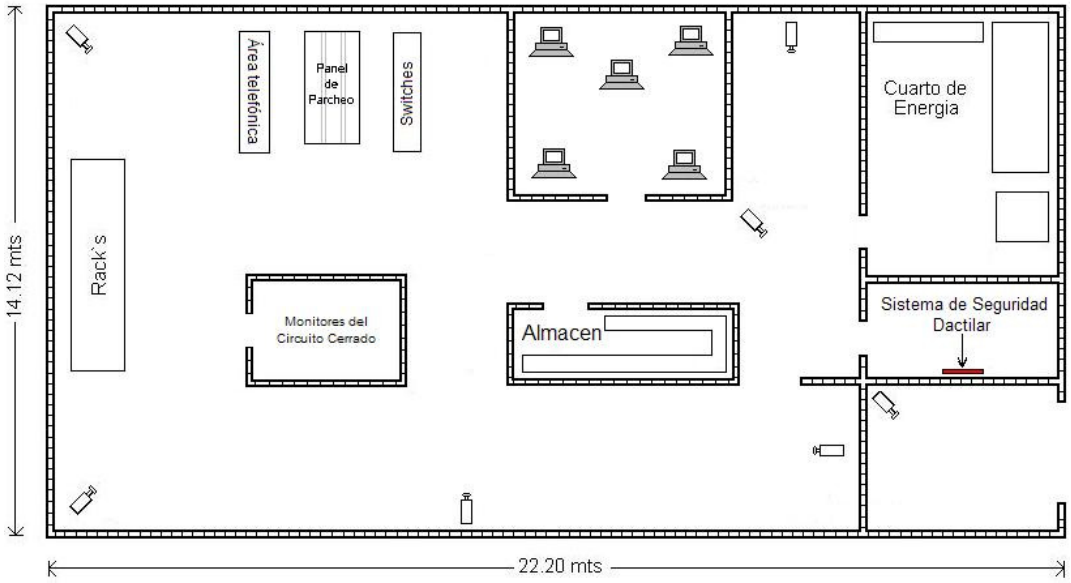
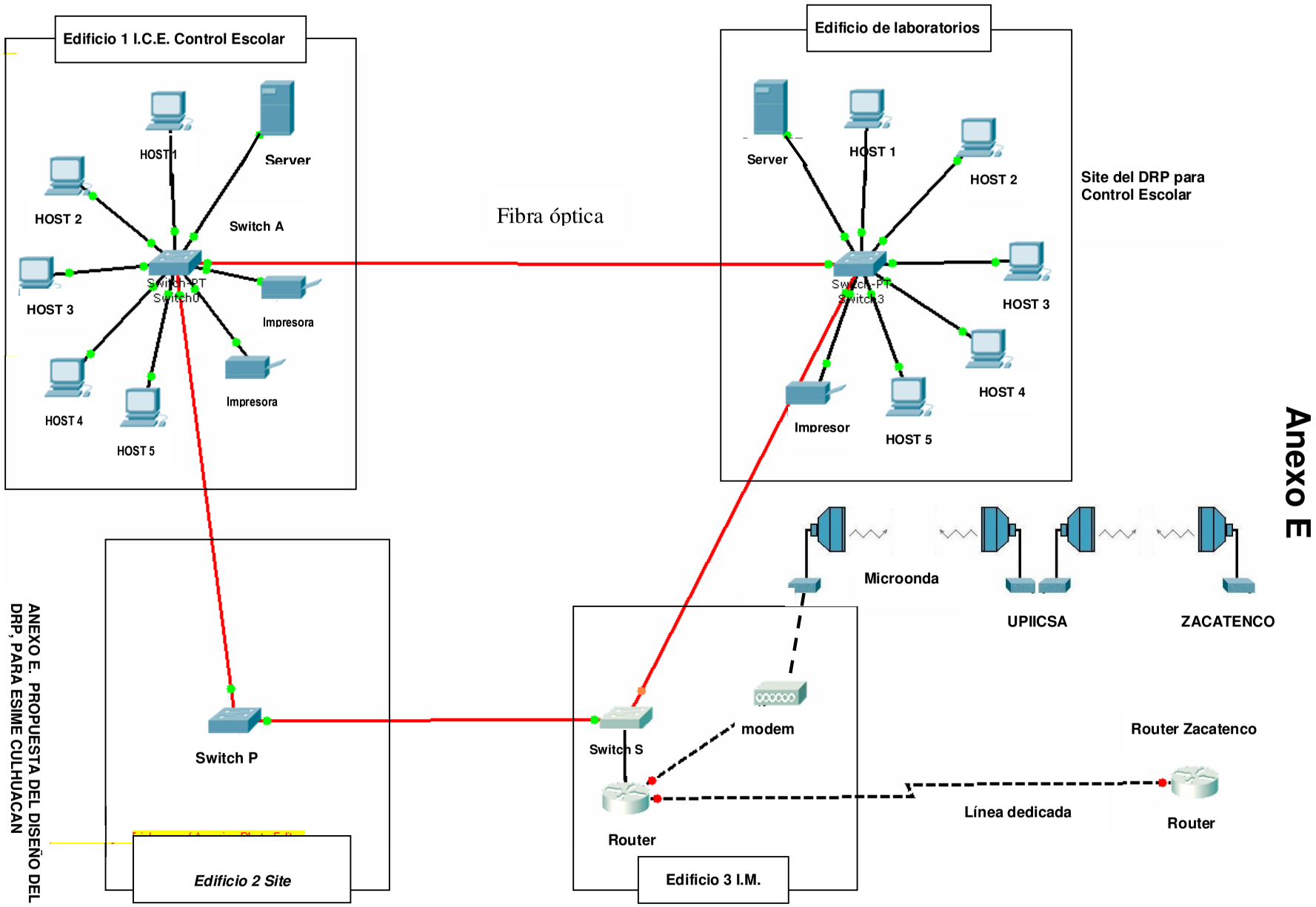


Figura 2 Distribución del Site


Edificio 1 I.C.E. Control Escolar
HOST 1
Server
HOST 2
Switch A
HOST 3
Switch-PT
Switch0
Impresora
Impresora
HOST 4
HOST 5
Fibra óptica
Edificio de laboratorios
Server
HOST 1
HOST 2
Site del DRP para
Control Escolar
HOST 3
Switch-PT
Switch3
HOST 4
Impresor
HOST 5
Anexo E
Microonda
UPIICSA
ZACATENCO
Switch P
Switch S
modem
Router Zacatenco
Línea dedicada
Router
Router
Edificio 2 Site
Edificio 3 I.M.
ANEXO E. PROPUESTA DEL DISEÑO DEL
DRP, PARA ESIME CULHUACAN

Anexo E

Cable	Nombre	Norma	Ancho de Banda	Velocidad	Impedancia	Long. de segmento	Nodos por Segmento	Topología	Conectores	Codificación
UTP-C5	100BaseTX	IEEE 802.3	125 MHz	100 Mbps	100 Ω	100 mts.	1024	Estrella	RJ-45	4B/5B

Tabla 1, Cable UTP

Cable	Nombre	Norma	Ancho de Banda	Velocidad	Impedancia	Long. de segmento	Nodos por Segmento	Topología	Conectores	Codificación
Fibra óptica	1000BaseSX	IEEE 802.3	------	1000 Mbps	0 Ω	550 mts.	------	Estrella	SC	------

Tabla 2, Fibra óptica

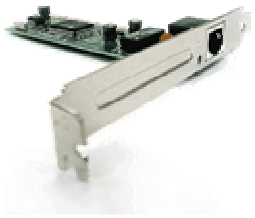


Figura 1, Tarjeta NIC

Figura 2, Switch

Figura 3, PC de escritorio

Figura 4, Impresora

Figura 5, Servidor

Anexo E

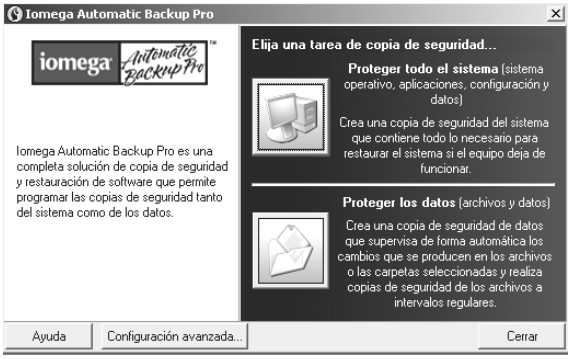


Figura 6.0, Programa Iomega

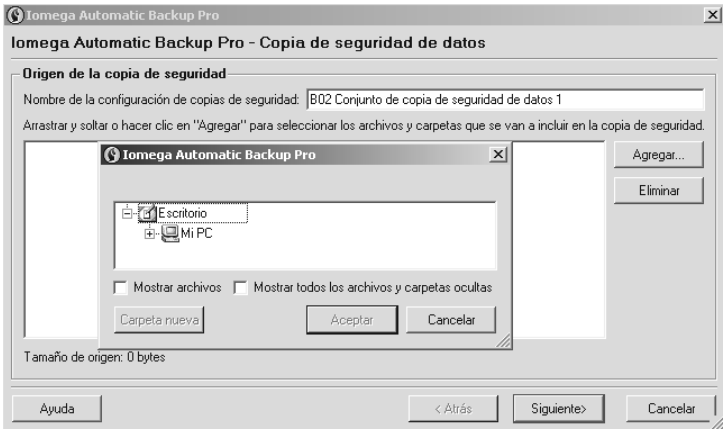


Figura 6.1, Copia de seguridad

FIGURA 6.2 Restauración

Anexo E

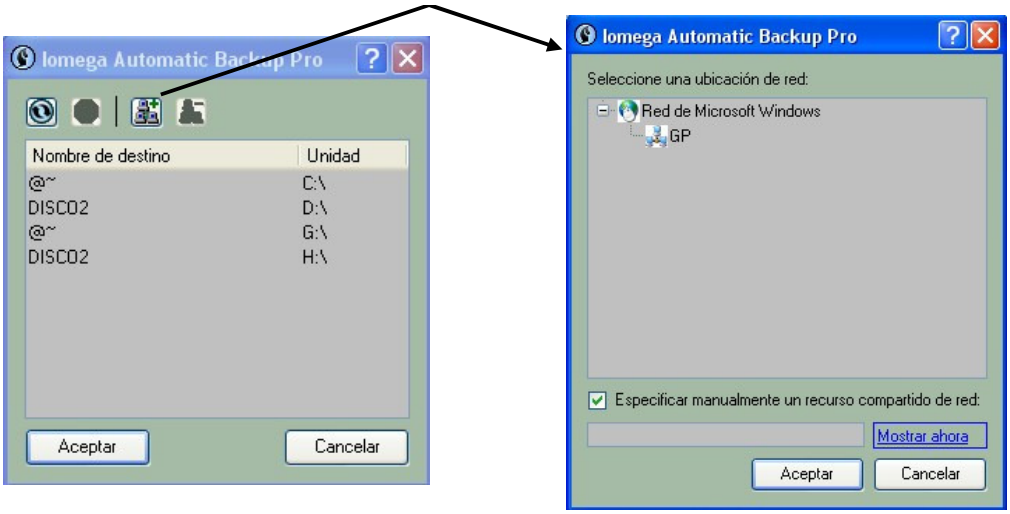


Fig. 6.3 Determinar dirección de copias de respaldo

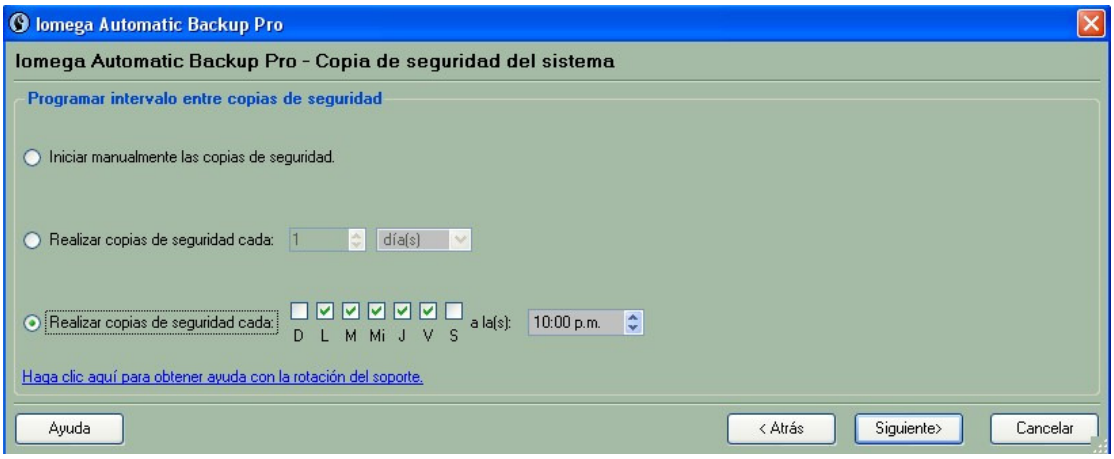
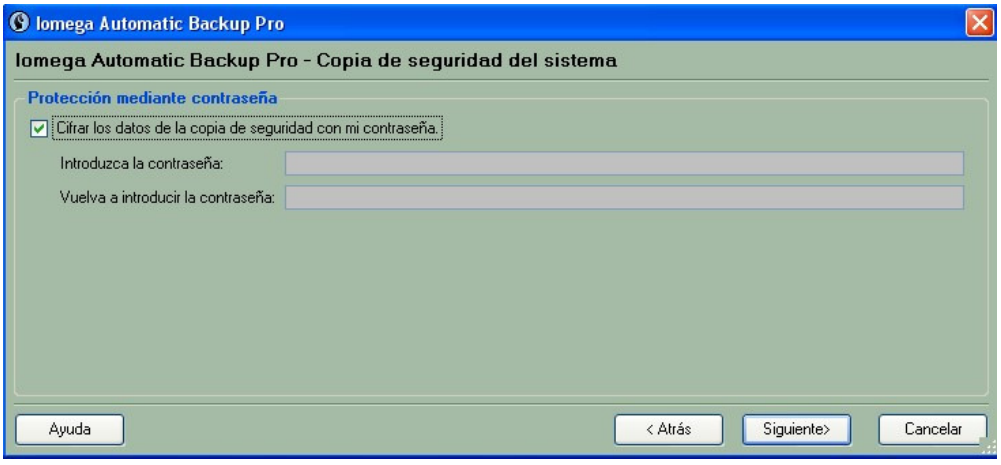


Fig. 6.4 Opciones para realizar copias de seguridad



6.5 Seguridad para las copias del sistema

INDICE DE TABLAS Y FIGURAS

GLOSARIO

Backbone
La parte de la red que transporta el tráfico más denso: conecta LANs, ya sea dentro de un edificio o a través de una ciudad o región.

E1
Es un formato de transmisión digital; su nombre fue dado por la administración de la (CEPT). Es una implementación de la portadora-E.
El formato de la señal E1 lleva datos en una tasa de 2,048 millones de bits por segundo y puede llevar 32 canales de 64 Kbps * cada uno, de los cuales treinta y uno son canales activos simultáneos para voz o datos en SS7 (Sistema de Señalización Número 7) en R2 el canal 16 se usa para señalización por lo que están disponibles 30 canales para voz o datos. E1 lleva en una tasa de datos algo más alta que el T-1 (que lleva 1,544 millones de bits por segundo) porque, a diferencia del T-1, no hace el bit-robbing y los ocho bits por canal se utilizan para cifrar la señal. E1 y el T-1 se pueden interconectar para uso internacional.

Fast Ethernet
Ethernet de alta velocidad a 100 Mbps (la Ethernet regular es de 10 Mbps). Existen dos tecnologías competidoras que surgen del IEEE. El primer método es el IEEE 802.3 100BaseT, que utiliza el método de acceso CSMA/CD con algún grado de modificación. Los estándares se anunciaron para finales de 1994 o comienzos de 1995.
El segundo, es el IEEE 802.12 100BaseVG, adaptado de 100VG-AnyLAN de HP. Utiliza un método de prioridad de demandas en lugar del CSMA/CD. Por ejemplo, a la voz y video de tiempo real podrían dárseles mayor prioridad que a otros datos.

Gigabit
No debe ser confundido con Gigabyte. Un gigabit es igual a 10^9 (1,000,000,000) bits, que equivalen a 125 megabytes decimales.

Gigabyte
El gigabyte (GB) equivale a 1.024 millones de bytes, o 1024 Megabytes. Se usa comúnmente para describir el espacio disponible en un medio de almacenamiento.

Hub
El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

Router
Un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino. El router esta conectado por lo menos a dos redes, y determina hacia que lado enviar el paquete de data dependiendo en el entendimiento del router sobre las redes que esta conectado. Los routers crean o mantienen una "tabla" de rutas disponibles, y

usa esta información para darle la mejor ruta a un paquete, en un determinado momento.

Servidor
Ordenador central de una red de ordenadores que suministra programas y servicios (impresora, disco duro, conexión a Internet...) a otros ordenadores menores llamados clientes. La filosofía cliente/servidor como base informática de las empresas está transformándose mediante sistemas basados en Internet e intranets.

Switch
Pequeños conmutadores que se utilizan para configurar la placa base y las tarjetas de los ordenadores.

Transceiver
En comunicaciones (informática) es un transmisor/receptor de señales de radio frecuencia (RF), sirve para conectar aparatos por vía inalámbrica.

TCP/IP
El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Transmisión Control Protocol (TCP) y el Internet Protocol (IP). En español es Protocolo de Control de Transmisión y Protocolo de Internet. Forma de comunicación básica que usa el Internet, la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

BIBLIOGRAFIA

- André J. Martín, DRP: Distribution Resource Planning : The Gateway to True Quick Response and Continuous Replenishment Edición Revisada

Nos presenta los puntos a crear para el DRP de la empresa

- Guía practica para el desarrollo de Planes de Continencia de Sistemas de Información, INEI, Instituto Nacional De Estadística e Información, Lima 2001

Maneja la seguridad informática como recurso primordial, Pagina de Gobernación Peruana

- CISP BOOT. AM.

Presentación en PDF, Presenta propuestas para la creación de un DRP, Buenos Aires Argentina, Febrero 2003, disponible en:

http://www.cccure.org/Documents/DonaldGlass/9_BusinessContinuityandDisasterRecoveryPlanning.pdf

- CONTINUIDAD DEL NEGOCIO

Presentación en PDF, Presenta los puntos viables para la creación de un DRP, Madrid, España 2004 disponible en:

http://es.sun.com/infospain/eventos/javaexpo2004/presentaciones/tracks9/FinalContingenciaUW.pdf

- KPMG

Presentación en PDF, presenta los puntos RPO y RTO de un DRP, México, D.F. Mayo del 2004, disponible en:

http://www.kpmg.com.mx/gobiernocorporativo/libreria_gc/gobierno-control/Administraci%C3%B3n%20Integral%20del%20Riesgo/Planificaci%C3%B3n%20de%20la%20Continuidad%20del%20Negocio.pdf

- "Redes de comunicación", Enciclopedia Microsoft(R) Encarta(R) 98. (c) 1993-1997 Microsoft Corporation. Reservados todos los derechos.
- REDES DE BANDA ANCHA en la dirección: http://www.ts.es/doc/area/produccion/ral/BANDA.HTM
- Laboratorio de Redes: http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html

Ral e Interconexión : http://www.ts.es/doc/area/produccion/ral/CABLE.HTM