UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

PLAN DE RECUPERACIÓN DE DESASTRE (DRP) EN EMPRESAS CON INFORMACIÓN TECNOLÓGICA

TESIS

QUE PARA OBTENER EL TITULO DE:

A C T U A R I O

PRESENTAN

ABIMAEL MENA TLAPANCO
ISABEL ANDREA CHAVARRIA CASTORENA
FRANCISCO HERNANDEZ MENDOZA

ASESOR: M. EN C. VICTOR MANUEL ULLOA ARELLANO

SEPTIEMBRE 2009

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Agradezco especialmente a Dios por todas las bendiciones que me dado y por permitirme alcanzar una de mis metas más importantes de mi vida.

A mis Padres, Ventura y Marcelina, por destinar parte de su vida para ayudarme a conseguir mis objetivos, gracias por su apoyo, comprensión y cariño.

A mis hermanas, Noemí, Erica y Areli, por estar siempre conmigo y porque mis alegrías también son suyas.

A mis compañeros de tesis, Andrea y Francisco, por su amistad y por soportarme un rato.

A mi asesor de tesis, Víctor Ulloa, por su tiempo, apoyo y dedicación para realizar este trabajo.

A la "Facultad de Estudios Superiores Acatlán" y a la "Máxima casa de estudios" que me han dado mucho a cambio de poco y de las cuales me siento orgulloso.

"Por mi raza hablará el Espíritu"

Abimael, Septiembre 2009

Esta meta, quiero compartirla y dedicarla:

A Dios.

Con todo mi amor,
agradecimiento y admiración:
A mi mamá: Isabel Castorena González.
A mi papá: Nicolás Chavarría Arroyo.

A mis queridas hermanas:
Margarita S. "Koko", por consentirme desde pequeña.
María del Carmen,
Mercedes,
Juanita, porque eres lo máximo,
Diana Agnela, mi "Kikitos"
A mi niña hermosa: Valeria.

Al amor de mi vida Gabino Héctor Barrera Guadarrama y a nuestro hijo: Arturo Nicolás Barrera Chavarría, gracias por existir te amo.

A mis queridos hermanos:
Juan,
Víctor Manuel, mi "negro hermoso",
Gustavo Adolfo,
José Nicolás,
Iván, mi "tachito"
A mis sobrinos; Rodrigo y Alán Pavel "eres grande".

Con profundo agradecimiento al M. en C. Víctor Manuel Ulloa Arellano.

A mis maestros sinodales por sus valiosas opiniones: Act. Luz Ma. Lavín, Act. Mahil Herrera Maldonado, Act. Miguel Ángel Macias y Fis. Mat. Jorge Luis Suárez Madariaga.

A mis amigos y compañeros de tesis: Frank y Abi, porque con ellos corroboré lo importante que es trabajar en equipo para conseguir juntos esta meta.

A la Alma Mater: Universidad Nacional Autónoma de México, Facultad de Estudios Superiores Acatlán, porque es mi orgullo ser universitaria.

A todos mis maestros y amigos.

"Por mi raza hablará el Espíritu"

Isabel Andrea, Septiembre 2009

Para llegar a esta meta agradezco:

A Dios por darme la oportunidad y fortuna de conocer y disfrutar de la vida.

A mis padres Catalina y Juan, que me han dado la vida y han sido un ejemplo a seguir.

A mi esposa Juanita por su comprensión y respaldo.

A Iván y Uriel por el tiempo que de ellos he invertido en este proyecto.

A mis hermanos, todos y cada uno por todo el apoyo que me han brindado cada vez que lo he requerido.

Un agradecimiento especial al M. en C. Víctor Manual Ulloa Arellano por su apoyo para la conclusión de este trabajo.

A los sinodales por sus valiosas opiniones, Act. Luz Ma. Lavín, Act. Miguel Ángel Macias, y Fis. Mat. Jorge Luis Suárez Madariaga, Act. Mahil Herrera Maldonado.

A mis amigos de todas las épocas y espacios, con el valor y aprecio que cada uno se merece.

Con especial atención y agradecimiento a mis compañeros de tesis: Abimael y Andrea, por su esfuerzo y solidaridad.

A la mejor Universidad América Latina y reconocida como una de las mejores del mundo, "Universidad Nacional Autónoma de México". "Facultad de Estudios Superiores Acatlán".

"Por mi raza hablará el Espíritu"

Francisco, Septiembre 2009

Contenido

		Página
Introducción		i
Capítulo 1.	**Importancia de la Información**	
1.1	Grandes Avances de la Tecnología en Información	2
1.2	Necesidad de Salvaguardar la Información	6
1.3	Seguridad de la información	11
1.3.1	Seguridad Física	11
1.3.2	Seguridad Lógica	23
1.3.3	Seguridad en Redes	31
Capítulo 2.	**El Análisis de Riesgos**	
2.1	Objetivo del Análisis	42
2.2	Identificación de Riesgos	43
2.3	Técnicas de Análisis	45
2.3.1	Métodos cuantitativos	45
2.3.1.1	Análisis de regresión	45
2.3.1.2	Series de tiempo	51
2.3.1.3	Probabilidad de Ocurrencia	55
2.3.1.4	Cálculo de Pérdida Probable (Impacto)	55
2.3.1.5	Pérdida Máxima Probable	56
2.3.2	Métodos cualitativos	56
2.3.2.1	Métodos Comparativos	56
2.3.2.2	Métodos Generalizados	58
2.4	Tratamiento del Riesgo	63
Capítulo 3.	**Estrategias de Prevención**	
3.1	Desastres de Probable Ocurrencia en México	68
3.2	Sistemas de Seguridad	70
3.2.1	Información	70
3.2.2	Características de la Información	71
3.2.3	Sistemas de Seguridad de la Información	71
3.3	Plan de Contingencia y su Utilidad	78
3.4	Plan de Contingencia: Origen, Elementos y Personal	78
Capítulo 4.	**Desarrollo del Plan de Recuperación**	
4.1	Introducción al Plan de Recuperación de Desastre	82
4.2	Relación Costo-Beneficio	83
4.3	Metodologías de Desarrollo	84
4.3.1	Metodología de William Toigo	84
4.3.2	Metodología de Hewlett Packard	86
4.4	Método Propuesto	91

Capítulo 5. Caso Práctico de un DRP en la compañía de telecomunicaciones "Directv México"
5.1 Visión General 116
5.2 Plan de Recuperación de Desastres 117
5.2.1 Etapa 1. Actividades Previas al Desastre 117
5.2.2 Etapa 2. Actividades Durante el Desastre 136
5.2.3 Etapa 3. Actividades Después del Desastre 141
5.3 Administración del Plan 143
5.4 Manuales 146

Conclusiones 147

Glosario 149

Anexos 155

Bibliografía 169

Sitios de Internet 171

Proveedores y servicios 172

Objetivo del Trabajo

Elaborar un plan de recuperación en caso de desastre que facilite superar situaciones adversas o no deseadas y que nos permita continuar las actividades normales de las empresas con información tecnológica a pesar de los daños que pueda haber sufrido a consecuencia de desastres de tipo natural o debido a fallas del equipo y humanas, para poder actuar con prontitud ante cualquier dificultad, organizar la reiniciación provisional de las labores más importantes y posteriormente reestablecer en forma integral todas las actividades.

Hipótesis

Desde la creación de una empresa u organización y a través de su vida activa, ésta se encuentra expuesta a diversas eventualidades que ponen en peligro su operación, riesgos de magnitud y de cobertura, agravados por los cambios en su naturaleza y de la cual consideramos que en México no se elabora el suficiente análisis en la planeación, por lo que consideramos necesario la existencia de la implementación de un DRP "*Disaster Recovery Planning*" o Plan de Recuperación en caso de Desastre, debido a que las medidas tradicionales de prevención tales como: sistemas de alarmas, vigilancia, seguros, entre otras, no son suficientes para lograr la continuidad de la operación de la empresa con información tecnológica.

Introducción.

Para la historia de la humanidad, que se remonta a más de 200,000 años, el siglo XX y el inicio del XXl representa apenas una diminuta fracción en el tiempo. En estos escasos poco más de 100 años, sin embargo, los seres humanos hemos visto cambios tan espectaculares en tantas ramas del conocimiento, que resulta muy difícil imaginarnos ahora la forma como vivían nuestros ancestros hace apenas un par de generaciones. Desde el motor de combustión interna que eliminó la tracción animal y dio origen al automóvil y al aeroplano, hasta la energía atómica con sus enormes riesgos y beneficios, la lista de innovaciones y descubrimientos en esta centuria rebasaría con mucho la imaginación más prolífica de los Verne, Newton, Da Vinci o cualquier ilustre inventor visionario de los siglos anteriores.

A pesar de todos los avances que han enmarcado esta época, si pudiéramos adelantar el tiempo y ver la historia de la humanidad dentro de 1000 años, veríamos que el siglo XX será recordado por las futuras generaciones como el período que dio inicio al procesamiento electrónico de datos y a la automatización de las operaciones repetitivas. Este será llamado el Siglo que marcó el inicio de la Era de la Información, el Siglo de la Computación.

A medida que ha emergido de sus años de infancia, la computadora ha ido asumiendo responsabilidades de trabajo cada vez mayores hasta convertirse, hoy en día en el caballo de batalla de nuestros negocios. Hospitales, empresas, agencias gubernamentales, de transportación y en general cualquier tipo de organización, usan computadoras para registrar y mantener el control de sus activos, nóminas, inventarios y otros valores. No sabemos hasta dónde llegará esta dependencia de la computadora en la sociedad, lo que si sabemos es que mientras más vital sea su función, más importante será protegerlas de fallas, catástrofes, ataques criminales, entre otras. Sin ellas, instituciones educativas, empresas y gobiernos podrían quedar totalmente varados.

En la actualidad, la computación se aplica a las funciones contables, de manufactura, diseño, publicidad, distribución, y muchas más actividades de las empresas. Existe una creciente dependencia de la administración hacia esta tecnología, sin embargo, la computadora resulta ser algo más que una herramienta de apoyo para la organización. De no ser por ella, muchas organizaciones no podrían ofrecer ciertos servicios o no podrían existir.

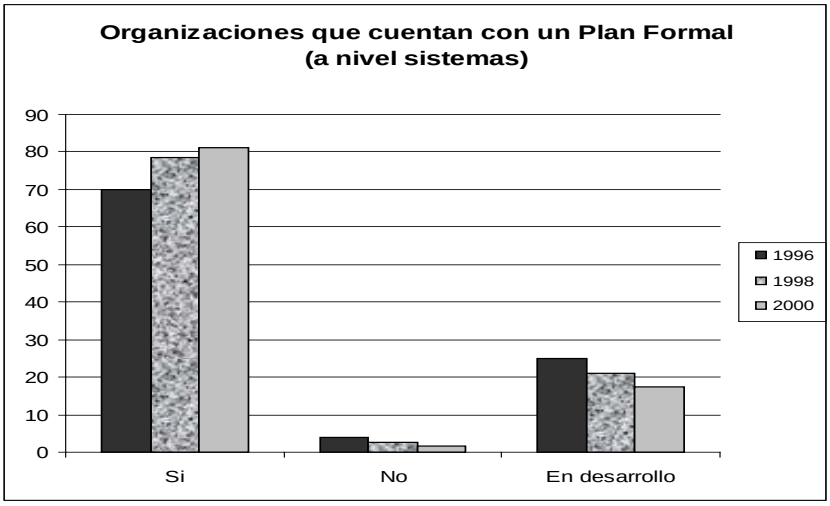
En particular, podemos decir que durante los últimos 20 años, el procesamiento de datos se ha convertido en el centro nervioso de la comunidad financiera (bancaria bursátil). La automatización de actividades cotidianas dentro del medio financiero ha provocado una dependencia de la computadora. Las instituciones han encontrado en ella una herramienta que simplifica, acelera y da confiabilidad a las operaciones. A medida que esta dependencia se incrementa, también lo hace el riesgo financiero asociado a una pérdida de la capacidad de procesamiento. Además, un factor más reciente que afecta la seguridad en forma creciente es la introducción de sistemas de distribución y el uso de redes e instalaciones de comunicaciones para transmitir datos entre terminales de usuario y computadoras y entre computadoras. Muy relacionado con esto, el fenómeno del *downsizing* (así como el *rightsizing*)♦, es una realidad en un número de empresas cada vez mayor. La seguridad de redes se necesita, principalmente, para proteger los datos durante su transmisión.
Por lo anterior, no es exagerado decir que el significado real de las computadoras es la supervivencia: por un lado la supervivencia de una operación vital dentro de una organización y por otro, la supervivencia de la empresa misma, sin embargo, esta fuerte dependencia rara vez es notada por aquellas personas que no tienen contacto directo con el procesamiento de la información a través de

♦ Término definido en el Glosario.

la computadora, aún estando dentro de la organización. Las consecuencias de una pérdida de los sistemas de información del negocio muchas veces no se consideran sino hasta que ocurre un desastre, la mayoría de la gente no piensa en esta posibilidad.

Sin embargo, los desastres ocurren y por eso las empresas deben de estar preparadas para tratar de evitar al máximo su ocurrencia o para minimizar las pérdidas causadas por ello. La presencia o ausencia de medidas de seguridad de la información es el factor más importante para que una empresa se vea o no, impactada por una eventualidad negativa. De manera similar, la presencia o ausencia de un plan de contingencia es el factor más importante para que una empresa sobreviva o desaparezca después de un desastre. Las compañías que desarrollan sus planes de contingencia, que diseñan procedimientos de emergencia y de recuperación, que entrenan a su personal en estos procedimientos y que los prueban y efectúan simulacros, tienen mayor probabilidad de sobrevivir a los desastres.

Figura A



En la *figura A*, la gráfica muestra que cada vez existen más empresas que han desarrollado un plan de contingencia en los Estados Unidos de Norteamérica. Una de las razones por la que la dirección de la empresa rara vez piensa en prepararse para afrontar un desastre, es precisamente la concepción que se tiene de éste. Al hablar de desastre se piensa inmediatamente en terremoto o incendio o tal vez también en inundación o explosión.

Se piensa entonces que la probabilidad de que un terremoto destruya la sede de la empresa es muy baja, es decir, pensar en desastre equivale a pensar en catástrofe y es correcto hasta cierto punto, una catástrofe provoca un desastre; pero no es la única causa que origina este evento adverso.

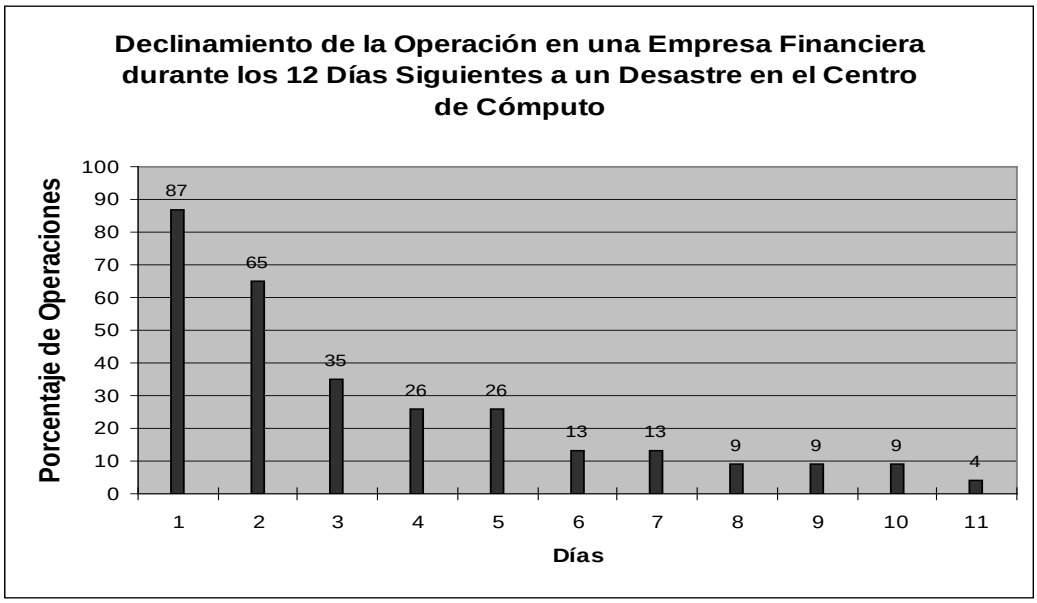
Por lo que se hace necesario establecer el concepto de desastre, para este trabajo el término desastre deberá entenderse como la interrupción en la capacidad de acceso a la información y procesamiento de la misma a través de las computadoras, necesaria para la operación normal de las empresas. Es decir, el concepto de contingencia o desastre va enfocado a una consecuencia más que a una causa, por lo tanto al utilizar cualquiera de estas dos palabras no nos estamos refiriendo a algún tipo de catástrofe ya sea natural o causada por el hombre, sino a una situación en la que se encuentra la empresa. Esta situación problemática (no poder acceder o procesar la información)

puede conducir a su vez a la suspensión total de operaciones del negocio y eventualmente a la desaparición del mismo.

El concepto de desastre se refiere tanto a la pérdida de la capacidad de procesamiento de información, como a la pérdida de información misma. En lo relativo a la pérdida de la capacidad de procesamiento de información, es evidente que lo ideal sería disponer del procesamiento todo el tiempo necesario; sin embargo esto podría no ocurrir así debido a una contingencia. Surge entonces la pregunta: ¿Cuánto tiempo puede suspenderse el procesamiento antes de que surjan efectos negativos como consecuencia?

La respuesta a esta pregunta depende de las circunstancias de cada empresa, del tipo de actividad que realice, del grado de automatización de sus procesos, de la importancia que tenga la tecnología de la información para la operación de la empresa, entre otros. Lo que si permanece constante es la importancia crítica del factor tiempo en la restauración del funcionamiento de los sistemas para sobrevivir a un desastre.

Figura B

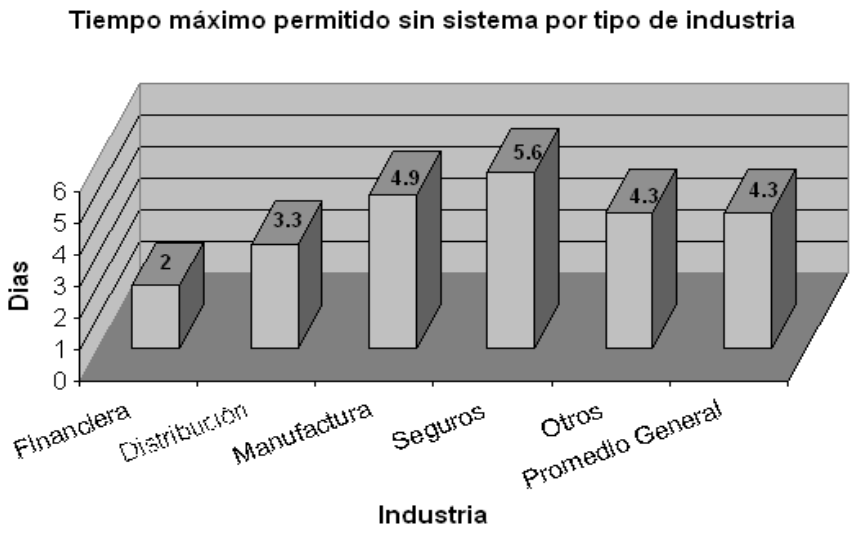


Existen ciertos estudios que se han hecho respecto a los efectos que tiene en las empresas el permanecer determinado tiempo sin funciones de cómputo. En la *figura B* se muestra la gráfica de un estudio realizado por la Universidad de Minnesota. En ella se muestra el impacto que tiene en las empresas del ramo financiero una suspensión en el procesamiento de datos durante los primeros once días.

Como puede observarse, una falla en el procesamiento con una duración de un día degradará la actividad normal del negocio en un 13%. Así mismo, una suspensión del procesamiento de once días ocasionará una pérdida del 96% de la actividad del negocio.

En el mismo estudio se examinó la vulnerabilidad de industrias específicas, demostrando el tiempo máximo sin procesamiento permitido por la industria, antes de que la recuperación sea virtualmente imposible.

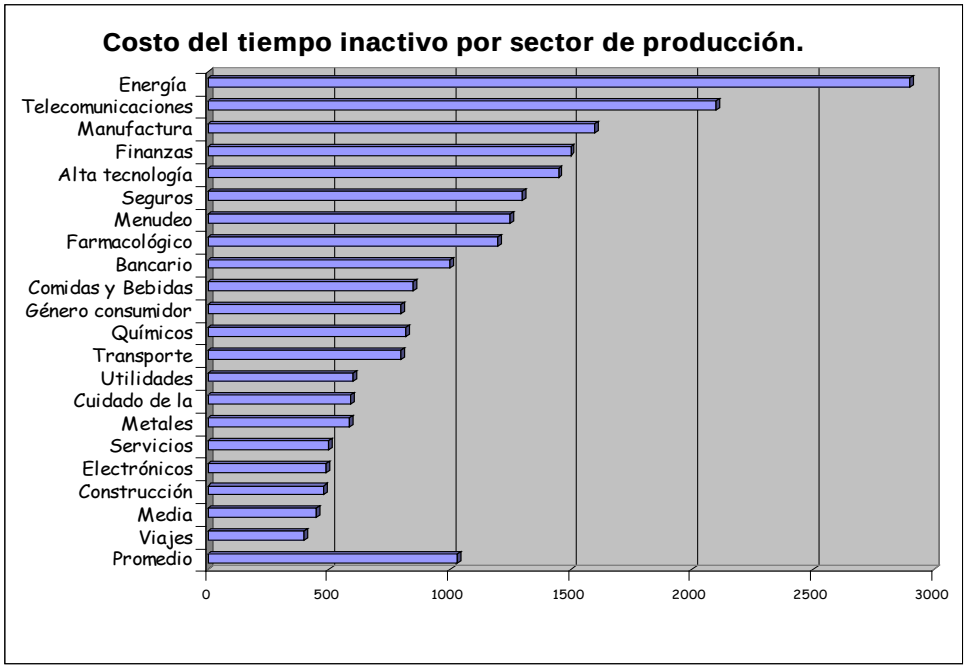
Figura C



Como se ve en la *figura C* las empresas financieras tienen la menor tolerancia a una suspensión prolongada, mientras que las de seguros y manufacturas pueden tolerar periodos un poco mayores sin un colapso del negocio (porque aún acostumbran el manejo de archivos impresos).

La suspensión de las operaciones en los diversos sectores productivos (*figura D*), trae como consecuencia un impacto económico que como puede verse actualmente en Estados Unidos es de 1,010,536 dólares por hora, siendo el sector energético el más afectado económicamente, seguido por el sector de telecomunicaciones.

Figura D



Para resaltar aún más la importancia de la necesidad de implantar medidas de seguridad de la información y desarrollar planes de contingencia, a continuación mostramos como la catástrofe del 11 de septiembre del 2001, siendo un acontecimiento local de la Unión Americana tuvo gran repercusión y difusión mundial.

World Trade Center, Las torres gemelas.
Es una verdad que por más protegidos que estén nuestros sistemas, siempre estarán expuestos a riesgos inconcebibles; este es el caso de Las Torres Gemelas en Nueva York.

Las Torres Gemelas del World Trade Center (Centro Mundial del Comercio) eran uno de los principales símbolos de la ciudad de Nueva York y el corazón del principal distrito financiero del mundo. Construidas en 1977, los edificios de 110 pisos y 411 metros de altura, eran la tercera construcción más alta del mundo. Unas 50,000 personas trabajaban en el complejo y más de 90,000 turistas la visitaban cada día, según las cifras de las autoridades del puerto de Nueva York.

El World Trade Center ya había sido blanco de un atentado terrorista el 26 de febrero de 1993 cuando un camión bomba explotó en el estacionamiento subterráneo del centro, causando la muerte de seis personas, más de 1,000 heridos, la evacuación inmediata del complejo de edificios y de 510 millones de dólares en pérdidas.

La explosión no solo afectó al World Trade Center, sino también sacó del aire a las estaciones de radio y televisión locales y causó congestionamiento en las calles de Manhattan fuera de todo control; todas las principales arterias de la sección baja de Manhattan fueron cerradas a todos los vehículos excepto los de emergencia.

El accidente tomó por sorpresa a las comunidades financieras y de negocios del mundo y desafortunadamente muchas compañías con centros de datos o centros de impresión remota en el complejo, no tenían un plan de recuperación de desastres.

11 de Septiembre...
El 11 de septiembre del 2001, el corazón financiero de la ciudad de Nueva York fue devastado, luego del atentado en que dos aviones boeing 767 de la empresa Airlinees, se estrellaron contra Las Torres Gemelas del World Trade Center. Estos gigantes de hierro y concreto albergaban un total de 376 empresas, de las cuales 193 se encontraban ubicadas en la Torre Norte y otras 183 en la Torre Sur.

La compañía de inversiones 'Cantor Fitzgerald', perdió a los cerca de 700 empleados que trabajaban en el edificio, entre ellos su vicepresidente y asociado, John Thomas Jr Mcerlean, de los aproximadamente mil trabajadores y directivos que integraban su plantilla. A su vez, la aseguradora 'Marsh y Mclennan', perdió a 300 de sus ejecutivos, la sociedad de inversiones 'Fred Alger Management' a 38 y 'Carr Futures' a 70, entre la extensa lista de sociedades financieras y comerciales arrendatarias de las torres que recibieron directamente el impacto de las aeronaves.

Entre las empresas más afectadas por la colisión figuran la aseguradora 'Sandler O'Neill and associated', 'Aon Corporation', la consultora financiera 'Keefe, Bruyett y Woods' y 'Morgan Stanley'. También disponían de oficinas en las torres siniestradas la aseguradora Allianz, American Express, AT&T Corporation, Avis Car Rental, Banco Latino Americano de Exportaciones, Bank of America, Bank of Indonesia, Bank of Taiwan, varios canales de televisión, entre ellos CNN, Delta

Airlines, Dow Jones, Dun & Bradstreet Research, Firts Commercial Bank Financial Institute, Fuji, Generali, Hyundai Securities Co. Investments, ITT, Kaiser Overseas Manufacturing, entre otras compañías.

Asimismo, los edificios destruidos albergaban organismos oficiales. En la Torre Norte se encontraba la sede de la Autoridad Portuaria de Nueva York y Nueva Jersey. También había oficinas del FBI y de los Servicios Secretos, del Ayuntamiento de Nueva York y de departamentos municipales que supervisan el tráfico, el Medio Ambiente y la oficina de acción inmediata contra terremotos y atentados con armas tóxicas.

Algunas empresas no pudieron rescatar en su totalidad sus sistemas de información debido a que no tuvieron acceso a sus sistemas o no contaban con respaldos fuera de la oficina, más aún porque se quedaron sin ejecutivos y personal operativo.

Algunas compañías arrendatarias de oficinas de los World Trade Center I y II de Nueva York ante la desaparición de la mayor parte de sus equipos directivos, se vieron obligadas a nombrar apresuradamente, sustitutos temporales para continuar sus actividades mercantiles. Las compañías más afectadas acometieron la reestructuración de sus organigramas con la discreción más absoluta para no perder así la confianza de sus clientes.

A niveles económicos se estiman daños aproximados de 120,000 millones de dólares, además de un total de 3,000 perdidas humanas sin mencionar a las empresas que ya no pudieron continuar con sus actividades comerciales.

Las pérdidas totales en vidas y propiedades le costaron a las compañías de seguros una suma estimada en 40,000 millones de dólares. Este costo directo fue insignificante en comparación con los costos indirectos. Se cerraron centros comerciales y restaurantes en todo el país por un mínimo de 24 horas, se evacuaron edificios de oficinas altamente vulnerables; se obligó a los aviones permanecer en tierra; y el mercado de valores cesó sus actividades durante cuatro días consecutivos.

Los ataques impactaron a toda la industria turística y de vacaciones en Estados Unidos, afectando desde parques hasta hoteles y cruceros. Walt Disney, Carnival Corp. Starwood Hotel and Resorts, dueño de los Sheraton Westin están entre las más golpeadas.

El aeropuerto de Los Ángeles perdió en tan solo una semana cerca de 16 millones de dólares. El impacto en las Líneas Aéreas ha sido notable, se calcula que una cifra superior a los 250 mil empleados de esta industria se quedó sin empleo en todo el mundo, como consecuencia de las reducciones en los vuelos internacionales.

En toda la historia de la humanidad no se había registrado un caso de esta magnitud que además de no contar con los recursos necesarios para continuar con las operaciones de tantas empresas, tampoco se dispusiera del personal experto para reorganizar la recuperación de sus operaciones comerciales y financieras.

El tema de desastres, tanto naturales como los ocasionados por acciones del hombre y sus graves consecuencias, así como la problemática que lo rodea, no corresponden únicamente a la época actual. Desde sus orígenes, el hombre en su lucha por sobrevivir ha tenido que enfrentar los riesgos que surgen de la necesidad de obtener los recursos indispensables para su subsistencia, ha evolucionado

a tal grado que ya no visualiza el riesgo como pérdida probable, sino da paso a la relación riesgo – oportunidad, lo que le permite tener una visión más completa.

Con el transcurso de los siglos, la situación ha ido mejorando debido a los avances científicos y tecnológicos, considerando la prevención y el combate hacia los diversos peligros a que está expuesta la población mundial en cada momento, sin embargo, desafortunadamente las cifras estadísticas de la ONU, muestran una tendencia creciente de desastres, tanto en magnitud como en alcance, que se ve agravada por los cambios de su naturaleza (variaciones de características y en los patrones de ocurrencia), debido a lo anterior y dada la importancia de los desastres, la Organización de las Naciones Unidas (ONU) desde 1990, estableció El Decenio Internacional de Reducción de Desastres Naturales.

En Estados Unidos, el tema de seguridad de la información, especialmente en planes de contingencia, ha tomado mucha importancia, debido a la confianza que existe hacia los sistemas de información.

En México, sentimos que falta una cultura de prevención, gozamos de escasez de proveedores de bienes y servicios relacionados con la seguridad tecnológica de la información. Por ejemplo, a la fecha existen dos despachos de consultoría que desarrollan planes de contingencia (Coopers and Lybran, S.A. de C.V) y Cauferrat Consultores.

En particular, en la Ciudad de México y zona Metropolitana, a partir del siglo XX, la explosión demográfica y la concentración de la población en esta área, han multiplicado las posibilidades de calamidades de origen humano y han hecho que las de origen natural incrementen sus posibilidades de provocar no solo peligros, sino también cuantiosos daños tanto a la población como a sus bienes y servicios. Baste recordar el sismo que sufrimos en 1985 y del que pocos estaban preparados para un evento de tal magnitud y de tan graves consecuencias.

Por lo anterior, resalta la necesidad de que las empresas mexicanas, particularmente las que se encuentran en la zona metropolitana de la ciudad de México, se concienticen de la importancia que tiene la prevención de siniestros así como la protección de sus recursos informáticos de las graves consecuencias que puede traerles la pérdida o inhabilitación de información para seguir operando, ejemplo: el deterioro del nivel de servicio de la empresa y mala imagen ante clientes y público consumidor. Incluso el cierre parcial o total de su empresa. Además de la importancia de la responsabilidad que asumen al manejar información de tipo confidencial de sus clientes, razones mínimas por lo que resulta totalmente básico e indispensable, contar con un programa integral de seguridad de su información y prepararse para eventualidades con el desarrollo de un PLAN DE RECUPERACION EN CASO DE DESASTRE; tema de tesis para el presente trabajo.

A lo largo de este trabajo, se consideran las técnicas de análisis y evaluación de riesgos así como los factores que pueden afectar a las empresas ubicadas en nuestro país, en el caso práctico aplicado a una empresa de telecomunicaciones DIRECTV identificamos las principales amenazas de las que podemos citar: rayos, huelgas, interrupciones de suministro eléctrico, amenazas de bomba o explosión, fuego, inundaciones, entre otros y se establecen algunas vulnerabilidades que no contempla el plan.

Para el desarrollo hemos utilizado una metodología científica, definiendo primeramente el problema, haciendo el trabajo de investigación y adaptando los métodos de solución de acuerdo a la necesidad, pero al mismo tiempo evaluando los riesgos que pueden afectar a estas empresas, proponiendo

técnicas de análisis y cálculo de perdidas con el afán de justificar una inversión que para ciertas empresas podría resultar muy costoso en el desarrollo de programas de recuperación.

En general el proyecto de investigación será tratado en cinco capítulos cuyos objetivos se describen a continuación:

En el capítulo 1, analizaremos como el manejo de información a través de máquinas se ha infiltrado poco a poco en nuestras tareas habituales y la gran influencia que por consiguiente ha tenido en nuestra vida diaria. Asimismo abordaremos sobre los peligros que amenazan la integridad, el carácter confidencial y la disponibilidad de los datos almacenados en los sistemas de cómputo.

En el capítulo 2, identificaremos los riesgos que afectan a la información, se evaluará el impacto que estos provocan, se presentaran las principales técnicas utilizadas para su análisis y las diferentes maneras de administrarlos.

De acuerdo a lo señalado en los capítulos anteriores, en el capítulo 3, continuaremos con la elaboración de una estrategia que nos permita, analizar la situación relativa a la seguridad de la información e identificar necesidades.

Posteriormente en el capítulo 4, presentamos el marco conceptual de los planes de recuperación de desastres e incluimos dos métodos para el desarrollo de planes de recuperación, además, proponemos en esta tesis, el diseño de una nueva metodología de desarrollo de un plan de recuperación en caso de desastres.

Por último en el capítulo 5, se desarrollará el caso práctico de un DRP tomando como objetivo, la compañía de telecomunicaciones "DIRECTV México", en este caso realizamos una aplicación práctica del método propuesto, dando como resultado una versión completa y definitiva de un DRP para la empresa objetivo.

Particularmente este trabajo se dirige a administradores de empresas con un alto grado de dependencia de la operación de computadoras, a profesionistas cuyo ámbito laboral este relacionado con el manejo electrónico de la información y a toda persona que tenga interés en conocer técnicas y herramientas para elaboración de planes de recuperación de desastres.

Capítulo 1

Importancia de la Información.

1.1. Grandes avances de la tecnología en información

El mundo de la alta tecnología nunca hubiera existido de no ser por el desarrollo de la computadora. La sociedad en conjunto utiliza estas máquinas, en distintos tipos y tamaños, para el almacenamiento y manipulación de datos. Los equipos informáticos han abierto una nueva era en su fabricación gracias a las técnicas de automatización y han permitido mejorar los sistemas modernos de comunicación. Son herramientas esenciales prácticamente en todos los campos de investigación y en tecnología aplicada.

La tecnología de información, que engloba a los equipos de procesamiento de datos, automatización de oficinas y telecomunicaciones, fue uno de los desarrollos científicos y tecnológicos que más transformó nuestro mundo en la segunda parte del siglo XX. El desarrollo de esta tecnología ha sido fantástico y sorprendente y se ha llevado a cabo de una forma extraordinariamente veloz.

La historia de la tecnología de información no es muy larga, en lo que al tiempo se refiere; sin embargo, es muy vasta por el número tan grande de elementos de hardware y software que han surgido en su desarrollo. Es interesante voltear hacia atrás para reconocer el camino andado y a los creadores de esta historia. Esto con el fin de reconocer y darle valor a lo que poseemos hoy día y tener elementos para dibujar un panorama de lo que nuestro mundo podrá ser en unos años más.

Si somos capaces de identificar los factores que han provocado los éxitos en esta historia, así como reconocer los errores que han conducido a algunos fracasos, podremos plantear proyectos factibles de realizar en el futuro y continuar con la conformación de un mundo que busque el bienestar de sus sociedades. Así mismo, estaremos en posibilidad de anticipar los grandes cambios y preparar, de esta manera, a nuestra gente y sus organizaciones para integrarse en la sociedad del futuro.

Nacimiento de la computadora.
PC IBM.
International Bussines Machines Corporation, IBM, fabricante estadounidense de ordenadores o computadoras, con sede en Armonk, Nueva York. IBM es uno de los grandes proveedores de sistemas de tratamiento de información, software, sistemas de comunicaciones, estaciones de trabajo y suministros y servicios auxiliares en todo el mundo. Sus productos se utilizan en una amplia variedad de entornos, desde las compañías privadas hasta los organismos públicos, pasando por las organizaciones científicas, la defensa, la medicina, la exploración del espacio y muchos más. La compañía se estableció en 1911 como Computing-Tabulating-Recording Company, producto de la fusión de tres compañías menores. Tras varias adquisiciones, absorbió a la International Business Machines Corporation en 1924 y tomó su propio nombre. Thomas Watson llegó ese mismo año y comenzó a convertir la indecisa compañía en un gigante industrial. IBM se convirtió con rapidez en el fabricante de relojes de control de personal más importante de Estados Unidos y desarrolló y comercializó la primera máquina de escribir eléctrica. En 1951 la compañía entró en el terreno de las computadoras. El desarrollo de la tecnología de IBM se financió en gran medida mediante contratos con la Comisión de Energía Atómica del gobierno de Estados Unidos. El paralelismo entre los productos fabricados para el gobierno y los comercializados por la compañía era evidente.

A finales de la década de 1950, IBM se distinguió por dos innovaciones: el concepto de familia de computadoras (su familia 360) que permitía ejecutar el mismo software en todos los equipos pertenecientes a la familia y la nueva máxima de la empresa, según la cual todos los clientes podrían utilizar con éxito un sistema IBM. Esta nueva política produjo una enorme lealtad hacia el Big Blue, o

gigante azul, sobrenombre con que se empezó a conocer a IBM. Entre la década de 1960 y la de 1980, IBM dominó el mercado global de las grandes computadoras, aunque durante los años ochenta comenzó a ceder terreno ante otros fabricantes en áreas especializadas como la computación de alto nivel. Cuando durante la década de 1970 aparecieron los miniordenadores o minicomputadoras, IBM los vio como una amenaza a su mercado de grandes computadoras y no supo reconocer su potencial, dando pie al éxito de competidores como Digital Equipment Corporation, Hewlett-Packard y Data General. Sin embargo, en 1981 IBM presentó con gran éxito el IBM PC, que se convirtió rápidamente en un modelo de la microinformática. La compañía tuvo menos éxito a la hora de defender su cuota de mercado frente a otras empresas en el terreno de los costos de fabricación. A finales de la década de los 80, IBM se convirtió en el mayor productor del mundo de una línea completa de computadoras y en el principal productor de equipos de oficina, incluyendo máquinas de escribir y fotocopiadoras. Así mismo, la compañía era el principal fabricante de circuitos integrados para sus propios productos.

La venta de grandes computadoras y el software y los periféricos correspondientes suponían casi la mitad del negocio de IBM y entre un 70% y un 80% de sus beneficios. A principios de la década de 1990, en plena recesión de la economía estadounidense, IBM se reorganizó formando divisiones autónomas más cercanas a los diversos mercados de la empresa. Como consecuencia, 40.000 empleados perdieron sus puestos de trabajo en 1992 y se anunciaron más recortes para 1993. A principios de 1993, tras batir el récord de pérdidas en 1992 y sufrir un recorte en los dividendos de las acciones por primera vez en su historia (a menos de la mitad de su valor anterior), John F. Akers, presidente desde 1985 dimitió. En abril de 1993 se designó como presidente de la compañía a Louis V. Gerstner, hijo. En 1994, IBM se asoció con Apple Computer Inc. para fabricar el Power PC, una computadora capaz de ejecutar programas de ambas empresas. En 1995, IBM adquirió la Lotus Development Corporation, una empresa de soporte lógico, para ampliar su presencia en dicho sector.

Su historia y evolución.

En 1981 IBM presentó el llamado IBM PC. Aunque no incorporaba la tecnología de computación más avanzada, el PC se convirtió en un hecho clave y fundamental dentro de este sector en ebullición. Demostró que la industria de las microcomputadoras era algo más que una moda pasajera y que, de hecho, las microcomputadoras eran una herramienta necesaria en el mundo empresarial. La incorporación de un microprocesador de 16 bits en el PC inició el desarrollo de micros más veloces y potentes. Así mismo, el uso de un sistema operativo al que podían acceder todos los demás fabricantes de computadoras abrió el camino para la estandarización de la industria.

A mediados de la década de 1980 se produjeron una serie de desarrollos especialmente importantes para el auge de las microcomputadoras. Uno de ellos fue la introducción de un potente procesador de 32 bits capaz de ejecutar sistemas operativos multiusuario avanzados a gran velocidad. Este avance redujo las diferencias entre micro y minicomputadora, dotando a cualquier equipo de sobremesa de una oficina con la suficiente potencia informática como para satisfacer las demandas de cualquier pequeña empresa y de la mayoría de las empresas medianas.

Otra innovación fue la introducción de métodos más sencillos y amigables para el control de las operaciones de las microcomputadoras. Al sustituir el sistema operativo convencional por una interfaz gráfica de usuario, computadores como el Apple Macintosh permiten al usuario seleccionar iconos —símbolos gráficos que representan funciones de la computadora— en la pantalla, en lugar de requerir la introducción de los comandos escritos correspondientes. Hoy en día ya existen nuevos sistemas controlados por la voz, en los que los usuarios operan sus computadoras utilizando las palabras y la sintaxis del lenguaje hablado.

Las microcomputadoras surgieron a finales de los 60, como elemento de transición entre las generaciones tercera y cuarta, con los circuitos integrados de media escala (MSI), sus destinatarios fueron grandes y medianas empresas, disponían de varias terminales y se organizaban en redes.

Computadoras de Cuarta Generación

El elemento que provocó el nacimiento de esta generación se considera habitualmente, aunque con cierta controversia, el microprocesador Intel 4004, desarrollado por Intel en 1971. El primer computadora personal en EE.UU. fue el Altair 8800 (1974) de la desaparecida empresa MITS. Microsoft tuvo el acierto de construir un intérprete BASIC para él, MITS sobrevivió un par de años, pero Microsoft inició un despegue imparable, dando un gran salto al facilitar a IBM el sistema operativo MS-DOS para la PC. En 1971 apareció el PET 2001 de Commodore, empresa absorbida por la holandesa Tulip, el TRS 80 de Radio Shack y el Apple II, fabricado en un garaje por dos jóvenes norteamericanos: Steven Jobs y Stephen Wozniak. A partir de 1980 se produce una eclosión de marcas. Destaca el Sinclair ZX80, precedente del ZX81 y del Spectrum, fabricante absorbido por Amstrad, que consiguió gran éxito vendiendo productos de muy baja calidad fabricados en Corea. Amstrad, como es lógico, abandonó la informática, aunque sigue con equipos musicales y antenas de televisión, de muy baja calidad. En Agosto de 1981 se presentó la IBM PC, que ha dado lugar una difusión masiva de la informática personal.

Computadora de Quinta Generación

En Octubre de 1981 el mundo de las computadoras se vio sacudido por el anuncio hecho en Japón, de una iniciativa de investigación y desarrollo orientada a producir una nueva generación de computadoras en la primera década de los años de los 90s, a las que se les dio el nombre de computadora de quinta generación.

Las computadoras de esta generación deben de ser capaces de resolver problemas muy complicados, algunos de los cuales requieren toda la experiencia, capacidad de razonamiento e inteligencia de las personas para ser resueltos. Deben de ser capaces de trabajar con grandes subconjuntos de los lenguajes naturales y estar asentados en grandes bases de conocimientos. A pesar de su complejidad la computadora de esta generación se están diseñando para ser manejados por personas no expertas en informática. Para conseguir estos fines tan ambiciosos estos equipos no tendrán un único procesador, sino un gran número agrupado en tres subsistemas fundamentales: un sistema inteligente, un mecanismo de inferencia y una interfaz de usuario inteligente.

Los avances se sitúan en materia de comunicaciones y una progresiva disminución de tamaño y costo del equipo, así como de técnicas de programación y desarrollo de Inteligencia Artificial y de control de procesos (robotización).

Actualmente no están desarrolladas plenamente estas computadoras, se trabaja en distintos países, cuyos programas de investigación más importantes son los siguientes:
EE.UU.: Proyectos DARPA y MCC
Unión Europea: Proyecto Sprit
Reino Unido: Proyecto Alvey

Japón: Proyecto ICOT

Según su propósito y su ámbito de uso esta clasificación se realiza en función del ámbito de aplicabilidad para el cual cada máquina concreta ha sido diseñada y comercializada.

Computadora de bolsillo: Verdadero sustituto, con tremenda ganancia de precisión, de la antigua regla de cálculo.
Computadora doméstica: Pensado para juegos, aprendizaje asistido por computadora de diversas materias, gestión de agendas, pequeñas contabilidades domésticas, entre otras.

Computadora profesional: Diseñado para satisfacer las necesidades de proceso de datos de una amplia gama de profesionales y también de pequeñas oficinas técnicas o empresas familiares.

Computadora departamental: Computadora con capacidad local para abordar con autosuficiencia la mayoría de necesidades del departamento, pero vinculado a un computadora de mayor potencia y capacidad de archivos para aquellos procesos que requieren una mayor potencia en el procesador.

Computadora central: Computadora central de la empresa a la cual recurren todos los usuarios de la empresa cuando la capacidad local es desbordada. Red de computadora: Conjunto de computadoras vinculadas entre sí para ofrecer un mismo tipo de servicio a todo un conjunto muy amplio de usuarios de forma repartida para evitar sobrecargas y evitar que la caída de una computadora única central represente la caída de todo el servicio.

Servidores: Pueden ser utilizados simultáneamente por muchos usuarios, en cálculos científicos o de simulación, su costo por lo general es de miles de millones de pesos y su velocidad es enorme.

Grandes servidores: Son equipos dedicados principalmente a la gestión, por lo que admiten gran cantidad de trabajos simultáneos, como por ejemplo controlar una red de terminales en las distintas sucursales de una empresa, o una red de cajeros automáticos de un Banco.
Son equipos en principio dedicados a tareas departamentales dentro de un organismo o empresa. Su capacidad principal es la de soportar gran cantidad de terminales, pues están orientados a la gestión. Dado su bajo precio en comparación con las grandes computadoras, están recogiendo cuota de mercado frente a ellos.

Transformación del Mundo con: Internet.
En 1969 los científicos de la Agencia de Investigaciones y Proyectos Avanzados (ARPA) del gobierno de los Estados Unidos, creó una red de computadoras denominada ARPANet.

La idea de esta red era facilitar el intercambio de información entre las agencias norteamericanas de defensa, en caso de una confrontación nuclear. Y ARPANet fue la respuesta a esta necesidad pues, a diferencia de otras redes de su época, podía funcionar a pesar de que la red experimentara fallas en algunos de sus equipos que la conformaban. Esto marcó el inicio de INTERNET.

El éxito de ARPANET fue tal que, rápidamente, muchas universidades y organizaciones quisieron participar en ella, hasta que el Gobierno Norteamericano decidió poner esta red bajo la administración de la Sociedad de Internet quien, desde entonces, es la responsable de marcar las líneas de desarrollo de esta red pública mundial de computadoras.

Un nuevo impulso a Internet lo dio la creación del estándar del Web por parte de los científicos de la CERN, una agencia de investigaciones de origen suizo, que creó el Web para facilitar las operaciones de intercambio de información entre su personal.

A partir de 1993, el World Wide Web ha sido el detonante principal del desarrollo de Internet en todo el mundo, pues ha llevado a nivel popular, el manejo de esta compleja red mundial. Y ha puesto la información en formato multimedia (texto, imágenes y sonido) al alcance de las manos de cualquier usuario.
Los servicios del Web, correo electrónico, transferencia de archivos, grupos de noticias, sociedades de intercambio, entre otros, han revolucionado la manera en que las empresas se administran y las sociedades conviven y lo más probable es que lo sigan haciendo aún más en el nuevo milenio.

Los productos y servicios del siglo XXI serán diseñados y construidos a partir de las necesidades específicas de cada cliente y no partiendo de necesidades generales a las cuáles uno, como consumidor, tendría que adaptarse.

La Tecnología de Información, principalmente representada por Internet, tendrá que ver mucho en este nuevo concepto de trabajo, en donde el individuo y sus características personales estarán privilegiados sobre lo demás.

En México, cada vez son más las empresas tradicionales que han efectuado cambios en la forma de llevar sus negocios y migran a la red digital. Esto no les implicó un giro en la producción de sus bienes y servicios, únicamente adecuaron sus estrategias de negocio. Según la consultora Select-IDC, 55% de las empresas mexicanas que decidieron incursionar en la economía digital ofrecen los mismos productos y servicios que antes, 33% cambiaron y 13% sólo utilizan internet para promocionarse.

Los actuales dispositivos informáticos y de telecomunicaciones manejan datos en forma digital empleando las mismas técnicas básicas. Estos datos pueden ser compartidos por muchos dispositivos y medios, procesarse en todos ellos y emplearse en una amplia gama de actividades de procesado de información.

En el mundo de los negocios actuales y futuros es indispensable mantener la completa armonía de la tecnología de información con los procesos de negocios que poseen las empresas. Esta es una de las formas y tal vez la más relevante, como las empresas pueden agregar valor a sus productos y servicios. La tecnología Cliente/Servidor aporta el eslabón para lograr éste alineamiento entre tecnología de información y negocios.
La tecnología de información se ha vuelto no sólo un instrumento de información sino una herramienta competitiva y una necesidad de supervivencia.

1.2 Necesidad de salvaguardar la información.

A partir de la década de 1950, con el surgimiento de las computadoras comerciales, estas han tenido cada vez mayor importancia en los procesos administrativos y productivos de las empresas en industrias; es decir, el progreso de la computación ha sido explosivo. Los sistemas de información son ahora componente básico de todos los negocios.

Una de las razones por las que la computación ha tenido tan exitosa irrupción en el mundo de los negocios ha sido que resulta de gran utilidad para el manejo de la información, en especial de grandes volúmenes de esta. Y ello cobra más importancia cuanto mayor es el valor de esta información para las empresas.

Un hecho que goza de aceptación generalizada en la actualidad, es que después del personal, la información es el recurso más importante para cualquier organización. Por otro lado, un objetivo de la administración es optimizar la utilización de los recursos, para obtener resultados que se reflejen en ventajas competitivas para la organización. Uniendo las dos premisas anteriores, llegamos a la conclusión de que la administración eficiente de la información en una empresa es determinante para el éxito de la misma.

Al hablar de administración de la información estamos incluyendo procesos como la obtención, organización, procesamiento, almacenamiento y entrega de los resultados en los tiempos y formas requeridos de forma continua. Esto nos lleva irreversiblemente a incluir aspectos relacionados con la seguridad de la información y la necesidad existente de salvaguardarla.

Es menester que la información esté disponible en cualquier momento; es decir, que exista la información y que existan los medios necesarios para tener acceso a ella. En otras palabras, hay que asegurar el uso de la información.

La computación es una herramienta fundamental para el manejo de información en las empresas de hoy; por lo tanto asegurar la información implica asegurar la disponibilidad en el uso del equipo de cómputo que la maneja, así como los medios que la contienen.

El no contar, por cualquier causa, con el equipo de cómputo, implica no poder utilizar la información, lo que equivale a no tenerla, es evidente que las consecuencias de esto son graves y las estadísticas así lo demuestran.

En promedio una compañía que registra una suspensión del servicio de cómputo que dura más de 10 días nunca se recuperará totalmente, 50% de ellas estarán fuera del negocio por 5 años (*Figura B* de la introducción). Las oportunidades de sobrevivir a un desastre que afecte al centro de procesamiento de datos son menos de 7 en 100.

La seguridad de la información tiene como meta proteger de cualquier pérdida los activos o recursos de las organizaciones de pérdida y asegurar la viabilidad de las operaciones de la organización si ésta llegara a ocurrir. William Stallings define seguridad de la información como "el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos".

Existen también otras causas de "accidentes" informáticos como son: errores del operador, errores o mal funcionamiento de hardware, errores en el software, errores en los datos, daños a las instalaciones, "performance" inadecuado del sistema, entre otros.

Otro factor que nos ayuda a dimensionar la necesidad de resguardar nuestra información es el de los Delitos informáticos:

La seguridad de la información también tiene como objetivo combatir lo que se ha dado en llamar "crimen por computadora" o "delitos informáticos". Los delitos informáticos pueden dirigirse al software, a los datos o al hardware.

La evolución tecnológica ha generado un importante número de conductas nocivas que aprovechando el poder de la información, buscan lucros ilegítimos y causan daños, sin olvidar los riesgos naturales e

impredecibles a los que hoy en día esta expuesta la información y en dado caso la continuidad de un negocio.

Es indudable que así como la computadora se presenta como una herramienta muy favorable para la sociedad, también se puede constituir en un verdadero instrumento de actos ilícitos. Este tipo de actitudes concebidas por el hombre encuentran sus orígenes desde el mismo surgimiento de la tecnología informática. La facilitación de las labores que traen consigo las computadoras, propician que en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de la computadora, cometiendo sin darse cuenta una serie de ilícitos.

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

> [1]*"Delito o crimen informático es toda interrupción, uso indebido, modificación, o fabricación de datos ajenos que se encuentren en sistemas de computación, sin autorización expresa o implícita de su dueño y/o de quien ostente la propiedad intelectual, con el objeto de obtener un provecho económico o no."*

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de la delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tienen estos tipos de delitos es

[1] Estrada Garavilla Miguel, "Delitos Informáticos", Ed. Universidad Abierta.

que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad. (Manual de la Naciones Unidas para la Prevención y Control del Delito)

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.
Si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias y de identificación de las personas. Y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado, o particulares; se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

La humanidad no esta frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

Según [2] Téllez Valdez, autor mexicano, los delitos informáticos presentan las siguientes características principales:

- *Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.*
- *Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.*
- *Son acciones de oportunidad ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.*
- *Provocan serias pérdidas económicas ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.*
- *Ofrecen posibilidades de tiempo y espacio ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.*
- *Son muchos los casos y pocas las denuncias y todo ello debido a la misma falta de regulación por parte del Derecho.*
- *Son muy sofisticados y relativamente frecuentes en el ámbito militar.*
- *Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.*
- *En su mayoría son imprudenciales y no necesariamente se cometen con intención.*
- *Ofrecen facilidades para su comisión a los menores de edad.*
- *Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.*

[2] El Derecho y la Sociedad de la Información: la importancia de internet en el mundo actual, en coautoría con Renato Jijena Leiva (Chile) y Julio Tellez Valdéz (México), Editorial Porrúa, México, 2003

Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios:

a) Conductas criminales, un medio o símbolo

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- *Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, entre otros.)*
- *Variación de los activos y pasivos en la situación contable de las empresas.*
- *Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, entre otros.)*
- *Lectura, sustracción o copiado de información confidencial.*
- *Modificación de datos tanto en la entrada como en la salida.*
- *Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.*
- *Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.*
- *Uso no autorizado de programas de cómputo.*
- *Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.*
- *Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.*
- *Obtención de información residual impresa en papel luego de la ejecución de trabajos.*
- *Acceso a áreas informatizadas en forma no autorizada.*
- *Intervención en las líneas de comunicación de datos o teleproceso.*

b) Conductas criminales, un fin

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- *Programación de instrucciones que producen un bloqueo total al sistema.*
- *Destrucción de programas por cualquier método.*
- *Daño a la memoria.*
- *Atentado físico contra la máquina o sus accesorios.*
- *Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.*
- *Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, entre otros)*

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- *Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.*
- *Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, entre otros.*
- *Infracción al Copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.*
- *Interceptación de E-mail: Lectura de un mensaje electrónico ajeno.*
- *Estafas electrónicas: A través de compras realizadas haciendo uso de la red.*
- *Transferencias de fondos: Engaños en la realización de este tipo de transacciones.*

Conductas criminales por Internet
Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Por lo anterior, consideramos prudente, incluir un apartado relacionado con la Legislación en México sobre Delitos Informáticos (ver Anexo I).

1.3 Seguridad de la Información

1.3.1 Seguridad física

La seguridad física de los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial. En otras palabras mecanismos, generalmente de prevención y detección destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de respaldo con toda la información que hay en el sistema, pasando por el propio CPU de la máquina.

Desgraciadamente, la seguridad física es un aspecto olvidado con demasiada frecuencia; en muchas organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio, pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan las impresiones del sistema. Esto motiva que en determinadas situaciones un atacante aproveche vulnerabilidades físicas en lugar de lógicas ya que posiblemente le sea más fácil robar una cinta con una imagen completa del sistema que intentar acceder a él mediante fallos en el software. Estamos conscientes de que la seguridad física es demasiado importante como para ignorarla: un ladrón que roba un ordenador para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones nos pueden hacer mucho más daño que un intruso que intenta conectar remotamente con una máquina no autorizada. No importa que utilicemos los más avanzados medios de cifrado para conectar a nuestros servidores, ni que hayamos definido una política de *firewalling* muy restrictiva: si no tenemos en cuenta factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada. Además, en el caso de organismos con requerimientos de seguridad medios, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas: como casi todos los atacantes de los equipos de estos entornos son casuales (esto es, no tienen interés específico sobre nuestros equipos, sino sobre cualquier equipo), si notan a través de medidas físicas que nuestra organización está

* Términos definidos en el glosario.

preocupada por la seguridad probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida.

No es nuestro objetivo centrarse en el diseño de edificios resistentes a un terremoto o en la instalación de alarmas electrónicas, si no comentar ciertas medidas de prevención y detección que se han de tener en cuenta a la hora de definir mecanismos y políticas para la seguridad de nuestros equipos. Debemos recordar que cada sitio es diferente y por tanto también lo son sus necesidades de seguridad; de esta forma, no se pueden dar recomendaciones específicas sino pautas generales a tener en cuenta, que pueden variar desde el simple sentido común (como es el cerrar con llave la sala de operaciones cuando salimos de ella) hasta medidas mucho más complejas, como la prevención de radiaciones electromagnéticas de los equipos o la utilización de *degaussers*. En entornos habituales suele ser suficiente con un poco de sentido común para conseguir una mínima seguridad física; de cualquier forma, en cada institución se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para que en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

Protección del hardware

El hardware es frecuentemente el elemento más caro de todo sistema informático. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la seguridad física de cualquier empresa con información tecnológica, especialmente en: universidades, centros de investigación e institutos tecnológicos suelen poseer entre sus equipos máquinas muy caras, desde servidores con una gran potencia de cálculo hasta *routers*[♦] de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica.

Son muchas las amenazas al hardware de una instalación informática; aquí se van a presentar algunas de ellas, sus posibles efectos y algunas soluciones, si no para evitar los problemas, sí al menos para minimizar sus efectos.

Acceso físico

La posibilidad de acceder físicamente a una máquina y en general, a cualquier sistema operativo hace inútiles casi todas las medidas de seguridad que hayamos aplicado sobre ella: hemos de pensar que si un atacante puede llegar con total libertad hasta una estación puede por ejemplo abrir la CPU y llevarse un disco duro; sin necesidad de privilegios en el sistema, sin importar la robustez de nuestros cortafuegos, sin ni siquiera una clave de usuario, el atacante podrá seguramente modificar la información almacenada, destruirla o simplemente leerla. Incluso sin llegar al extremo de desmontar la máquina, que quizás resulte algo exagerado en entornos clásicos donde hay cierta vigilancia, como un laboratorio o una sala de informática, la persona que accede al equipo puede pararlo o arrancar una versión diferente del sistema operativo sin llamar mucho la atención.

La seguridad física es necesaria para garantizar la seguridad global de la red y los sistemas conectados a ella; evidentemente el nivel de seguridad física depende completamente del entorno donde se ubiquen los puntos a proteger cualquier elemento físico que se pueda utilizar para amenazar la seguridad, como una toma de red apartada en cualquier rincón de un edificio de nuestra organización. Mientras que parte de los equipos estarán bien protegidos, por ejemplo los servidores de un departamento o las máquinas de los despachos, otros muchos estarán en lugares de acceso semipúblico, como laboratorios de prácticas; es justamente sobre estos últimos sobre los que

[♦] Términos definidos en el glosario.

debemos extremar las precauciones ya que lo más fácil y discreto para un atacante es acceder a uno de estos equipos y, en segundos, lanzar un ataque completo sobre la red.

Prevención

Para prevenir un acceso físico no autorizado a un determinado punto, hay soluciones para todos los gustos y también de todos los precios: desde analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta. Todos los modelos de autenticación de usuarios son aplicables, aparte para controlar el acceso lógico a los sistemas, para controlar el acceso físico; de todos ellos, quizás los más adecuados a la seguridad física sean los biométricos y los basados en algo poseído; aunque suelen resultar algo caros para utilizarlos masivamente en entornos de seguridad media.

Pero no hay que diseñar sistemas tan complejos para prevenir accesos físicos no autorizados; normas tan elementales como cerrar las puertas con llave al salir de un laboratorio o un despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados son en ocasiones más que suficientes para prevenir ataques. También basta el sentido común para darse cuenta de que el cableado de red es un elemento importante para la seguridad, por lo que es recomendable apartarlo del acceso directo; por desgracia, en muchas organizaciones podemos ver excelentes ejemplos de lo que no hay que hacer en este sentido: cualquiera que pasee por entornos más o menos amplios (el campus de una universidad, por ejemplo) seguramente podrá ver o cortar cables descolgados al alcance de todo el mundo, especialmente durante el verano, época que se suele aprovechar para hacer obras.

Todos hemos visto películas en las que se mostraba un estricto control de acceso a instalaciones militares mediante tarjetas inteligentes, analizadores de retina o verificadores de la geometría de la mano; aunque algunos de estos métodos aún suenen a ciencia ficción y sean demasiado caros para la mayor parte de entornos (recordemos que si el sistema de protección es más caro que lo que se quiere proteger tenemos un grave error en nuestros planes de seguridad), otros se pueden aplicar y se aplican, en muchas organizaciones.

Detección

Cuando la prevención es difícil por cualquier motivo (técnico, económico, humano) es deseable que un potencial ataque sea detectado cuanto antes, para minimizar así sus efectos. Aunque en la detección de problemas, generalmente accesos físicos no autorizados, intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas, en entornos más normales el esfuerzo en detectar estas amenazas se ha de centrar en las personas que utilizan los sistemas y en las que sin utilizarlos están relacionadas de cierta forma con ellos; sucede lo mismo que con la seguridad lógica: se ha de ver toda la protección como una cadena que falla si falla su eslabón más débil.

Es importante concientizar a todos de su papel en la política de seguridad del entorno; si por ejemplo un usuario autorizado detecta presencia de alguien de quien sospecha que no tiene autorización para estar en una determinada estancia debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario. No obstante, utilizar este servicio debe ser solamente un último recurso: generalmente en la mayoría de entornos no estamos tratando con terroristas, sino por fortuna con elementos mucho menos peligrosos. Si cada vez que se sospecha de alguien se avisa al servicio de seguridad esto puede repercutir en el ambiente de trabajo de los usuarios autorizados estableciendo cierta presión que no es en absoluto recomendable; un simple "¿puedo ayudarte en algo?" suele ser más efectivo que un guardia

solicitando una identificación formal. Esto es especialmente recomendable en lugares de acceso restringido, como laboratorios de investigación o centros de cálculo, donde los usuarios habituales suelen conocerse entre ellos y es fácil detectar personas ajenas al entorno.

Desastres naturales

En el anterior punto hemos hecho referencia a accesos físicos no autorizados a zonas o a elementos que pueden comprometer la seguridad de los equipos o de toda la red; sin embargo, no son estas las únicas amenazas relacionadas con la seguridad física. Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear graves consecuencias, es el derivado de los desastres naturales y su falta de prevención.

Terremotos

Los terremotos son desastres naturales más o menos probables según la ubicación geográfica en la que nos encontremos, pueden sin duda alcanzar magnitudes de diferente intensidad desde muy imperceptibles hasta catastróficos, pero sin duda todos con la intensidad necesarias para causar daños en los equipos e incluso a todas las instalaciones. Por tanto, se suelen tomar medidas serias contra los movimientos sísmicos, según los antecedentes de grado de severidad en la zona. Particularmente en nuestro país la probabilidad de que sucedan estos fenómenos merece la pena invertir dinero para minimizar sus efectos y consecuencias.

De cualquier forma, aunque algunas medidas contra terremotos son excesivamente caras para la mayor parte de organizaciones, no cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar nunca equipos delicados en superficies muy elevadas (aunque tampoco es bueno situarlos al ras de suelo, como veremos al hablar de inundaciones). Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo hardware, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente (y barato) utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los *routers*. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos ya que si lo que cae son esos objetos también dañarán el hardware.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas y en ese caso la pérdida de datos o hardware pierde importancia frente a los posibles accidentes (incluso mortales) que puede causar una pieza voluminosa a las personas a las que les cae encima.

Quizás al hablar de terremotos no debemos referirnos únicamente a los grandes desastres que derrumban edificios y destrozan vías de comunicación; quizás sería más apropiado hablar incluso de vibraciones, desde las más grandes (los terremotos) hasta las más pequeñas (un simple motor cercano a los equipos). Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con hardware más mecánico, como las impresoras: estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima de la CPU de una máquina es una idea nefasta.

Tormentas eléctricas

Las tormentas eléctricas, especialmente frecuentes en verano (cuando mucho personal se encuentra de vacaciones, lo que las hace más peligrosas) generan incrementos de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica, como veremos a continuación. Si cae un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos. Sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir hardware incluso protegido contra voltajes elevados.

Sin embargo, las tormentas poseen un lado positivo: son predecibles con más o menos exactitud, lo que permite a un administrador detener sus máquinas y desconectarlas. El problema recae en los responsables de los equipos: la caída de un rayo es algo poco probable, pero no imposible, en una gran ciudad donde existen artefactos destinados justamente a atraer rayos de una forma controlada; tanto es así que mucha gente ni siquiera ha visto caer cerca un rayo, por lo que directamente tiende a asumir que eso no le va a suceder nunca y menos a sus equipos. Por tanto, muy pocos administradores se molestan en parar máquinas y desconectarlas ante una tormenta; si el fenómeno sucede durante las horas de trabajo y la tormenta es fuerte, quizás sí que lo hace, pero si sucede un sábado por la noche nadie va a ir a la sala de operaciones a proteger a los equipos y nadie antes se habrá tomado la molestia de protegerlos por una simple previsión meteorológica.

Otra medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad; se han de almacenar lo más alejados posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el hardware la pérdida de toda la información de nuestros sistemas.

Inundaciones y humedad

Cierto grado de humedad es necesario para un correcto funcionamiento de nuestras máquinas: en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, en un daño irreparable al hardware y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina.

Controlar el nivel de humedad en los entornos habituales es algo innecesario ya que por norma nadie ubica estaciones en los lugares más húmedos o que presenten situaciones extremas; no obstante, ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de todos aquellos de los que tengamos dudas. Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o demasiada humedad, especialmente en sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

Cuando ya no se habla de una humedad más o menos elevada sino de completas inundaciones, los problemas generados son mucho mayores. Casi cualquier medio (una máquina, una cinta, un *router*) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos.

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención (frente a las de detección); podemos utilizar detectores de agua en los suelos o falsos suelos de las salas de operaciones y apagar automáticamente los sistemas en caso de que se activen. Tras apagar los sistemas podemos tener también instalado un sistema automático que corte la corriente: algo muy común es intentar sacar los equipos, previamente apagados o no de una sala que se está empezando a inundar; esto, que a primera vista parece lo lógico, es el mayor error que se puede cometer si no hemos desconectado completamente el sistema eléctrico ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar equipos. Por muy caro que sea el hardware o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a lo que supone la pérdida de vidas humanas. Otro error común relacionado con los detectores de agua es situar a los mismos a un nivel superior que a los propios equipos a salvaguardar (incluso en el techo, junto a los detectores de humo); evidentemente, cuando en estos casos el agua llega al detector poco se puede hacer ya por las máquinas o la información que contienen.

Medidas de protección menos sofisticadas pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones.

Desastres del entorno

Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

El problema menos común en las instalaciones modernas son las altas de tensión, conocidas como "picos" porque generalmente duran muy poco: durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al hardware o a los datos gracias a que en la mayoría de equipos hay instalados fusibles, elementos que se funden ante una alta de tensión y dejan de conducir la corriente, provocando que la máquina permanezca apagada. Disponga o no de fusibles el equipo a proteger (lo normal es que sí los tenga) una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo de una sala o edificio, o simplemente hacia cualquier lugar con voltaje nulo. Una toma de tierra sencilla puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se introduce lo más posible en el suelo.

Incluso teniendo un sistema protegido con los métodos anteriores, si las altas y bajas en la tensión duran demasiado, o si son demasiado rápidas, podemos sufrir daños en los equipos; existen reguladores de tensión comerciales que protegen de los picos hasta en los casos más extremos y que también se utilizan como filtros para ruido eléctrico. Aunque en la mayoría de situaciones no es necesario su uso, si nuestra organización tiene problemas por el voltaje excesivo quizás sea conveniente instalar alguno de estos aparatos.

Otro problema, mucho más habitual, son los cortes en el fluido eléctrico que llega a nuestros equipos. Aunque un simple corte de corriente no suele afectar al hardware, lo más peligroso (y que sucede en muchas ocasiones) son las idas y venidas intempestivas de la corriente; en esta situación, aparte de perder datos, nuestras máquinas pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar un SAI (Servicio de Alimentación Ininterrumpido) conectada al elemento que queremos proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable, protegiendo así los equipos de altas, cortes y bajas de tensión; tienen capacidad para seguir alimentando las máquinas incluso en caso de que no reciban electricidad (evidentemente no las alimentan de forma indefinida, sino durante un cierto tiempo, el necesario para detener el sistema de forma ordenada).

Un último problema contra el que ni siquiera los SAI nos protegen, es la corriente estática, un fenómeno extraño del que la mayoría de la gente piensa que no afecta a los equipos, sólo a otras personas. Nada más lejos de la realidad: simplemente tocar con la mano la parte metálica de teclado o un conductor de una placa puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño, sólo un pequeño calambrazo, el ordenador sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM.

Ruido eléctrico

El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otros ordenadores o por multitud de aparatos, especialmente muchos de los instalados en los laboratorios de organizaciones y se transmite a través del espacio o de líneas eléctricas cercanas a nuestra instalación.

Para prevenir los problemas que el ruido eléctrico puede causar en nuestros equipos lo más barato es intentar no situar hardware cercano a la maquinaria que puede causar dicho ruido; si no tenemos más remedio que hacerlo, podemos instalar filtros en las líneas de alimentación que llegan hasta los ordenadores. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o *walkie-talkies (Sistema de intercomunicación de corto alcance)*; estos elementos puede incluso dañar permanentemente a nuestro hardware si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

Incendios y humo

Una causa casi siempre relacionada con la electricidad son los incendios y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple corto circuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el hardware no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero sí que quedara destrozado por el agua expulsada. Con

este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón; este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas: por un lado, resulta excesivamente contaminante para la atmósfera y por otro puede asfixiar a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un silbido.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos. Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor, pero hemos de recordar que puede existir humo sin necesidad de que haya un fuego: por ejemplo, en salas de operaciones donde se fuma. Aunque muchos no apliquemos esta regla y fumemos demasiado, siempre es demasiado delante de nuestros equipos, sería conveniente no permitir esto; aparte de la suciedad generada que se deposita en todas las partes de un ordenador, desde el teclado hasta el monitor, generalmente todos tenemos el cenicero cerca de los equipos, por lo que el humo afecta directamente a todos los componentes; incluso al ser algo más habitual que un incendio, se puede considerar más perjudicial para los equipos y las personas, el humo del tabaco que el de un fuego.

En muchos manuales de seguridad se insta a los usuarios, administradores, o al personal en general a intentar controlar el fuego y salvar el equipamiento; esto tiene, como casi todo, sus pros y sus contras. Evidentemente, algo lógico cuando estamos ante un incendio de pequeñas dimensiones es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente. Sin embargo, cuando las dimensiones de las llamas son considerables lo último que debemos hacer es intentar controlar el fuego nosotros mismos, arriesgando vidas para salvar hardware; como sucedía en el caso de inundaciones, no importa el precio de nuestros equipos o el valor de nuestra información: nunca serán tan importantes como una vida humana. Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar su control en manos de personal especializado.

Temperaturas extremas

No hace falta ser un genio para comprender que las temperaturas extremas ya sea un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos operen entre 10 y 32 grados Celsius, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de los sistemas.

Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un acondicionador de aire, aparato que también influirá positivamente en el rendimiento de los usuarios (las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente). Otra condición básica para el correcto funcionamiento de cualquier equipo que éste correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU. La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

Protección de los datos

La seguridad física también implica una protección a la información de nuestro sistema, tanto a la que está almacenada en él como a la que se transmite entre diferentes equipos. Aunque los apartados comentados en la anterior sección son aplicables a la protección física de los datos (ya que no olvidemos que si protegemos el hardware también protegemos la información que se almacena o se transmite por él), hay ciertos aspectos a tener en cuenta a la hora de diseñar una política de seguridad física que afectan principalmente, aparte de a los elementos físicos, a los datos de nuestra organización; existen ataques cuyo objetivo no es destruir el medio físico de nuestro sistema, sino simplemente conseguir la información almacenada en dicho medio.

Eavesdropping ♦

La interceptación, también conocida por ♦*passive wiretapping* es un proceso mediante el cual un agente capta información en claro o cifrada que no le iba dirigida; esta captación puede realizarse por muchísimos medios (por ejemplo, capturando las radiaciones electromagnéticas). Aunque es en principio un ataque completamente pasivo, lo más peligroso del eavesdropping es que es muy difícil de detectar mientras se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo.

Un medio de interceptación bastante habitual es el *sniffing*♦, consistente en capturar tramas que circulan por la red mediante un programa ejecutándose en una máquina conectada a ella o bien mediante un dispositivo que se engancha directamente al cableado. Estos dispositivos denominados *sniffers*♦, se conectan en paralelo con el cable de forma que la impedancia total del cable y el aparato es similar a la del cable solo, lo que hace difícil su detección. Contra estos ataques existen diversas soluciones; la más barata a nivel físico es no permitir la existencia de segmentos de red de fácil acceso, lugares idóneos para que un atacante conecte uno de estos aparatos y capture todo nuestro tráfico. No obstante esto resulta difícil en redes ya instaladas, donde no podemos modificar su arquitectura; en estos existe una solución generalmente gratuita pero que no tiene mucho que ver con el nivel físico: el uso de aplicaciones de cifrado para realizar las comunicaciones o el almacenamiento de la información (hablaremos más adelante de algunas de ellas). Tampoco debemos descuidar la toma de redes libres, donde un intruso con un portátil puede conectarse para capturar tráfico; es recomendable analizar regularmente nuestra red para verificar que todas las máquinas activas estén autorizadas.

Como soluciones igualmente efectivas contra la interceptación a nivel físico podemos citar el uso de dispositivos de cifra (no simples programas, sino hardware), generalmente chips que implementan algoritmos como DES; esta solución es muy poco utilizada en entornos ya que es muchísimo más cara que utilizar implementaciones software de tales algoritmos y en muchas ocasiones la única diferencia entre los programas y los dispositivos de cifra es la velocidad. También se puede utilizar como solución más cara, el cableado en vacío para evitar la interceptación de datos que viajan por la red: la idea es situar los cables en tubos donde artificialmente se crea el vacío o se inyecta aire a presión; si un atacante intenta pinchar el cable para interceptar los datos, rompe el vacío o el nivel de presión y el ataque es detectado inmediatamente. Como decimos, esta solución es enormemente cara y solamente se aplica en redes de perímetro reducido para entornos de alta seguridad.

♦ Términos definidos en el glosario.

Antes de finalizar este punto debemos recordar un peligro que muchas veces se ignora: el de la interceptación de datos emitidos en forma de sonido o simple ruido en nuestro entorno de operaciones. Imaginemos una situación en la que los responsables de la seguridad de nuestra organización se reúnen para discutir nuevos mecanismos de protección; todo lo que en esa reunión se diga puede ser capturado por multitud de métodos, algunos de los cuales son tan simples que ni siquiera se contemplan en los planes de seguridad. Por ejemplo, una simple tarjeta de sonido instalada en un PC situado en la sala de reuniones puede transmitir a un atacante todo lo que se diga en esa reunión; mucho más simple y sencillo: un teléfono mal colgado intencional o inintencionadamente, también puede transmitir información muy útil para un potencial enemigo. Para evitar estos problemas existen numerosos métodos: por ejemplo, en el caso de los teléfonos fijos suele ser suficiente un poco de atención y sentido común ya que basta con comprobar que están bien colgados o incluso desconectados de la red telefónica. El caso de los móviles suele ser algo más complejo de controlar ya que su pequeño tamaño permite camuflarlos fácilmente; no obstante, podemos instalar en la sala de reuniones un sistema de aislamiento para bloquear el uso de estos teléfonos: se trata de sistemas que ya se utilizan en ciertos entornos (por ejemplo en conciertos musicales) para evitar las molestias de un móvil sonando y que trabajan bloqueando cualquier transmisión en los rangos de frecuencias en los que trabajan los diferentes operadores telefónicos.

Backups (Respaldos)

En este apartado vamos a tratar la protección física de la información almacenada en respaldos, esto es, de la protección de los diferentes medios donde residen nuestras copias de seguridad. Hemos de tener siempre presente que si las copias contienen toda nuestra información tenemos que protegerlas igual que protegemos nuestros sistemas.

Un error muy habitual es almacenar los dispositivos de backup en lugares muy cercanos a la sala de operaciones, cuando no en la misma sala; esto, que en principio puede parecer correcto (y cómodo si necesitamos restaurar unos archivos) puede convertirse en un problema: imaginemos simplemente que se produce un incendio de grandes dimensiones y todo el edificio queda reducido a cenizas. En este caso extremo tendremos que unir al problema de perder todos nuestros equipos que seguramente cubrirá el seguro, por lo que no se puede considerar una catástrofe, el perder también todos nuestros datos, tanto los almacenados en los discos como los guardados en backups (esto evidentemente no hay seguro que lo cubra). Como podemos ver, resulta recomendable guardar las copias de seguridad en una zona alejada de la sala de operaciones, aunque en este caso descentralicemos la seguridad y tengamos que proteger el lugar donde almacenamos los backups igual que protegemos la propia sala o los equipos situados en ella, algo que en ocasiones puede resultar caro.

También suele ser común etiquetar las cintas donde hacemos copias de seguridad con abundante información sobre su contenido; esto tiene una parte positiva y una negativa; la positiva es que para un administrador es fácil encontrar el backup deseado y la negativa es que para un intruso es fácil conseguir el acceso a la información que desea.

Otros elementos

En muchas ocasiones los responsables de seguridad de los sistemas tienen muy presente que la información a proteger se encuentra en los equipos, en las copias de seguridad o circulando por la red, pero olvidan que esa información también puede encontrarse en lugares menos obvios, como listados de impresora, facturas telefónicas o la propia documentación de una máquina.

Evidentemente, hay que tomar medidas contra estos problemas. En primer lugar, las impresoras, *plotters, faxes, teletipos*, o cualquier dispositivo por el que pueda salir información de nuestro sistema ha de estar situado en un lugar de acceso restringido; también es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos. Sería conveniente que un usuario que recoge una copia se acredite como alguien autorizado a hacerlo, aunque quizás esto puede ser imposible, o al menos muy difícil, en grandes sistemas (imaginemos que en una máquina con cinco mil usuarios obligamos a todo aquél que va a recoger una impresión a identificarse y comprobamos que la identificación es correcta antes de darle su documento con toda seguridad necesitaríamos una persona encargada exclusivamente de este trabajo), siempre es conveniente demostrar cierto grado de interés por el destino de lo que sale por nuestra impresora: sin llegar a realizar un control férreo, si un atacante sabe que el acceso a los documentos este mínimo control se pensará dos veces antes de intentar conseguir algo que otro usuario ha impreso.

Elementos que también pueden ser aprovechados por un atacante para comprometer nuestra seguridad son todos aquellos que revelen información de nuestros sistemas o del personal que los utiliza, como ciertos manuales (proporcionan versiones de los sistemas operativos utilizados), facturas de teléfono del centro (pueden indicar los números de nuestros módems) o agendas de operadores (revelan los teléfonos de varios usuarios, algo muy provechoso para alguien que intente efectuar ingeniería social contra ellos). Aunque es conveniente no destruir ni dejar a la vista de todo el mundo esta información, si queremos eliminarla no podemos limitarnos a arrojar documentos a la papelera: en el capítulo siguiente hablaremos del basureo, algo que aunque parezca sacado de películas de espías realmente se utiliza contra todo tipo de entornos. Es recomendable utilizar una trituradora de papel, dispositivo que dificulta mucho la reconstrucción y lectura de un documento destruido; por poco dinero podemos conseguir uno de estos aparatos, que suele ser suficiente para acabar con cantidades moderadas de papel.

Radiaciones electromagnéticas

Podíamos haber hablado del acceso no autorizado a los datos a través de las radiaciones que el hardware emite; sin embargo, este es un tema que ha cobrado especial importancia (especialmente en organismos militares) a raíz del programa TEMPEST, un término (Transient ElectroMagnetic Pulse Emanation Standard) que identifica una serie de estándares del gobierno estadounidense para limitar las radiaciones eléctricas y electromagnéticas del equipamiento electrónico, desde estaciones de trabajo hasta cables de red, pasando por terminales, *mainframes*♦, ratones.

La idea es sencilla: la corriente que circula por un conductor provoca un campo electromagnético alrededor del conductor, campo que varía de la misma forma que lo hace la intensidad de la corriente. Si situamos otro conductor en ese campo, sobre él se induce una señal que también varía proporcionalmente a la intensidad de la corriente inicial; de esta forma, cualquier dispositivo electrónico (no sólo el informático) emite continuamente radiaciones a través del aire o de conductores, radiaciones que con el equipo adecuado se pueden captar y reproducir remotamente con la consiguiente amenaza a la seguridad que esto implica. Conscientes de este problema obviamente las emisiones de una batidora no son peligrosas para la seguridad, pero sí que lo pueden ser las de un dispositivo de cifrado o las de un teclado desde el que se envíen mensajes confidenciales. En la década de los 50 el gobierno de Estados Unidos introdujo una serie de estándares para reducir estas radiaciones en los equipos destinados a almacenar, procesar o transmitir información que pudiera

♦ Término definido en el glosario.

comprometer la seguridad nacional. De esta forma, el hardware certificado TEMPEST se suele usar con la información clasificada y confidencial de algunos sistemas gubernamentales para asegurar que el *eavesdropping* electromagnético no va a afectar a privacidad de los datos.

Casi medio siglo después de las primeras investigaciones sobre emanaciones de este tipo, casi todos los países desarrollados y organizaciones militares internacionales tienen programas similares a TEMPEST con el mismo fin: proteger información confidencial. Para los gobiernos, esto es algo reservado a informaciones militares, nunca a organizaciones normales y mucho menos a particulares (la NRO, National Reconnaissance Office, eliminó en 1992 los estándares TEMPEST para dispositivos de uso doméstico); sin embargo y como ejemplo algo extremo quizás de hasta que punto un potencial atacante puede llegar a comprometer la información que circula por una red o que se lee en un monitor, vamos a dar aquí unas nociones generales sobre el problema de las radiaciones electromagnéticas.

Existen numerosos tipos de señales electromagnéticas; sin duda las más peligrosas son las de video y las de transmisión serie ya que por sus características no es difícil interceptarlas con el equipamiento adecuado. Otras señales que también son fáciles de captar son las de enlaces por radiofrecuencia o las de redes basadas en infrarrojos: no presentan tantos problemas ya que desde un principio los diseñadores fueron conscientes de la facilidad de captación y las amenazas a la seguridad que una captura implica; esta inseguridad tan palpable provocó la rápida aparición de mecanismos implementados para dificultar el trabajo de un atacante, como el salto en frecuencias o el espectro disperso, o simplemente el uso de protocolos cifrados. Este tipo de emisiones quedan fuera del alcance de TEMPEST, pero son cubiertas por otro estándar denominado NONSTOP, también del Departamento de Defensa estadounidense.

Sin embargo, nadie suele tomar precauciones contra la radiación que emite su monitor, su impresora o el cable de su módem. Y son justamente las radiaciones de este hardware desprotegido las más preocupantes en ciertos entornos ya que lo único que un atacante necesita para recuperarlas es el equipo adecuado. Dicho equipo puede variar desde esquemas extremadamente simples y baratos, pero efectivos, hasta complejos sistemas que en teoría utilizan los servicios de inteligencia de algunos países.

Para protegernos contra el *eavesdropping* de las radiaciones electromagnéticas de nuestro hardware, existe un amplio abanico de soluciones, desde simples medidas de prevención hasta complejos y caros sistemas para apantallar los equipos. La solución más barata y simple que podemos aplicar es la distancia: las señales que se transmiten por el espacio son atenuadas conforme aumenta la separación de la fuente, por lo que si definimos un perímetro físico de seguridad lo suficientemente grande alrededor de una máquina, será difícil para un atacante interceptar desde lejos nuestras emisiones. No obstante, esto no es aplicable a las señales inducidas a través de conductores, que aunque también se atenúan por la resistencia e inductancia del cableado, la pérdida no es la suficiente para considerar seguro el sistema.

Otra solución consiste en la confusión: cuantas más señales existan en el mismo medio, más difícil será para un atacante filtrar lo que está buscando; aunque esta medida no hace imposible la interceptación, sí la dificulta enormemente. Esto se puede conseguir simplemente manteniendo diversas piezas emisoras (monitores, terminales, cables.) cercanas entre sí y emitiendo cada una de ellas información diferente (si todas emiten la misma, facilitamos el ataque ya que aumentamos la intensidad de la señal inducida). También existe hardware diseñado explícitamente para crear ruido

electromagnético, generalmente a través de señales de radio que enmascaran las radiaciones emitidas por el equipo a proteger; dependiendo de las frecuencias utilizadas, quizás el uso de tales dispositivos pueda ser ilegal: en todos los países el espectro electromagnético está dividido en bandas, cada una de las cuales se asigna a un determinado uso y en muchas de ellas se necesita una licencia especial para poder transmitir.

La solución más efectiva y más cara, consiste en el uso de dispositivos certificados que aseguran mínima emisión, así como de instalaciones que absorben las radiaciones. En el hardware hay dos aproximaciones principales para prevenir las emisiones: una es la utilización de circuitos especiales que apenas emiten radiación (denominados de fuente eliminada) y la otra es la contención de las radiaciones, por ejemplo aumentando la atenuación; generalmente ambas aproximaciones se aplican conjuntamente. En cuanto a las instalaciones utilizadas para prevenir el *eavesdropping,* la idea general es aplicar la contención no sólo a ciertos dispositivos, sino a un edificio o a una sala completa. Quizás la solución más utilizada son las jaulas de *Faraday* sobre lugares donde se trabaja con información sensible; se trata de separar el espacio en dos zonas electromagnéticamente aisladas (por ejemplo, una sala y el resto del espacio) de forma que fuera de una zona no se puedan captar las emisiones que se producen en su interior. Para implementar esta solución se utilizan materiales especiales, como algunas clases de cristal, o simplemente un recubrimiento conductor conectado a tierra.

Antes de finalizar este punto quizá es recomendable volver a insistir en que todos los problemas y soluciones derivados de las radiaciones electromagnéticas no son aplicables a los entornos o empresas normales, sino que están pensados para lugares donde se trabaja con información altamente confidencial, como ciertas empresas u organismos militares o de inteligencia. Aquí simplemente se han presentado como una introducción para mostrar hasta donde puede llegar la preocupación por la seguridad en esos lugares. La radiación electromagnética no es un riesgo importante en la mayoría de organizaciones ya que suele tratarse de un ataque costoso en tiempo y dinero, de forma que un atacante suele tener muchas otras puertas para intentar comprometer el sistema de una forma más fácil.

1.3.2 Seguridad Lógica

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información y por lo tanto deben existir técnicas, mas allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica

Es decir que la Seguridad Lógica consiste en la *aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. Ver aspectos relevantes de la seguridad lógica. (Anexo II)*

Controles de acceso

Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas: para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el *National Institute for Standars and Technology (NIST)* ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

Identificación y Autentificación
Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, entre otros.
2. Algo que la persona posee: por ejemplo una tarjeta magnética.
3. Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas, se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por su difícil implementación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, para acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina *"single log-in"* o sincronización de *passwords.*

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

Proceso de solicitud establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.

Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.

Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoria o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.

Detección de actividades no autorizadas, además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.
Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularan de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Roles
El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador, líder de

proyecto, gerente de un área usuaria, administrador del sistema, entre otros. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

Transacciones
También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

Limitaciones a los servicios
Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema del sistema .Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de acceso
Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:
Lectura: El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
Escritura: Este tipo de acceso permite agregar datos, modificar o borrar información.
Ejecución: Este acceso otorga al usuario el privilegio de ejecutar programas.
Borrado: Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

Creación: Permite al usuario crear nuevos archivos, registros o campos.
Búsqueda: Permite listar los archivos de un directorio determinado.

Ubicación y horario
El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

Control de acceso interno
<u>Palabras claves (passwords)</u>
Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varías palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Consideramos de gran importancia asumir la idea útil de usar passwords seguros ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

Sincronización de passwords: Consiste en permitir que un usuario acceda con el mismo password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar un solo password para todos los sitios a los que tengan acceso y que si se les fuerza a elegir diferentes passwords tienden a guardarlos escritos para no olvidarlos, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

Caducidad y control: este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios y se define como el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, en un período máximo que puede transcurrir para que éstos caduquen.

Encriptación
La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

Listas de control de accesos
Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

Límites sobre la interfase de usuario
Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones especificas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas especificas.

Etiquetas de seguridad
Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, entre otros. Estas etiquetas no son modificables.

Control de acceso externo
Dispositivos de control de puertos
Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

Acceso de personal contratado o consultores
Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso

Accesos públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

Administración

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requieren diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa especifico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituirse un compromiso vacío, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.

Administración del personal y usuarios

Organización del Personal
Este proceso lleva generalmente cuatro pasos:
Definición de puestos: Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.

Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial

Elección de la persona para cada puesto: Requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.

Entretenimiento inicial y continuo del empleado: Cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tares que se le asignen, debe comunicársele, las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto a la seguridad pueden asumir su responsabilidad individual, para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: El personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

Niveles de seguridad informática
El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book10, desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C I y el D.

Nivel D
Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad, sin sistemas no confiables, no hay protección para

el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

Nivel C1: Protección Discrecional
Se requiere identificación de usuarios que permite el acceso a distinta información.
Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de administración del sistema sólo pueden ser realizadas por este "super usuario", quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:
Acceso de control discrecional: Distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
Identificación y Autentificación: Se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

Nivel C2: Protección De Acceso Controlado
Este subnivel fue diseñado para solucionar las debilidades del Cl, cuenta con características adicionales que crean un ambiente de acceso controlado, se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos, además tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos permitidos o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.
Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejores cuentas de las tareas relacionadas con la administración del sistema ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Nivel Bi: Seguridad Etiquetada
Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultra secreta, se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema (usuario, dato, entre otros.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, entre otros.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

Nivel B2: Protección Estructurada
Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

Nivel B3: Dominios de Seguridad
Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Nivel A: Protección Verificada
Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.3.3 Seguridad en Redes

La definición más general de una red de área local (Local Area Network, LAN), es la de una red de comunicaciones utilizada por una sola organización a través de una distancia limitada, la cual permite a los usuarios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, entre otros.

Elementos de una red
Una red de computadoras consta tanto de hardware como de software. En el hardware se incluyen: estaciones de trabajo, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad. En el software se encuentra el sistema operativo de red (Network Operating System, NOS).

Estaciones de trabajo
Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red, con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otras computadoras, esta puede ser desde una PC XT hasta una Pentium, equipada según las necesidades del usuario; o también de otra arquitectura diferente como Macintosh, Silicon Graphics, Sun, entre otros.

Servidores
Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales. Los tipos de servidores obtienen el nombre dependiendo del recurso que comparten. Algunos de ellos son: servidor de discos, servidor de archivos, servidor de archivos distribuido, servidores de archivos dedicados y no dedicados, servidor de terminales, servidor de impresoras, servidor de discos compactos, servidor web y servidor de correo.

Tarjeta de Interfaz de Red
Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC). Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo. Las tarjetas internas casi siempre se utilizan para las PC's, PS/2 y estaciones de trabajo como las SUN's. Las tarjetas de interfaz también pueden utilizarse en minicomputadoras y mainframes. A menudo se usan cajas externas para Mac's y para algunas computadoras portátiles. La tarjeta de interfaz obtiene la información de la PC, la convierte al formato adecuado y la envía a través del cable a otra tarjeta de interfaz de la red local, esta tarjeta recibe la información, la traduce para que la PC pueda entender y la envía a la PC.

Son ocho las funciones de la NIC:

- Comunicaciones de host a tarjeta
- Buffering
- Formación de paquetes
- Conversión serial a paralelo
- Codificación y decodificación
- Acceso al cable
- Saludo
- Transmisión y recepción

Estos pasos hacen que los datos de la memoria de una computadora pasen a la memoria de otra.

Cableado
La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos. Si sólo hubiera un tipo de cableado disponible, la decisión sería sencilla. Lo cierto es que hay muchos tipos de cableado, cada uno con sus propios defensores y como existe una gran variedad en cuanto al costo y capacidad, la selección no debe ser un asunto trivial.
Cable de par trenzado: Es con mucho, el tipo menos caro y más común de medio de red.

Cable coaxial: Es tan fácil de instalar y mantener como el cable de par trenzado y es el medio que se prefiere para las LAN grandes.
Cable de fibra óptica: Tiene mayor velocidad de transmisión que los anteriores, es inmune a la interferencia de frecuencias de radio y capaz de enviar señales a distancias considerables sin perder su fuerza. Tiene un costo mayor.

Equipo de conectividad en redes
Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada.

Hubs o concentradores: Son un punto central de conexión para nodos de red que están dispuestos de acuerdo a una topología física de estrella.

Repetidores: Un repetidor es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal de red.

Puentes: Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN.

Ruteadores: Los ruteadores son similares a los puentes, sólo que operan a un nivel diferente. Requieren por lo general que cada red tenga el mismo sistema operativo de red, para poder conectar redes basadas en topologías lógicas completamente diferentes como Ethernet y Token Ring.

Compuertas: Una compuerta permite que los nodos de una red se comuniquen con tipos diferentes de red o con otros dispositivos.

Sistema operativo de red
Después de cumplir todos los requerimientos de hardware para instalar una LAN, se necesita instalar un sistema operativo de red (Network Operating System, NOS), que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades.

Los servicios que el NOS realiza son:
Soporte para archivos: Esto es, crear, compartir, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.
Comunicaciones: Se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico, o imprime.
Servicios para el soporte de equipo: Aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, entre otros.

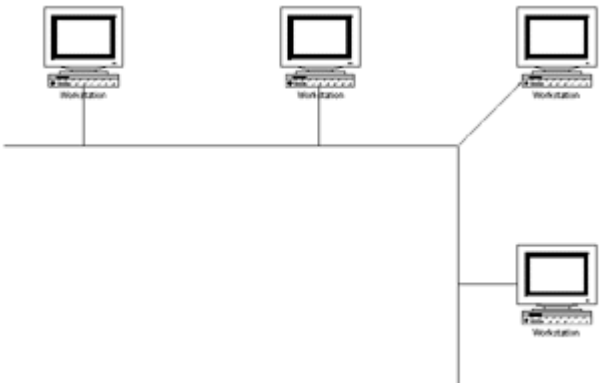
Topología de redes
Los nodos de red (las computadoras), necesitan estar conectados para comunicarse, a la forma en que están conectados los nodos se le llama topología. Una red tiene dos diferentes topologías: una física y una lógica. La topología física es la disposición física actual de la red, la manera en que los nodos están conectados unos con otros. La topología lógica es el método que se usa para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los diferentes nodos de la misma.

Las topologías físicas y lógicas pueden ser iguales o diferentes. Las topologías de red más comunes son: bus, anillo y estrella.

Red en Bus

En una topología de bus (ver Figura 1.1), cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir, un cable largo que va de un extremo a otro de la red y al cual se conecta cada nodo de la misma. El cable puede ir por el piso, por las paredes, por el techo, o puede ser una combinación de éstos, siempre y cuando el cable sea un segmento continuo.

Figura 1.1



Red en anillo

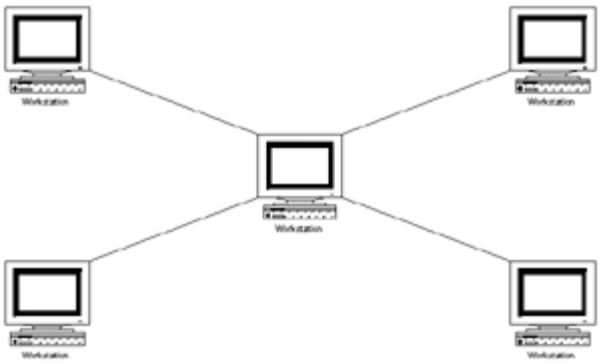
Una topología de anillo bus (ver Figura 1.2) consta de varios nodos unidos formando un círculo lógico. Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional, no obstante, sólo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como flecha o contraseña de paso.

Figura 1.2

Red en estrella

Uno de los tipos más antiguos de topologías de redes es la estrella (ver Figura 1.3), la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico ya que todos los mensajes de una topología LAN en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos.

Figura 1.3



Arquitectura de redes

Las redes están compuestas por muchos componentes diferentes que deben trabajar juntos para crear una red funcional. Los componentes que comprenden las partes de hardware de la red incluyen tarjetas adaptadoras de red, cables, conectores, concentradores y hasta la computadora misma. Los componentes de red los fabrican, por lo general, varias compañías. Por lo tanto, es necesario que haya entendimiento y comunicación entre los fabricantes, en relación con la manera en que cada componente trabaja e interactúa con los demás componentes de la red. Afortunadamente, se han creado estándares que definen la forma de conectar componentes de hardware en las redes y el protocolo (o reglas) de uso cuando se establecen comunicaciones por red. Los tres estándares o arquitecturas más populares son: ARCnet, Ethernet y Token Ring. Ethernet y Token Ring son estándares respaldados por el organismo IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), mientras que ARCnet es un estándar de la industria que ha llegado a ser recientemente uno de los estándares del ANSI (Instituto Nacional de Estándares Americanos).

Redes ARCnet

Producida en los años setenta por *Datapoint Corporation*, la red de cómputo de recursos conectados (ARCnet) es un estándar aceptado por la industria, aunque no lleva un número estándar de IEEE. ANSI reconoció a ARCnet como estándar formal, lo que la hizo parte de su estándar de LAN ANSI 878.1. Como soporta una velocidad de transferencia de datos de 2.5 Mbps, ARCnet usa una topología lógica de bus y una ligera variación de la topología física de estrella. Cada nodo de la red está conectado a un concentrador pasivo o a uno activo. La NIC en cada computadora está conectada a un cable que a su vez está conectado a un concentrador activo o pasivo. ARCnet se basa en un esquema de paso de señal (token passing) para administrar el flujo de datos entre los nodos de la red. Cuando un nodo está en posesión del token (señal), puede transmitir datos por la red. Todos los nodos, a excepción del receptor pretendido, pasan por alto los datos. Conforme se pasa el token a cada nodo, el nodo puede enviar datos. Ya que cada nodo sólo puede enviar datos cuando tiene el token, en ARCnet no suceden las colisiones que suelen darse en un esquema como el de CSMA/CD. Por lo tanto, ARCnet es menos susceptible a la saturación de la red que Ethernet. Durante algún tiempo ARCnet fue el estándar para LAN más popular; pero por causa en parte a su relativa baja velocidad (2.5 Mbps comparados con los 10 Mbps de Ethernet), casi no se usa para instalaciones nuevas.

Redes Ethernet

Ethernet, al que también se conoce como IEEE 802.3, es el estándar más popular para las LAN que se usa actualmente. Emplea una topología lógica de bus y una topología física de estrella o de bus. Ethernet transmite datos a través de la red a una velocidad de 10 Mbps. Ethernet usa un método de

transmisión de datos conocido como Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD). Antes de que un nodo envíe algún dato a través de una red Ethernet, primero escucha y se da cuenta si algún otro nodo está transfiriendo información. De no ser así, el nodo transferirá la información a través de la red. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información. En caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío. La topología lógica de bus de Ethernet permite que cada nodo tome su turno en la transmisión de información a través de la red. Así, la falla de un solo nodo no hace que falle la red completa. Aunque CSMA/CD es una forma rápida y eficiente para transmitir datos, una red muy cargada podría llegar al punto de saturación. Sin embargo, con una red diseñada adecuadamente, la saturación rara vez es preocupante. Existen tres estándares de Ethernet, 10BASE5, 10BASE2 y 10BASE-T, que definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar nodos en la red.

Redes Token Ring

Token Ring, también llamado IEEE 802.5, fue ideado por IBM y algunos otros fabricantes. Con operación a una velocidad de 4 Mbps o 16 Mbps, Token Ring emplea una topología lógica de anillo y una topología física de estrella. La NIC de cada computadora se conecta a un cable que, a su vez, se enchufa a un *hub* central llamado unidad de acceso a multiestaciones (MAU). Token Ring se basa en un esquema de paso de señales (token passing), es decir que pasa un token (o señal) a todas las computadoras de la red. La computadora que esté en posesión del token tiene autorización para transmitir su información a otra computadora de la red. Cuando termina, el token pasa a la siguiente computadora del anillo. Si la siguiente computadora tiene que enviar información, acepta el token y procede a enviarla. En caso contrario, el token pasa a la siguiente computadora del anillo y el proceso continúa. La MAU se salta automáticamente un nodo de red que no esté encendido. Sin embargo, dado que cada nodo de una red Token Ring examina y luego retransmite cada token (señal), un nodo con mal funcionamiento puede hacer que deje de trabajar toda la red. Token Ring tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes con poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, Token Ring llega a ser más eficiente que CSMA/CD.

Nuevas tecnologías

Existen varias tecnologías nuevas que satisfacen las necesidades de las redes actuales, incluyendo a Fast Ethernet, FDDI, Frame Relay y ATM.

Fast Ethernet, llamado también 100BASEX, es una extensión del estándar Ethernet que opera a velocidades de 100 Mbps, un incremento 10 veces mayor que el Ethernet estándar de 10 Mbps.

La interfaz de distribución de datos por fibra óptica (FDDI) es un estándar para la transferencia de datos por cable de fibra óptica. El estándar ANSI X3T9.5 para FDDI especifica una velocidad de 100 Mbps. Dado que el cable de fibra óptica no es susceptible a la interferencia eléctrica o tan susceptible a la degradación de la señal de red como sucede con los cables de red estándar, FDDI permite el empleo de cables mucho más largos que otros estándares de red.

El Frame Relay (retransmisión de tramas) es un servicio orientado a la conexión, para mover datos de un nodo a otro a una velocidad razonable y bajo costo. El frame relay puede verse como una línea virtual rentada. El usuario renta un circuito virtual permanente entre dos puntos y entonces puede enviar tramas o frames (es decir, paquetes) de hasta 1600 bytes entre ellos. Además de competir con las líneas rentadas, el frame relay compite con los circuitos virtuales permanentes de X.25.

ATM, que significa modo de transferencia asíncrona, es un conjunto de estándares internacionales para la transferencia de datos, voz y video por medio de una red a muy altas velocidades. Puesto que

opera a velocidades que van desde 1.5 Mbps hasta 1.5 Gbps, ATM incorpora parte de los estándares Ethernet, Token Ring y FDDI para la transferencia de datos.

Descripción del modelo OSI

El modelo de referencia OSI es la arquitectura de red actual más prominente. El objetivo de éste es desarrollar estándares para la interconexión de sistemas abiertos *(Open System Interconnection, OSI)*. El término OSI es el nombre dado a un conjunto de estándares para las comunicaciones entre computadoras, terminales y redes. OSI es un modelo de 7 capas, donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI. Algunas de las funciones de cada capa o nivel se describen en la Figura 1.4.

Nivel de Aplicación. Se definen una serie de aplicaciones para la comunicación entre distintos sistemas, las cuales gestionan:

- Transferencia de archivos (FTP).
- Intercambio de mensajes (correo electrónico).

Nivel de Presentación. En esta capa se realizan las siguientes funciones:

- Se da formato a la información para visualizarla o imprimirla.
- Se interpretan los códigos que estén en los datos (conversión de código).
- Se gestiona la encriptación de datos.
- Se realiza la compresión de datos.

Figura 1.4

Programa de aplicación del usuario		
Nivel 7	Aplicación	Provee servicios generales relacionados con apliciones (transferencia de archivos)
Nivel 6	Presentación	Formato de datos (ASCII)
Nivel 5	Sesión	Coordina la interacción en la sesión (diálogo) de los usuarios
Nivel 4	Transporte	Provee una transmisión de datos confiable punto a punto
Nivel 3	Red	Enruta unidades de información
Nivel 2	Enlace de datos	Provee intercambio de datos entre dispositivos en el mismo medio
Nivel 1	Físico	Transmite un flujo de bits a través del medio físico

Nivel de Sesión. Provee mecanismos para organizar y estructurar diálogos entre procesos de aplicación. Actúa como un elemento moderador capaz de coordinar y controlar el intercambio de los datos. Controla la integridad y el flujo de los datos en ambos sentidos. Algunas de las funciones que realiza son las siguientes:

- Establecimiento de la conexión de sesión.
- Intercambio de datos.
- Liberación de la conexión de sesión.
- Sincronización de la sesión.
- Administración de la sesión.

Nivel de Transporte. Esta capa asegura que se reciban todos los datos y en el orden adecuado. Realiza un control de extremo a extremo. Algunas de las funciones realizadas son:
Acepta los datos del nivel de sesión, fragmentándolos en unidades más pequeñas en caso necesario y los pasa al nivel de red.

Multiplexaje.
Regula el control de flujo del tráfico de extremo a extremo.
Reconoce los paquetes duplicados.
Nivel de Red. En esta capa se determina el establecimiento de la ruta.
Esta capa mira las direcciones del paquete para determinar los métodos de conmutación y enrutamiento.

- Realiza control de congestión.
- Nivel de Enlace de Datos.
- Detección y control de errores (mediante el empleo del CRC).
- Control de secuencia.
- Control de flujo.
- Control de enlace lógico.
- Control de acceso al medio.
- Sincronización de la trama.

Nivel Físico.
Define las características físicas (componentes y conectores mecánicos).
Define las características eléctricas (niveles de tensión).
Define las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
Solamente reconoce bits individuales, no reconoce caracteres ni tramas multicaracter.

Firewalls o puertas de seguridad
Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

Sin duda que todos estos antecedentes de la seguridad de la información nos sirven de base, para reconocer puntos de partida, los cuales debemos de considerar siempre en el desarrollo de este trabajo, poniendo particular interés que los elementos que se exponen en este capítulo relacionados

principalmente con las medidas de seguridad física, lógica y de redes se reflejen en la implementación del método propuesto y como consecuencia en el caso práctico, DRP para una empresa de Telecomunicaciones, expuesto en el capítulo 5.

De primordial importancia resulta conocer los procedimientos y técnicas para realizar evaluación de proyectos, estimaciones de pérdidas y la administración de riesgos, puntos que tocaremos en el siguiente capítulo.

Capítulo 2

El Análisis de Riesgos

En la actualidad todas las organizaciones necesitan enfrentar riesgos para sobrevivir, la mayoría de ellas necesitan incrementar el nivel de riesgos que le permitan ser exitosas a largo plazo, con el significativo incremento en el nivel de competencia sobre sus adversarios, marcando objetivos y metas agresivos, que se conviertan en normas de supervivencia y competitividad

El análisis de riesgos proporciona herramientas útiles para cuantificar, medir y evaluar los alcances de factores adversos, lo cual nos permitirá tener los elementos necesarios para calificar el riesgo y decidir asumirlo, reducirlo o transferirlo.

Podemos definir el riesgo como, posibilidad de que ocurra algún evento no deseado para las personas y/o empresas. En atención a esta definición, señalaremos que cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos y externos, tan variables como su propio entorno, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología utilizada.

En elemento adicional de riesgo es la alta concentración que hoy en día tenemos en centros de proceso de información, de operaciones que hasta hace algunos años se registraban y conservaban completamente por separado.

Los equipos de cómputo que habitualmente se utilizan en las empresas están sujetos al riesgo de que ocurra alguna eventualidad que los dañe. El costo de asumir esa eventualidad puedes ser muy alto, si se considera que en muchas ocasiones no basta con reponer un equipo, sino absorber las pérdidas consecuenciales de la falta del mismo.

2.1 Objetivo del Análisis

El objetivo general del análisis de riesgos es cuantificar los riesgos a que están sujetos los activos de una empresa, la pérdida esperada y el costo de tomar medidas de control. Cuando este costo es menor a la perdida esperada, se debe realizar la acción.

Objetivos específicos
Los objetivos específicos del análisis de riesgos son:

a) Identificar cuales son los activos existentes.
Al determinar los activos existentes es recomendable realizar un inventario detallado. Además, se deben evaluar los costos de las pérdidas potenciales y cuantificar los costos de reposición y reparación.
Podemos señalar tres áreas de riesgo básicas:

- Instalaciones de proceso de información
- Información
- Comunicaciones

b) Llevar a cabo un minucioso análisis de riesgos y debilidades.
Identificar las fuentes, alcances, métodos y amenazas potenciales. Estimar la probabilidad de cada ocurrencia e identificar las debilidades potenciales y todos los tipos de amenazas y vulnerabilidades.
c) Identificar los recursos del sistema, definir y revisar todos los controles de seguridad y las defensas ya existentes.

d) Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.
El análisis de riesgos deberá definir cuales son las medidas a implantar y las ventajas y desventajas de cada decisión.
e) Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.
El tiempo y lo recursos necesarios para atacar los problemas dependerán del tipo de riesgo considerado. Se debe tomar en cuenta que muchas veces se incrementa la pérdida por la interrupción de labores o bien que puede existir una pérdida de oportunidades para la empresa en caso de que la restitución tome mucho tiempo. Los recursos actualmente disponibles ayudaran a contrarrestar los gastos y deben considerarse dentro del análisis.

La descripción adecuada de los activos existentes es de gran importancia ya que puede revelar riesgos ignorados hasta el momento. Es recomendable contar con un inventario detallado de todo el equipo, evaluando el costo de reposición y los recursos de sustitución ya disponibles.

Es importante señalar que, aunque el equipo esta constantemente expuesto al riesgo, no todos ocurren con la misma frecuencia, ni su efecto tiene el mismo impacto sobre la empresa en términos de costo.

Para determinar la probabilidad de que ocurra un evento que dañe las instalaciones se recurre a diversas técnicas. El objetivo del análisis de riesgos, bajo este criterio, se divide en dos:

- Reducir la probabilidad de que ocurra el evento.
- Proporcionar los elementos de seguridad y protección adecuados para que, en caso de que ocurra un desastre, los costos en que incurra no sean tan altos.

2.2 Identificación de Riesgos

La identificación de riesgos ocurre cuando los integrantes del equipo de análisis de riesgos, reconocen a que tipos de riesgos están expuestos sus equipos, inventarios, empleados, inmuebles, información tecnológica, etc., de tal manera que son capaces de separarlos en base a su clasificación.

Para el presente trabajo los riesgos se clasifican en dos y estos son:

a) Riesgos externos
Los riesgos externos se definen como aquellos que se presentan en el ambiente físico y social que rodea a una instalación de procesamiento de información. Si bien no es posible eliminarlos, si es factible tomar las medidas necesarias para que minimicen la probabilidad de pérdida de información o destrucción de las instalaciones. Pueden ser naturales u ocasionadas por el hombre.

Los ocasionados por desastres naturales tales como:

- Inundaciones
- Temblores
- Tornados
- Tormentas eléctricas
- Huracanes
- Erupciones volcánicas

Aquellos propiciados por el hombre.

- Incendios
- Explosiones
- Accidentes laborales
- Bombas
- Destrucción intencional
- Sabotaje
- Terrorismo
- Robos
- Fraude
- Contaminación ambiental, etc.

b) Riesgos internos

Los riesgos internos se generan desde la misma empresa, por su origen, son más sencillos de prever, sin embargo y aun cuando parezca contradictorio, será más fácil que se presenten ya que el conocimiento de los procedimientos internos de operación hará más sencillo el camino de alguna persona interesada en dañar a la institución. Por ejemplo:

- Robo:
- De material
- Recursos
- Información
- Sabotaje
- Destrucción
- De datos
- De recursos
- Huelgas
- Fraudes

Una vez determinados los riesgos, es importante que se realice una evaluación del presupuesto asignado para reducirlos. Se deben considerar los siguientes puntos:

Objetivo

Lo qué se busca con un plan de reducción de riesgos.

Alcance y recursos

Determinar la magnitud de las necesidades de la empresa y los recursos de la organización para satisfacerlas.

Planeación profunda

El plan debe considerar todas las posibilidades y evaluar hasta el más mínimo riesgo existente.

Organización del proyecto

Es necesario contar con un responsable de los trabajos realizados, que tenga pleno conocimiento de lo que ha hecho.

Esfuerzo conjunto

Si existen voluntarios capaces de contribuir de manera efectiva al plan, se deben aceptar su ayuda.

2.3 Técnicas de Análisis

En esta etapa se busca obtener el entendimiento y conocimiento de los riesgos identificados de tal manera que se pueda recopilar información que permita el cálculo del nivel de riesgo al cual está expuesto el objeto en la actualidad, Identificar los controles existentes implementados para mitigar el impacto ante la ocurrencia de los riesgos, permitiendo de esta manera valorar los niveles del riesgo, la efectividad de los controles y el nivel de exposición.

El riesgo es analizado a través de la combinación de estimativos de probabilidad y de las consecuencias en el contexto de las medidas de control existentes. El análisis de riesgos involucra un debido examen de las fuentes de riesgo, sus consecuencias y la probabilidad de que esas consecuencias puedan ocurrir. Pueden llegar a identificarse factores que afectan tanto las consecuencias como la probabilidad.

Los estimativos pueden determinarse utilizando análisis, estadísticas y cálculos. Alternativamente donde no hay datos históricos disponibles, se pueden hacer estimativos subjetivos que reflejen el grado de creencia de un grupo o de un individuo en que un evento en particular o suceso ocurran.

La evaluación de riesgos incluye comparar el nivel de riesgo encontrado durante el proceso de análisis contra el criterio de riesgo establecido previamente y decidir si los riesgos pueden ser aceptados.

El análisis de riesgos y los criterios contra los cuales los riesgos son comparados en la valoración deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados como números específicos, tales como fatalidad, frecuencia o valores monetarios. El resultado de una evaluación de riesgos es una lista priorizada de riesgos para definirles acciones de tratamiento posteriores.

Básicamente, existen dos tipos de métodos para la realización de análisis de riesgos a saber:

-Métodos cuantitativos
-Métodos cualitativos

2.3.1 Métodos cuantitativos

2.3.1.1 Análisis de regresión

Regresión es la cantidad de cambio de una variable asociada a un cambio único de otra variable.
La correlación se refiere al hecho de que dos variables se encuentren relacionadas y a la estrecha relación que existe entre ellas. La regresión a su vez, se refiere a la naturaleza de la relación.

El análisis de regresión es una herramienta muy útil en el análisis de riesgos ya que podríamos estimar la probabilidad de que se presente un evento no deseado, ver el comportamiento y tendencias de variables (ventas, producción, ganancias, pérdidas, necesidad de materias primas, etc.) y estimar algún evento en especial. En esta tesis se utilizará para pronosticar el comportamiento de llamadas y estimar el cálculo de la pérdida probable en caso de que no se contara con un DRP y se estuviera sin sistema durante algún tiempo determinado.

Ejemplos:

- Una venta es igual a un cliente.
- Cada cliente me da a ganar $100.
- Por cada hora tengo ganancias de $10,000.

Estos ejemplos implican la correlación de dos variables, pero van más allá e indican en términos numéricos como están relacionadas estas variables.

Variable independiente (X)	Variable dependiente (Y)	Ecuación de la regresión
Venta	Cliente	Y = X
Cliente	Pesos	Y = 100X
Por cada hora	Ganancias	Y = 10000X

Existen varios modelos utilizados en el análisis de regresión, estos pueden ser:

- Modelo Lineal
- Modelo geométrico
- Modelo Logarítmico
- Modelo Cuadrático
- Modelo Raíz Cuadrada

El análisis de regresión es una técnica de investigación, modelando la relación entre variables.
Las aplicaciones de regresión son numerosas y se aplican en todos los campos, de hecho, podríamos decir que es la técnica estadística que más ampliamente es usada.

<u>Modelo Lineal:</u>

El símbolo **a** recibe el nombre de intercepto, puesto que cuando ***x*** es igual a cero, ***y*** = ***a***; cuando ***a*** es igual a cero, ***y*** es también igual a cero. El símbolo ***b*** se denomina pendiente, puesto que determina la inclinación de la recta. Es fácil apreciar que ***b*** es la cantidad de cambio de ***y***, asociada a un cambio unitario de ***x***, por lo consiguiente, esta recibe el nombre de coeficiente de regresión.

$$\hat{Y} = a + b\,X$$

Las fórmulas de trabajo son:

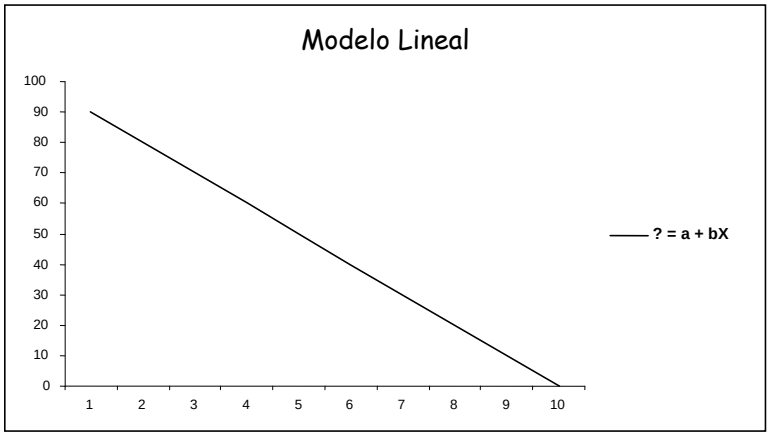
$$a = \overline{Y} - b\,\overline{X}\ , \qquad b = \frac{\left[\sum XY - \frac{\sum X \sum Y}{n}\right]}{\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right]}$$

Otro factor importante en el análisis de regresión es el coeficiente de determinación. Este coeficiente mide el nivel de ajuste de la curva de regresión con relación al fenómeno planteado. Puede estar en términos de porcentaje o referido a la unidad. Es de gran utilidad para decidir entre diferentes modelos de regresión cual es el mejor.

Su cálculo es el siguiente:

$$R^2 = \frac{\left[\sum XY - \frac{\sum X \sum Y}{n}\right]^2}{\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right] * \left[\sum Y^2 - \frac{\left(\sum Y\right)^2}{n}\right]}$$

Figura 2.1

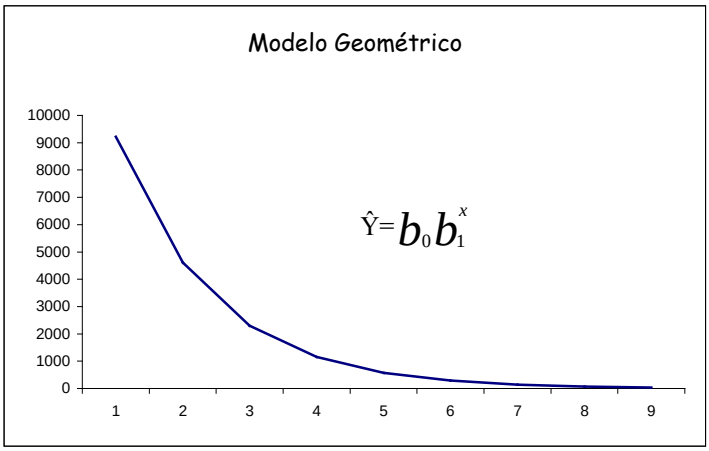


Cabe mencionar que para efectos de la presente tesis utilizaremos el modelo lineal, para estimar la pérdida probable en nuestro caso práctico desarrollado en el capítulo 5. Sin embargo, no siempre se puede explicar la relación entre 2 variables con el modelo lineal. Para tal efecto existen una gama de modelos de regresión que bien se podría decir que se puede representar cualquier fenómeno natural bajo alguno de los modelos.

La función más eficaz, será la que se ajuste mejor, es decir, se trata de encontrar la función en la cual la suma de los cuadrados de las diferencias entre los valores observados y esperados sea menor.

<u>Modelo geométrico:</u>

Figura 2.2



Donde:

$$\hat{Y} = b_0 b_1^X$$

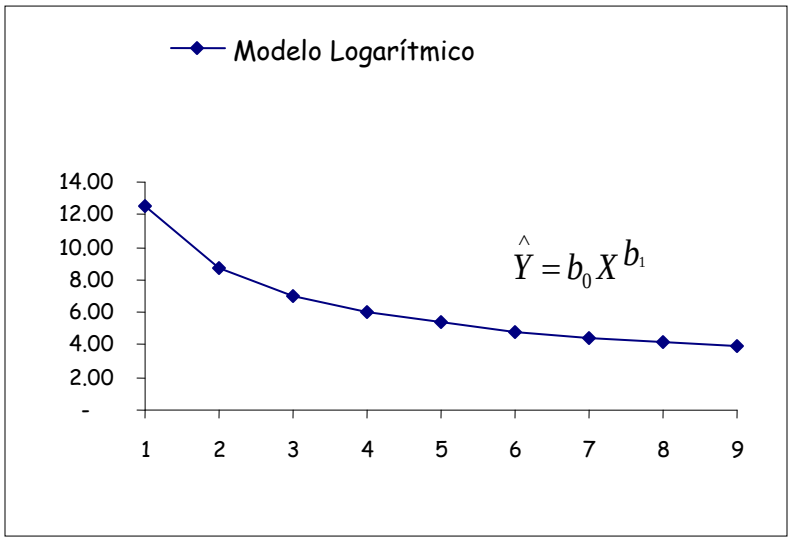
$$b_0 = \exp^{\left(\frac{\sum \ln Y}{n} - b_1 * X\right)}$$

$$b_1 = \frac{\sum X \ln Y - \sum X * \frac{\left(\sum \ln Y\right)}{n}}{\sum X^2 - \frac{\left(\sum X\right)^2}{n}}$$

$$R^2 = \frac{\left[\sum X \ln Y - \sum X \frac{\sum \ln Y}{n}\right]^2}{\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right] * \left[\sum Y^2 - \frac{\left(\sum Y\right)^2}{n}\right]}$$

<u>Modelo Logarítmico:</u>

Figura 2.3



Donde:

$$\hat{Y} = b_0 X^{b_1}$$

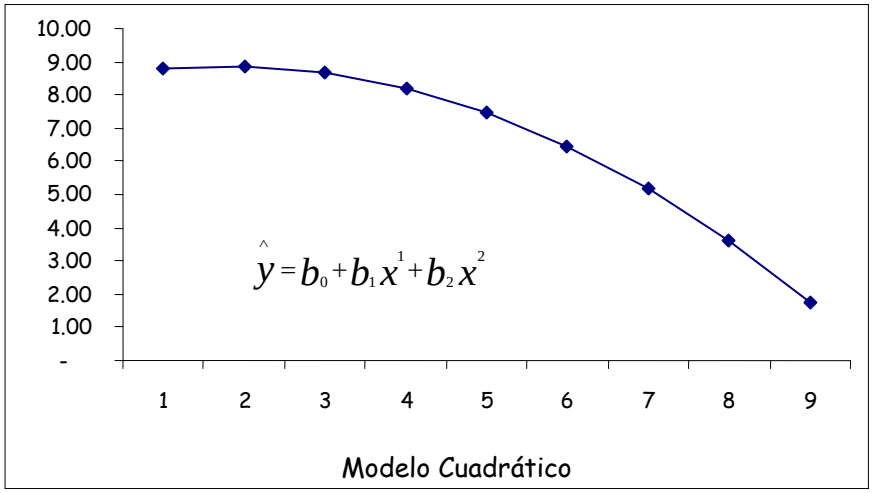
$$b_0 = \exp^{\left(\sum \ln \bar{Y} * b_1 * \ln \bar{X}\right)}$$

$$b_1 = \frac{\sum \ln X \ln Y - \frac{\sum \ln X * \sum \ln Y}{n}}{\sum (\ln X)^2 - \frac{\left(\sum \ln X\right)^2}{n}}$$

$$R^2 = \frac{\left[\sum \ln X \ln Y - \frac{\sum \ln X \sum \ln Y}{n}\right]^2}{\left[\sum \ln X^2 - \frac{\left(\sum \ln X\right)^2}{n}\right] * \left[\sum \ln Y^2 - \frac{\left(\sum \ln Y\right)^2}{n}\right]}$$

<u>Modelo Cuadrático:</u>

Figura 2.4



Donde:

$$\hat{Y} = b_0 + b_1 X^1 + b_2 X^2$$

$$b_0 = \overline{Y} - b_1 \overline{X} - b_2 \overline{X}^2$$

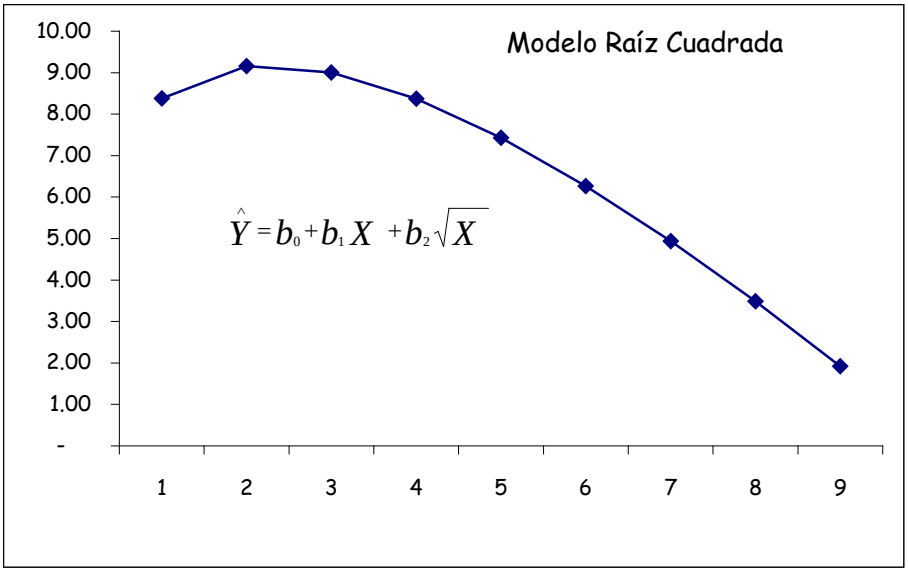
$$b_1 = \frac{\left[\left[\sum XY - \frac{\sum X \sum Y}{n}\right] * \left[\sum X^4 - \frac{\left(\sum X^2\right)^2}{n}\right]\right] - \left[\left[\sum X^2 Y - \frac{\sum X^2 \sum Y}{n}\right] * \left[\sum X^3 - \frac{\sum X \sum X^2}{n}\right]\right]}{\left[\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right] * \left[\sum X^4 - \frac{\left(\sum X^2\right)^2}{n}\right]\right] - \left[\sum X^3 - \frac{\sum X \sum X^2}{n}\right]^2}$$

$$b_2 = \frac{\left[\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right] * \left[\sum X^2 Y - \frac{\sum X^2 \sum Y}{n}\right]\right] - \left[\left[\sum X^3 - \frac{\sum X \sum X^2}{n}\right] * \left[\sum XY - \frac{\sum X \sum Y}{n}\right]\right]}{\left[\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right] * \left[\sum X^4 - \frac{\left(\sum X^2\right)^2}{n}\right]\right] - \left[\sum X^3 - \frac{\sum X \sum X^2}{n}\right]^2}$$

$$R^2 = \frac{b_1\left[\sum XY - \frac{\sum X * \sum Y}{n}\right] + b_2\left[\sum X^2 Y - \frac{\sum X^2 * \sum Y}{n}\right]}{\sum Y^2 - \frac{\left(\sum Y\right)^2}{n}}$$

<u>Modelo Raíz Cuadrada:</u>

Figura 2.5



Donde:

$$b_0 = \overline{Y} - b_1 - b_2\overline{R}$$

$$R = \sqrt{X}$$

$$b_1 = \frac{\left[\left[\sum XY - \frac{\sum X \sum Y}{n}\right] * \left[\sum X - \frac{\left(\sum R\right)^2}{n}\right]\right] - \left[\left[\sum RY - \frac{\sum R \sum Y}{n}\right] * \left[\sum RX - \frac{\sum R \sum X}{n}\right]\right]}{\left[\left[\sum X - \frac{\left(\sum R\right)^2}{n}\right] * \left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right]\right] - \left[\sum RX - \frac{\sum R \sum X}{n}\right]}$$

$$b_2 = \frac{\left[\left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right] * \left[\sum RY - \frac{\sum R \sum Y}{n}\right]\right] - \left[\left[\sum RX - \frac{\sum R \sum X}{n}\right] * \left[\sum XY - \frac{\sum X \sum Y}{n}\right]\right]}{\left[\left[\sum R^2 - \frac{\left(\sum R\right)^2}{n}\right] * \left[\sum X^2 - \frac{\left(\sum X\right)^2}{n}\right]\right] - \left[\sum RX - \frac{\sum R \sum X}{n}\right]^2}$$

$$R^2 = \frac{b_1\left[\sum XY - \frac{\sum X * \sum Y}{n}\right] + b_2\left[\sum RY - \frac{\sum R \sum Y}{n}\right]}{\sum Y^2 - \frac{\left(\sum Y\right)^2}{n}}$$

2.3.1.2 Series de tiempo

En las sociedades donde vivimos, el riesgo y la incertidumbre ante el futuro aparecen como problemas a los que distintos agentes tratan de adaptarse de diferentes maneras. Para reducir el grado de incertidumbre se suele recurrir a la elaboración de previsiones que tratan de anticipar la evolución de algún fenómeno. El disponer de un conocimiento sobre el futuro, aunque sea de manera aproximada, facilita la toma de decisiones en las que incurrimos cuando pretendemos modificar o prever alguna realidad.

Toda institución, empresa, el gobierno e incluso la familia, tiene que hacer planes para el futuro si ha de sobrevivir y progresar. Hoy en día diversas instituciones requieren conocer el comportamiento futuro de ciertos fenómenos con el fin de planificar, prever o prevenir.

La planificación racional exige prever los sucesos del futuro que probablemente vayan a ocurrir. La previsión, a su vez, se suele basar en lo que ha ocurrido en el pasado. Se tiene pues un nuevo tipo de inferencia estadística que se hace acerca del futuro de alguna variable o compuesto de variables basándose en sucesos pasados.

En el caso de las ventas de servicios de televisión digital, por ejemplo requerimos conocer las tendencias de demanda, las cuales particularmente requieren de estimarse para planeación y determinación de metas de ventas estacionales o de eventos de temporada, como podría ser la serie mundial de béisbol, el campeonato del mundo de fútbol, entre otros eventos de relevancia para sectores específicos de la población.

Igualmente los impactos que podría tener la empresa por la presencia de riesgos de temporada como huracanes en verano o cortes de electricidad en época de vientos como febrero y marzo y con ello poder predeterminar las pérdidas por fenómenos meteorológicos.

Una de las técnicas más importante para hacer inferencias sobre el futuro con base en lo ocurrido en el pasado, es el ***análisis de series de tiempo***.

Existen aplicaciones en distintas áreas del conocimiento, tales como, en economía, física, geofísica, química, electricidad, en demografía, en marketing, en telecomunicaciones, en transporte, etc. (ver ejemplos en la figura 2.6).

Uno de los problemas que intenta resolver las series de tiempo es el de predicción. Esto es dado una serie $\{x(t1),\ldots,x(tn)\}$ nuestros objetivos de interés son describir el comportamiento de la serie, investigar el mecanismo generador de la serie temporal, buscar posibles patrones temporales que permitan sobrepasar la incertidumbre del futuro.

Primeramente buscaremos como construir un modelo para explicar la estructura y prever la evolución de una variable que observamos a lo largo del tiempo. La variables de interés puede ser

macroeconómica (índice de precios al consumo, demanda de electricidad, series de exportaciones o importaciones, etc.), microeconómica (ventas de una empresa, existencias en un almacén, gastos en publicidad de un sector), física (velocidad del viento en una central eólica, temperatura en un proceso, caudal de un río, concentración en la atmósfera de un agente contaminante), o social (número de nacimientos, matrimonios, defunciones, o votos a un partido político).

Figura 2.6

Series De Tiempo	***Ejemplos***
1. Series económicas:	- Precios de un artículo - Tasas de desempleo - Tasa de inflación - Índice de precios, entre otros
2. Series Físicas:	- Meteorología - Cantidad de agua caída - Temperatura máxima diaria - Velocidad del viento (energía eólica) - Energía solar, etc.
3. Geofísica:	- Series sismologías
4. Series demográficas:	- Tasas de crecimiento de la población - Tasa de natalidad, mortalidad - Resultados de censos poblacionales
5. Series de marketing:	- Series de demanda, gastos, ofertas - Ventas de temporada - Nivel de audiencia televisiva, publicidad
6. Series de telecomunicación:	- Análisis de señales
7. Series de transporte:	- Series de tráfico

Llamamos *Serie de Tiempo* f a un conjunto de mediciones de cierto fenómeno o experimento registradas secuencialmente en el tiempo. Estas observaciones serán denotadas por $\{x(t_1), x(t_2), ..., x(t_n)\} = \{x(t) : t \in T \subseteq R\}$ con $x(t_i)$ el valor de la variable x en el instante t_i.

A través del tiempo estas medidas se pueden ser tomadas en determinados puntos en el tiempo o de manera continua, así entonces, estos dos tipos de series se llaman discretas y continuas, respectivamente.

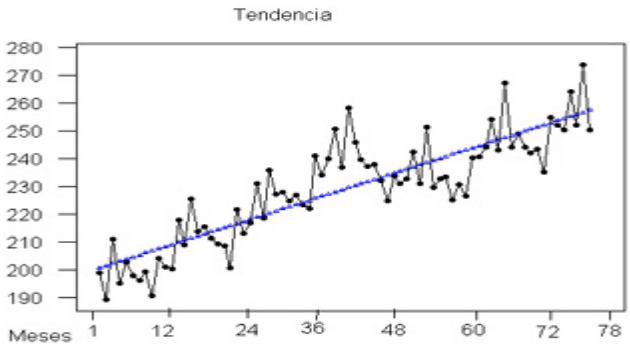
<u>Análisis de series de tiempo.</u>

El primer paso en el análisis de series de tiempo, consiste en graficar la serie. Esto nos permite detectar las componentes esenciales de la serie. El gráfico de la serie permitirá entonces:

a) Permite detectar tendencia: la tendencia representa el comportamiento predominante de la serie. Este componente es de gran interés ya que refleja la dirección del movimiento de una determinada variable en la figura 2.7 se muestra un ejemplo gráfico.

b) Variación estacional: la variación estacional representa un movimiento periódico de la serie de tiempo. La duración de la unidad del periodo es generalmente menor que un año. Puede ser un trimestre, un mes o un día, etc. (ver figura 2.8)

Figura 2.7[1]

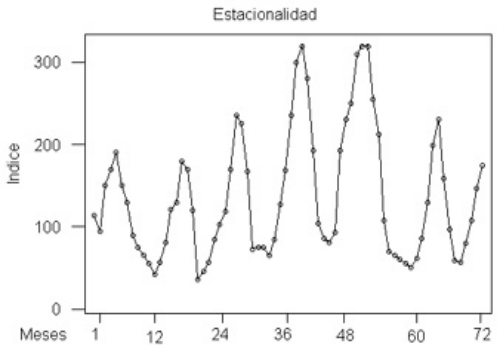


Las principales fuerzas que causan una variación estacional son las condiciones del tiempo, como por ejemplo:

1) en invierno las ventas de helado
2) en verano la venta de lana
3) exportación de fruta en marzo.

Todos estos fenómenos presentan un comportamiento estacional (anual, semanal, etc.)

Figura 2.8[2]



c) Detectar Componente irregular (*Outlier*): se refiere a puntos de la serie que se escapan de lo normal. Un outliers es una observación de la serie que corresponde a un comportamiento anormal del fenómeno (sin incidencias futuras) o a un error de medición.

Se debe determinar desde fuera si un punto dado es outlier o no. Si se concluye que lo es, se debe omitir o reemplazar por otro valor antes de analizar la serie.

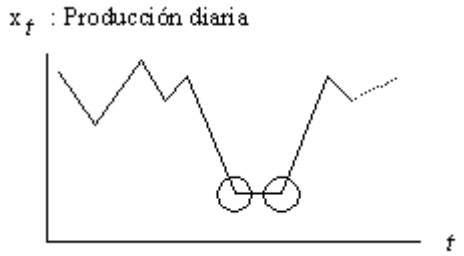
Por ejemplo, en un estudio de la producción diaria en una fábrica se presentó la situación que se muestra en la figura 2.9

Los dos puntos enmarcados en un círculo parecen corresponder a un comportamiento anormal de la serie. Al investigar estos dos puntos se vio que correspondían a dos días de paro, lo que naturalmente

[1]Figura tomada del libro: Carmen Rodríguez Morilla, "Análisis de Series Temporales", Ed. La Muralla S.A.
[2] Figura tomada del libro: Carmen Rodríguez Morilla, "Análisis de Series Temporales", Ed. La Muralla S.A.

afectó la producción en esos días. El problema puede solucionarse eliminando las observaciones e interpolando.

Figura 2.9[3]



d) Variaciones irregulares (componente aleatoria): los movimientos irregulares (al azar) representan todos los tipos de movimientos de una serie de tiempo que no sea tendencia, variaciones estacionales y fluctuaciones cíclicas.

<u>Modelos Clásicos de Series de Tiempo</u>

Un modelo clásico para una serie de tiempo, supone que una serie *x(1), ..., x(n)* puede ser expresada como suma o producto de tres componentes: *tendencia*, *estacionalidad* y un término de *error aleatorio*.

Existen tres modelos de series de tiempos, que generalmente se aceptan como buenas aproximaciones a las verdaderas relaciones, entre los componentes de los datos observados. Estos son:

i). Aditivo: $X(t) = T(t) + E(t) + A(t)$

ii). Multiplicativo: $X(t) = T(t) \cdot E(t) \cdot A(t)$

iii). Mixto: $X(t) = T(t) \cdot E(t) + A(t)$

Donde:

- $X(t)$ serie observada en instante t
- $T(t)$ componente de tendencia
- $E(t)$ componente estacional
- $A(t)$ componente aleatoria (accidental)

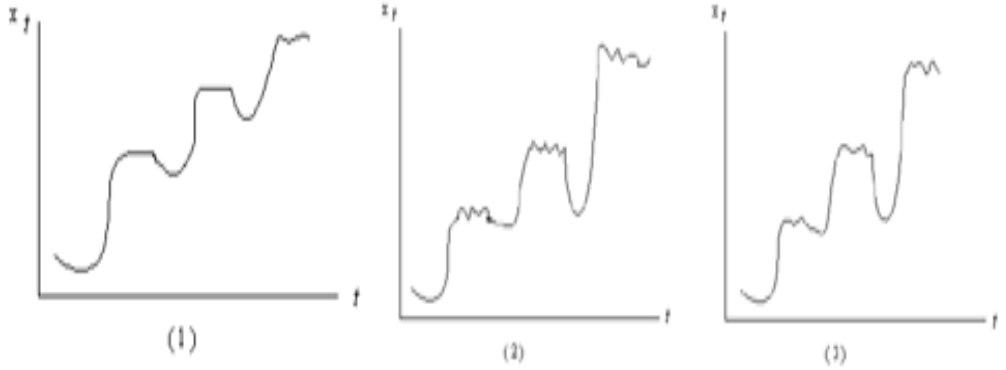
Una suposición usual es que $A(t)$ sea una componente aleatoria con media cero y varianza constante.

Un modelo aditivo (i), es adecuado, por ejemplo, cuando $E(t)$ no depende de otras componentes, como $T(t)$, sí por el contrario la estacionalidad varía con la tendencia, el modelo más adecuado es un modelo multiplicativo (ii). Es claro que el modelo ii puede ser transformado en aditivo, tomando logaritmos. El problema que se presenta, es modelar adecuadamente las componentes de la serie.

La figura 2.10 ilustra posibles patrones que podrían seguir series representadas por los modelos (i), (ii) y (iii).

[3] Figura tomada del libro: Carmen Rodríguez Morilla, "Análisis de Series Temporales", Ed. La Muralla S.A.

Figura 2.10[4]



A modo de síntesis, con el análisis de series de tiempo pretendemos extraer las regularidades que se observan con el comportamiento pasado de la variable, obtener el mecanismo que la genera, para en base a ello, tener un mejor conocimiento de la misma en el tiempo y bajo el supuesto de que las condiciones estructurales que conforman el fenómeno objeto de estudio pertenecen constantes, predecir el comportamiento futuro reduciendo, de esta forma, la incertidumbre en la toma de dediciones.

2.3.1.3 Probabilidad de Ocurrencia

Muchas veces determinar la probabilidad de que ocurra un desastre es altamente complicado. La determinación de la probabilidad de ocurrencia de un evento depende básicamente del conocimiento que el hombre tenga del fenómeno en particular. Todas las circunstancias desconocidas involucran necesariamente un elemento aleatorio. Cuando se da el caso de que los acontecimientos se presentan frecuentemente, el elemento azar puede ser modelado hasta cierto punto. Entonces, bajo en criterio frecuentista se puede calcular la probabilidad de que ocurra el evento en un momento dado. Sin embargo, la mayoría de los desastres naturales no ocurren con altas frecuencias.

Cuando no se cuenta con información suficiente sobre algún fenómeno, lo que se hace es buscar la opinión de los expertos. Así, por ejemplo, existe el método DELPHI, que consiste en reunir a un grupo de expertos en cierto tema y hacerles preguntas sobre el mismo, hasta llegar a un consenso.

Por lo general, los eventos con menor probabilidad de ocurrencia son los que pueden llegar a producir mayores daños. Sin embargo no se deben menospreciar los pequeños eventos ocurridos a diario ya que muchas veces el costo acostumbrado de enfrentarlos sobrepasa el costo producido por un desastre de mayor magnitud.

2.3.1.4 Cálculo de Pérdida Probable (Impacto)

Una vez que se ha determinado la probabilidad (P) de que ocurra un evento en un período dado de tiempo (generalmente un año), se deben cuantificar la pérdida esperada en el período (C) tomando en consideración las pérdidas probables que podrían ser ocasionadas por eventos similares. El riesgo expresado en términos de pérdida probable (R), en un cierto periodo, se obtiene de la relación:

[4] Figura tomada del libro: Carmen Rodríguez Morilla, "Análisis de Series Temporales", Ed. La Muralla S.A.

(Se describe con mayor amplitud este tema en el anexo III, "Elementos de Probabilidad").

R = P * C

R: Riesgo
P: Probabilidad de que ocurra un evento
C: Perdida operacional en el periodo

Cuando existen diversos riesgos, la pérdida probable a nivel global es simplemente la suma de todas las pérdidas probables:

$$RT = \sum_{i=1}^{n} P_i * C_i$$

Al evaluar la pérdida en el periodo C_i producida por cualquier evento, es de vital importancia considerar los siguientes factores:

- Costo de reparación o reemplazo.
- Tiempo de respuesta
- Costo de instalación y servicios.
- Interrupción de labores debida a la suspensión en el procesamiento
- Personal adicional.
- Pérdida de oportunidades.
- Pérdida de beneficios esperados.
- Detrimento de la imagen de la empresa.

2.3.1.5 Pérdida Máxima Probable

Es el evento de más elevado importe que podría producirse, ponderando tanto las características propias del riesgo, como todo los factores que de uno u otro modo podrían influir en el mismo.

2.3.2 Métodos cualitativos

Las técnicas cualitativas únicamente indican, en términos relativos y sin llegar a una cuantificación, la pérdida que ocasionaría cierta eventualidad comparada con otra.

Los métodos cualitativos se caracterizan por no recurrir a cálculos numéricos. Pueden ser métodos comparativos y métodos generalizados.

2.3.2.1 Métodos comparativos

Se basan en la utilización de técnicas obtenidas de la experiencia adquirida en equipos e instalaciones similares existentes, así como en el análisis de sucesos que hayan ocurrido en establecimientos parecidos al que se analiza. Principalmente son cuatro métodos los existentes:

- Manuales técnicos o códigos y normas de diseño
- Listas de comprobación o "Safety check lists"
- Análisis histórico de accidentes
- Análisis preliminar de riesgos o PHA

Manuales técnicos. Códigos y normas de diseño

Consisten en la elaboración de manuales internos de carácter técnico que especifiquen las características de diseño, instalación, operación y utilización de los equipos existentes en un determinado establecimiento. Estos manuales se deben basar en las normas y los códigos internacionales y nacionales de diseño. Para completar el análisis, se deben realizar periódicamente auditorias de seguridad que permitan juzgar el estado de los materiales, procedimientos, operaciones, emergencias que se han establecido.

Las normas y los códigos de diseño son elaboradas por organismos internacionales de reconocido prestigio en el campo de la normalización. A nivel mundial, la organización internacional más importante es la International Organization for Standarization, ISO.

En Europa, cada país ha establecido un sistema de normalización de carácter oficial o semioficial. Las más importantes son las siguientes:

España: Asociación Española de Normalización y Certificación, AENOR. Elabora las normas UNE a partir de las ISO u otras.

Alemania: Normas DIN. Normas VDI/VDE, Verein Deutscher Ingenieure.

Reino Unido: British Standards, BS.

En Estados Unidos de América, existen varias organizaciones gubernamentales y privadas que se dedican a la elaboración de normas:

- American National Standards Institute, ANSI
- American Society for Testing and Materials, ASTM
- American Petroleum Institute, API
- National Fire Protection Association, NFPA
- American Society of Mechanical Engineers, ASME

Listas de Comprobación: Safety Check Lists

Se utilizan para determinar la adecuación de los equipos, procedimientos, materiales, etc. a un determinado procedimiento o reglamento establecido por la propia organización basado en experiencia y en los códigos de diseño y operación. Se pueden aplicar en cualquier fase de un proyecto o modificación: diseño, construcción, puesta en marcha, operación y paradas.

Permite comprobar con cierto detalle la adecuación de las instalaciones y constituye una buena base de partida para complementarlas con otros métodos de identificación que tienen un alcance superior al cubierto por los reglamentos e instrucciones técnicas.

Análisis Histórico de Accidentes

Consiste en el estudio de los accidentes registrados en el pasado en empresas tecnológicas y de telecomunicaciones. La principal ventaja radica en que se refiere a accidentes que ya han ocurrido, por lo que el establecimiento de hipótesis de posibles accidentes se basa en casos reales. No

obstante, en los bancos de datos existentes, no se cubren todos los casos posibles, sino sólo los que se han dado, además de que los datos de que dispone pueden no ser completos, sin embargo DIRECTV aprovecha esta información para generar probabilidades de desastres.

La información puede provenir de diferentes fuentes:

- Bibliografía especializada
- Bancos de datos informatizados de accidentes
- Registro de accidentes/incidentes de la propia empresa
- Informes de otros accidentes ocurridos por zonas geográficas

Análisis Preliminar de Riesgos (APR): Preliminary Hazard Analysis (PHA)

Desarrollado inicialmente por las Fuerzas Armadas de USA, ha sido el precursor de análisis más complejos y es utilizado únicamente en la fase de desarrollo de las instalaciones y para casos en los que no existen experiencias anteriores, sea del proceso o del tipo de instalación.

Selecciona las principales áreas de riesgo como son bodegas y áreas de almacenamiento, así como los equipos principales de la planta y revisa los puntos en los que se piensa que se pueda liberar energía de forma incontrolada en: materias, equipos de planta, componentes de sistemas, procesos, operaciones, instalaciones, equipos de seguridad, etc. Los resultados del análisis incluyen recomendaciones para reducir o eliminar estos peligros, siempre de forma cualitativa.

Se requiere relativamente poca inversión en su realización ya que se puede encomendar a 2 ó 3 personas con experiencia en seguridad, códigos de diseño, especificaciones de equipos y materiales; quienes revisaran las instalaciones y los equipos así como la producción en proceso; emitirán su juicio sobre sus observaciones y permitirán que otros especialistas evalúen los costos de asumir los riesgos. Esta técnica resulta pues adecuada para examinar los proyectos de modificaciones a industrias o plantas nuevas en su etapa inicial.

2.3.2.2 Métodos generalizados

Los métodos generalizados de análisis de riesgos, se basan en estudios de las instalaciones y procesos mucho más estructurados desde el punto de vista lógico-deductivo que los métodos comparativos. Normalmente siguen un procedimiento lógico de deducción de fallos, errores, desviaciones en equipos, instalaciones, procesos, operaciones, etc. que trae como consecuencia la obtención de determinadas soluciones para este tipo de eventos.

Existen varios métodos generalizados. Los más importantes son:

- Análisis "What if ...?"
- Análisis funcional de operabilidad, HAZOP
- Análisis de árbol de fallos, FTA
- Análisis de árbol de sucesos, ETA
- Análisis de modo y efecto de los fallos, FMEA
- Mapeo de riesgos “Risk Mapping”

Método de Análisis "What if ...?": ¿Qué pasaría si ...?

Consiste en el planteamiento de las posibles desviaciones en el diseño, construcción, modificaciones y operación de una determinada instalación de todo tipo incluyendo las empresas de telecomunicaciones, utilizando la pregunta que da origen al nombre del procedimiento: "¿Qué pasaría si ...?". Requiere un conocimiento básico del sistema y cierta disposición mental para combinar o sintetizar las desviaciones posibles, por lo que normalmente es necesaria la presencia de personal con amplia experiencia para poder llevarlo a cabo.

Se puede aplicar a cualquier instalación o área o proceso: instrumentación de un equipo, seguridad eléctrica, protección contra incendios, almacenamientos, sustancias peligrosas, etc. Las preguntas se formulan y aplican tanto a proyectos como a plantas en operación, siendo muy común ante cambios en instalaciones ya existentes.
El equipo de trabajo lo forman 2 ó 3 personas especialistas en el área a analizar con documentación detallada de la planta, proceso, equipos, procedimientos, seguridad, entre otros.

El resultado es un listado de posibles escenarios o sucesos incidentales, sus consecuencias y las posibles soluciones para la reducción o eliminación del riesgo. En el capítulo 5, caso práctico, se ejemplifica este método en el inciso 5.2.1.

Análisis Funcional de Operatividad (AFO): Hazard and Operability (HAZOP)

El HAZOP es una técnica de identificación de riesgos inductiva basada en la premisa de que los riesgos, los accidentes o los problemas de operabilidad, se producen como consecuencia de una desviación de las variables de proceso con respecto a los parámetros normales de operación en un sistema dado y en una etapa determinada. Por tanto, ya se aplique en la etapa de diseño, como en la etapa de operación, la sistemática consiste en evaluar, en todas las líneas y en todos los sistemas las consecuencias de posibles desviaciones en todas las unidades de proceso, tanto si es continuo como discontinuo. Se tiene que llegar a los orígenes para encontrar las fallas, pues esta técnica se fundamenta en analizar sistemáticamente las causas y las consecuencias de las desviaciones de las variables de proceso, Se busca una explicación para cada problema detectado, pero revisando las desviaciones a los parámetros estándares de operación.

El método surgido en 1963 en la compañía Imperial Chemical Industries "ICI", se ha venido generalizando y formalizando, y actualmente es una de las herramientas más utilizadas internacionalmente en la identificación de riesgos en instalaciones principalmente de tipo industrial, pero que se puede adaptar para valorar los riesgos a los que se enfrentan otro tipo de empresas como las de telecomunicaciones.

Análisis por Árbol de Fallos, AAF: Fault Tree Analysis, FTA

El Análisis por Árboles de Fallos (AAF), es una técnica deductiva que se centra en un suceso accidental particular (accidente) y proporciona un método para determinar las causas que han producido dicho accidente. Nació en la década de los años 60 para la verificación de la fiabilidad de diseño del cohete Minuteman y ha sido ampliamente utilizado en el campo nuclear y químico. El hecho de su gran utilización se basa en que puede proporcionar resultados tanto cualitativos mediante la

búsqueda de caminos críticos, como cuantitativos, en términos de probabilidad de fallos de componentes.

Para el tratamiento del problema se utiliza un modelo gráfico que muestra las distintas combinaciones de fallos de componentes y/o errores humanos cuya ocurrencia simultánea es suficiente para desembocar en un suceso accidental.
La técnica consiste en un proceso deductivo basado en las leyes del Álgebra de Boole, que permite determinar la expresión de sucesos complejos estudiados en función de los fallos básicos de los elementos que intervienen en él.

Consiste en descomponer sistemáticamente un suceso en sucesos intermedios hasta llegar a sucesos básicos, ligados normalmente a fallos de componentes, errores humanos, errores operativos, etc. Este proceso se realiza enlazando dichos tipos de sucesos mediante lo que se denomina puertas lógicas que representan los operadores del álgebra de sucesos.

Análisis por Árboles de Sucesos, AAS: Event Tree Analysis, ETA

La técnica de análisis por árboles de sucesos consiste en evaluar las consecuencias de posibles accidentes resultantes del fallo específico de un sistema, equipo, suceso o error humano, considerándose como sucesos iniciadores y/o sucesos o sistemas intermedios de mitigación, desde el punto de vista de la atenuación de las consecuencias.

Las conclusiones de los árboles de sucesos son consecuencias de accidentes, es decir, conjunto de sucesos cronológicos de fallos o errores que definen un determinado accidente.
Partiendo del suceso iniciador, se plantean sistemáticamente dos bifurcaciones: en la parte superior se refleja el éxito o la ocurrencia del suceso condicionante y en la parte inferior se representa el fallo o no ocurrencia del mismo.

El suceso iniciador puede ser cualquier desviación importante, provocada por un fallo de un equipo, error de operación o error humano. Dependiendo de las salvaguardias tecnológicas del sistema, de las circunstancias y de la reacción de los operadores, las consecuencias pueden ser muy diferentes. Por esta razón, un AAS, está recomendado para sistemas que tienen establecidos procedimientos de seguridad y emergencia para responder a sucesos iniciadores específicos.

Posteriormente a este análisis cualitativo, la estimación de la magnitud de cada suceso requiere de un análisis de consecuencias mediante modelos de cálculo adecuados, capaces de estimar los efectos del suceso contemplado.
El método se puede usar además para estimar las probabilidades de ocurrencia del suceso final, asignando valores de probabilidad al suceso incidental y valores sucesivos de probabilidad para cada acción enumerada en el árbol.

Análisis de los Modo y Efecto de los fallos, AMFE: Failure Modes and Effects Analysis, FMEA

El método consiste en la elaboración de tablas o listas con los posibles fallos de componentes individuales, los modos de fallo, la detección y los efectos de cada fallo.

Un fallo se puede identificar como una función anormal de un componente, una función fuera del rango del componente, función prematura, entre otros. Los fallos que se pueden considerar son típicamente situaciones de anormalidad tales como:
Abierto, cuando normalmente debería estar cerrado
Cerrado, cuando normalmente debería estar abierto
Marcha, cuando normalmente debería estar parado
Fugas, cuando normalmente deba ser estanco

Los efectos son el resultado de la consideración de cada uno de los fallos identificados individualmente sobre el conjunto de los sistemas de la planta o instalación.

El método FMEA establece finalmente qué fallos individuales pueden afectar directamente o contribuir de una forma destacada al desarrollo de accidentes de una cierta importancia en la planta.

Es un método válido en las etapas de diseño, construcción y operación y se usa habitualmente como fase previa a la elaboración de árboles de fallos, ya que permite un buen conocimiento del sistema. Con ciertas limitaciones se puede usar como método alternativo al HAZOP.

El equipo necesario suele ser de dos personas perfectamente conocedoras de las funciones de cada equipo o sistema así como de la influencia de estas funciones en el resto de la línea de proceso. Es necesario para la correcta ejecución del método disponer de listas de equipos y sistemas, conocimiento de las funciones de cada equipo, junto al conocimiento de las funciones de los sistemas en su conjunto dentro de la planta.

Es posible incluir en la última columna de la tabla de trabajo lo que se denomina índice de gravedad, que representa mediante una escala del 1 al 4 un valor que describe la gravedad de los posibles efectos detectados. El valor 1 representaría un suceso sin efectos adversos; el 2 efectos que no requieren parada del sistema; el 3 riesgos de cierta importancia que requieran parada normal y el 4 peligro inmediato para el personal e instalaciones, por lo que se requiere parada de emergencia. En este caso, el análisis se denomina Análisis del Modo de Fallos, Efectos y Criticidad, FMECA (AMFEC).

Como contrapeso a los riesgos, las medidas de seguridad reducen la probabilidad de perdida o daño una vez que ocurre el evento. Muchas veces estas medidas llegan incluso a eliminar el riesgo casi por completo.

De la misma manera como se procedió para cuantificar las perdidas se procederá al cálculo de los costos de instalar y mantener medidas de seguridad.

Existen dos posibilidades, la primera consiste en que el evento siga ocurriendo con la misma probabilidad (frecuencia) y que las medidas de control únicamente reduzcan la pérdida esperada.

Si el costo de instalar el control, digamos es "s" es menor a "C" (pérdida esperada si ocurre el evento), esto quiere decir que es rentable para la empresa introducir las medidas de seguridad requeridas.

Si por el contrario "s" es mayor a "C", no es conveniente instalar los controles. Es importante determinar con que frecuencia se incurrirá en el gasto "s" ya que si es menor a la probabilidad con la que ocurre el evento, posiblemente los gastos sean compensados.

El segundo caso, es cuando al instalar medidas de seguridad se reduce significativamente la probabilidad de ocurrencia del evento en cuestión. En este caso debe calcularse la nueva probabilidad de ocurrencia, por ejemplo "p", así como el costo de los controles, "s" y al igual que en el caso anterior, determinar si la diferencia entre implantar o no las medidas produce beneficios para la empresa.

Mapeo de riesgos "Risk Mapping"

El Mapeo de Riesgos es una herramienta sistemática y efectiva, apoyada en el perfil de riesgos, con la que un administrador de riesgos o encargado de la seguridad, se puede comunicar y hacer entender por los inversionistas o socios de un corporativo.

El Mapeo de Riesgos consiste en la creación de una gráfica que describe los escenarios a los que las Empresas de un Corporativo están expuestas, manejados de manera integral y nunca de forma aislada.

En la gráfica o perfil se deben visualizar los riesgos según los niveles de probabilidad y niveles de severidad.

La identificación de riesgos: consiste en visitar las diferentes áreas que conforman el negocio o planta, para visualizar y colectar varios escenarios de todo tipo (perspectiva total del riesgo a 360°). Una vez identificadas estas áreas de oportunidad, serán agrupadas y evaluadas, permitiendo determinar el impacto operacional que estos riesgos representan de manera particular (ubicación/planta) y de manera global (grupo/corporativo).

Las agrupaciones o "clusters", son grupos de observaciones representativas de riesgos definidos, tales como accidentes de trabajo, fallas en instalaciones eléctricas, sistemas de protección contra incendio, fallas de comunicación entre áreas, entre otras.

La identificación y evaluación, darán la pauta para enfocar los esfuerzos y toma de decisiones para la administración y control/prevención de pérdidas.

En resumen el Mapeo de Riesgos resulta ser una herramienta vital para la apreciación de riesgos, donde el objetivo es evitar el riesgo ó riesgos mayores ó catastróficos de cualquier empresa, el factor "sorpresa", e identificar las necesidades para todo el corporativo, además, aplicando esta metodología se permitirá la transparencia y una mejor atención y distribución de recursos de prevención de pérdidas (*Strategic Risk Management*).

Comparación entre análisis de riesgo cuantitativo y análisis de riesgo cualitativo

Muchas veces se tiene la idea de que un análisis cuantitativo, en cualquier área de estudio es superior a un análisis de tipo cualitativo, sin embargo, esta información no siempre es correcta, en el caso del análisis de riesgos, los dos enfoques son necesarios para determinar cuál es el tratamiento más adecuado a los riesgos y necesidades de la empresa.

Los métodos cuantitativos tienen la gran ventaja de que el proceso en si despierta una conciencia de peligros existentes y desconocidos hasta el momento. Sin embargo, la desventaja que tiene es que

pueden resultar muy costosos en tiempo y recursos. Además algunas veces pueden interpretarse erróneamente los resultados y tomar decisiones equivocadas.

En cambio los métodos cualitativos implican únicamente un conjunto básico de controles, elaborado con los resultados de experiencias anteriores. En este sentido la organización puede sustituir a través de una auditoria, el análisis cuantitativo de riesgos con solo identificar las amenazas principales a su equipo. La ventaja de realizar un análisis de este tipo es que hay un ahorro considerable en tiempo y recursos. Muchas veces este ahorro puede utilizarse para instalar los controles necesarios.

Generalmente es obligado incluir un enfoque cuantitativo para la instalación y administración un equipo de cómputo grande y centralizado. Este argumento se basa en el supuesto de que comúnmente una falla o daño en un sistema centralizado tiene efectos sobre todas las partes del sistema. Además, los riesgos que sufre un sistema centralizado hace que todo el equipo este expuesto, por esta razón es necesario contar con una cuantificación precisa de todas las pérdidas probables, pues sin duda que el impacto económico es de gran importancia. Por otro lado, en el caso una red distribuida con pequeños subsistemas es suficiente con un enfoque cualitativo pues las dimensiones permiten fragmentar el riesgo y los problemas pueden ser localizados fácilmente.

Para seleccionar el procedimiento de análisis a seguir en cada caso, se deberá partir de las características y necesidades propias de las empresas, de sus programas de seguridad y protección, de lo sofisticado de sus centros de cómputo y de sus recursos económicos para invertir. Pero si no existen limitaciones económicas es deseable considerar la aplicación de análisis de riesgo tanto cuantitativo como cualitativo pues a la larga los dos se complementan y el incluir ambos en cada programa de evaluación nos permitirá tomar mejores decisiones y llegar a soluciones más acertadas en cada proyecto.

2.4 Tratamiento del Riesgo

Después de valorar y priorizar los riesgos y dependiendo del nivel de exposición, se debe determinar la opción de tratamiento que más conviene aplicar en cada caso. El tratamiento de riesgos incluye la identificación de la gama de opciones de tratamiento del riesgo, la evaluación de las mismas, la preparación de planes de tratamiento de riesgos y su posterior implementación.

Las opciones de tratamiento que se relacionan a continuación no son mutuamente exclusivas ni serán apropiadas en todas las circunstancias:

Evitar el riesgo: Se decide, en situaciones permitidas, no proceder con servicios, procesos y/o actividades que podrían generar riesgos inaceptables, buscando con ello eludir el riesgo inherente asociado a esos objetos. Es siempre la primera alternativa que debe considerarse.

Minimizar o reducir el riesgo: La organización decide prevenir y/o reducir el riesgo. Si el riesgo no se puede evitar porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible, el cual debe ser compatible con las actividades de las áreas. Se consigue mediante la optimización de los procedimientos y la implementación de controles.
Cuando la empresa o la institución, reconoce un riesgo dentro de las actividades de la misma, pero decide definir nuevos controles o medidas de seguridad orientadas a minimizar el grado de

exposición al riesgo identificado. Esto significa invertir recursos en beneficios preventivos, logrando una mayor tranquilidad y confianza en la realización de nuestras actividades.

Las operaciones de la misma en caso de ocurrir el evento adverso, no afectarán seriamente, pues las medidas preventivas y correctivas que se incorporaron minimizarán los efectos negativos. Hemos puesto en marcha un rudimentario Plan de contingencia.

Reducir la probabilidad de ocurrencia: Prevención del riesgo a través de la implementación de acciones tendientes a controlar su frecuencia o probabilidad.

Reducir las consecuencias o mitigar el riesgo: reducción del riesgo a través de la implementación de acciones o medidas de control dirigidas a disminuir el impacto o severidad de las consecuencias del riesgo si éste ocurre.

Atomizar el riesgo: La organización decide segmentar el objeto sobre el cual recae la amenaza de riesgo o, distribuir la localización de los objetos.

Transferir el riesgo. La organización decide traspasar o trasladar riesgos a otra parte o lugar de manera total o parcial. Las transferencias parciales son conocidas como compartir el Riesgo. La distribución o localización del riesgo en diversos lugares se conoce como dispersión o atomización del riesgo. En algún caso, se requerirá el apoyo de una Compañía de Seguros.

Transfiriendo a estas organizaciones los riesgos, estamos enfrentando los riesgos con ventaja. Sin embargo no se trata de olvidar, que en el ambiente de informática (sistemas de cómputo, que el objetivo de este trabajo), de una empresa no puede soportar un periodo largo entre el momento del siniestro y la reposición de los bienes perdidos (información).

Asumir el riesgo: La organización decide aceptar los riesgos como ellos existen en la actualidad y establece políticas o estrategias financieras apropiadas para su tratamiento. En este caso la organización considera que el riesgo residual actual es de nivel bajo y decide convivir con él, aceptando la pérdida probable, con lo cual las estrategias de prevención se vuelven esenciales.

Cuando la empresa o el corporativo reconoce un riesgo dentro de las actividades de su operación, sin embargo al efectuar un estudio de costo-beneficio encuentra que las pérdidas estimadas, en caso de que se llegue a consumar el evento esperado, no justifican la incorporación de mas controles o mas medidas de seguridad, por el tamaño de la inversión que se tuviera que hacer, se dice que se ha decido asumir el riesgo.

Cualquiera que sea la alternativa que tomemos, es necesario realizar evaluaciones periódicas que nos muestren los grados de exposición y cambios que se estén dando, para efectuar las correcciones y adecuaciones que se requieran.

Consideramos que lo ideal es adoptar una alternativa mixta, es decir minimizar ciertos riesgos utilizando seguridad de la información y transferir otros asegurándose.

Para el monitoreo y la revisión, pocos riesgos permanecen estáticos. Por lo tanto, riesgos y la efectividad de sus medidas de control necesitan ser monitoreados continuamente para asegurar que circunstancias cambiantes no alteren las prioridades.

Revisiones progresivas son esenciales para asegurar que los planes de tratamiento permanecen relevantes. Los factores que afectan la probabilidad y la consecuencia de un resultado pueden cambiar, al igual que los factores que afectan la viabilidad o el costo de las opciones de tratamiento.

La prevención como la primera forma de evitar situaciones que pongan en dificultades económicas a las empresas.

Las medidas de prevención en todos los ámbitos sin duda constituye, la primera forma de estar preparado para enfrentar cualquier situación adversa que pudiera presentarse en la vida activa de cualquier empresa, institución o negocio.

En todo caso se debe hacer un análisis cuidadoso de los diferentes factores que pueden dañar un negocio, esto quiere decir evaluar las distintas posibilidades que se pueden presentar durante la vida de una empresa en todos sus aspectos y tomar las medidas preventivas para cada riesgo que pudiera presentarse.

Seguramente que los aspectos físicos son los primeros que se revisaran, pueden ser la construcción, ubicación del inmuebles, extintores y sistemas contra incendio, sistemas de monitoreo para toda la planta, alarmas, servicio de vigilancia humana, canina e incluso robótica.

Otro aspecto en el que se debe poner mucha atención serán los de acceso a las instalaciones, no solo en el sentido de no permitir que cualquiera entre a las instalaciones, sino que los que entren, sean personas de confianza que no atenten contra las instalaciones, principalmente cuidar los centros informáticos y de almacenamiento de la documentos y sistemas vitales para la empresa.

Las herramientas de identificación, medición y cálculo del riesgo, nos dan los elementos para describir las diferentes estrategias de prevención, dentro del marco de los riesgos de mayor incidencia a los que como país estamos expuestos, estudio que se presentará en el siguiente capítulo, haciendo hincapié en las necesidad de crear una cultura de la prevención y de la seguridad informática.

Capítulo 3

Estrategias de Prevención

3.1 Desastres de probable ocurrencia en México.

Cuando se piensa en desastre, nos viene a la mente una infinidad de posibles eventos todos de carácter destructivo, que causan pérdidas económicas, materiales, pérdidas de información y sin olvidar las pérdidas humanas que son quizás las que más sentimos sobre todo cuando sucede con personas conocidas o cercanas a nosotros.

En el capítulo anterior se esquematizaron conceptos sobre el tratamiento del riesgo, cuyos orígenes como ya se expuso, son provenientes de causas de orden natural y las generadas por las actividades humanas o una combinación de ambas. Pero en todos los casos los grados de severidad y de frecuencia suelen ser de diferente índole. Consideremos los que se presentan una mayor recurrencia en nuestro país.

Básicamente, los esquemas conceptuales a través de los que se maneja el Sistema Nacional de Protección Civil (SINAPROC) consideran a los desastres como un proceso que debe comprender tres componentes identificables, a saber: agentes perturbadores, agentes afectables y agentes reguladores.

Definiendo como:
Agente perturbador: Al fenómeno de origen natural o humano que puede alterar el funcionamiento normal de los agentes afectables y producir en ellos un estado de desastre.
Agente afectable: Cuando el hombre y su entorno físico donde se desarrolla, se ven alterados por el agente perturbador.
Agente regulador: Es la organización que constituye las acciones o normas para prevenir, mitigar o controlar los efectos destructivos de un agente perturbador.

Tales desastres o tragedias provienen de diferentes orígenes, pero sin duda todos con un alto grado de destrucción y con lamentables consecuencias en todos los ámbitos de la vida del país afectando aspectos económicos y sociales.

Al igual que cualquier otra, las empresas de telecomunicaciones están expuestas a los riesgos de origen natural, o por fallas humanas, atentados deliberados con el afán de destruir, o por reacciones de la propia naturaleza a los mismos daños que la humanidad en su conjunto le ha ocasionado por el uso y abuso de los recursos naturales, sustancias y armas de destrucción masiva que han modificado la geografía de los bosques, las aguas, los glaciares y las grandes concentraciones humanas.

Tan solo por su ubicación dentro de zonas de riesgo las empresas están expuestas cada vez más al alto índice de destrucción de huracanes, tornados, incendios, inundaciones, sequías, vientos tempestuosos, entre otros fenómenos naturales, así como a la cada vez más frecuente presencia de atentados terroristas, accidentes en industrias, accidentes aéreos y todo tipo de accidentes donde el hombre ha intervenido voluntaria o involuntariamente.

De manera similar que otros países están expuestos a sufrir tragedias con las consecuentes pérdidas señaladas, México y las empresas instaladas en su territorio (DIRECTV tiene su base de operaciones en la Cd. De México), se encuentran expuestos a sufrir los mismos estados de emergencia por situaciones naturales y accidentes por fallas en actividades del hombre. Meditemos pues en los grandes peligros que afectan a grandes sectores de la población e instituciones públicas y privadas,

las cuales sufrirían tropiezos económicos desde ligeras pérdidas financieras, hasta la perdida total y cierre de las empresas.

Particularmente la Ciudad de México, por su situación geográfica esta expuesta a fenómenos destructivos y de desastres, principalmente provocados situaciones de origen sísmico; para muestra mencionaremos el movimiento telúrico del 19 de septiembre de 1985 y sus terribles consecuencias que todos conocemos, además de inundaciones, incendios y explosiones, entre otros.

Peor aún si consideramos que en ella se localizan los principales centros educativos, hospitalarios, comerciales, financieros, políticos, e incluso turísticos, lo que hace los alcances de los desastres aún mas elevados y costosos.

Los desastres que pueden presentarse en nuestro país de acuerdo a la clasificación establecida por el Sistema Nacional de Protección Civil (SINAPROC), es la siguiente:

Químicos: Se refieren al desarrollo industrial y tecnológico y al uso de diversas formas de energía, entre los que podemos citar:

- Contaminantes
- Envenenamientos
- Incendios
- Explosiones
- Radiaciones

Geológicos: Se refieren a la actividad de las placas tectónicas, entre los que podemos citar:

- Sismos y consecuencias como tsunamis
- Erupciones volcánicas
- Hundimiento del suelo
- Grietas

Hidrometereológicos: Se derivan de la acción violenta de los agentes atmosféricos, huracanes, inundaciones entre otros, entre los que podemos citar:

- Lluvias
- Tormentas de granizo y eléctricas
- Inundaciones
- Temperaturas extremas
- Sequías
- Vientos

Sanitarios: Se refiere a la población y sus medidas higiénicas y de salud, entre los que podemos citar:

- Epidemias
- Plagas

Socio-organizativos: Se refieren a las normas de las actividades de concentraciones humanas, entre los que podemos citar:

- Explosión demográfica
- Fallas humanas
- Disturbios sociales

- Delincuencia
- Accidentes
- Guerras
- Alcoholismo y drogadicción
- Interrupción de servicios

En México a manera de ejemplificar un fenómeno provocado por el hombre, podemos señalar el ataque terrorista contra Banamex-Citigroup, el 8 de agosto de 2001 en tres sucursales de Banamex, cuando en los miembros de las Fuerzas Armadas Revolucionarias del Pueblo (FARP) estallaron artefactos de fabricación casera.

Otro ejemplo en el caso de México e incluso situación que se presenta en todo el mundo, es que a consecuencia del sobrecalentamiento de la tierra, se presenta el fenómeno de *"El Niño"* que hace su aparición a intervalos de dos a siete años y se caracteriza porque la superficie del mar y la atmósfera sobre él presentan una condición anormal de temperatura durante un período que va de doce a dieciocho meses.

"El Niño", no solamente hace su aparición en corrientes oceánicas cálidas en las costas de América, pues también genera alteración del sistema global océano-atmósfera que se origina en el Océano Pacífico Ecuatorial (es decir, en una franja oceánica cercana al Ecuador), generalmente durante un periodo comprendido entre diciembre y marzo. El Jefe del departamento de Comunicación del CICESE (Centro de Investigación Científica y Estudios Superiores de Ensenada), señala que *"en términos prácticos, la ocurrencia de El Niño significa que muchas regiones normalmente húmedas, como Indonesia, llegan a ser secas, mientras que las áreas normalmente secas, como las de la costa Oeste de América, se humedecen con precipitaciones intensas"*[1].

3.2 Sistemas de Seguridad

3.2.1. Información

Definimos como dato a la unidad mínima con un valor significativo o representativo.
Información: "*Es una agrupación de datos que tiene un significado específico más allá de cada uno de los componentes y tendrá un sentido particular según como y quién lo procese*".

Existe información del tipo pública y privada. Si hablamos del tipo pública, se entiende que la misma puede ser visualizada por cualquier persona, pues esta se hace del conocimiento de todos a través de los medios de comunicación o simplemente no tiene ninguna restricción; en tanto que aquella que es privada sólo puede ser visualizada por un grupo selecto de personas que trabaja y hace uso de ella dentro de la empresa, por lo que se deben maximizar esfuerzos para preservarla como confidencial, considerando que la información cuando es conocida por persona ajenas, puede poner en una situación critica la continuidad operativa del negocio o institución, esto significa que es sensible a cualquier divulgación, pues se considera un activo con valor en sí misma.

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse accidentes y ciertas personas con

[1] *www.cicese.mx*

intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información.

3.2.2. Características de la Información

Integridad: Es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema. El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo, información de censos, indicadores económicos o sistemas de transacciones financieras.

Disponibilidad u operatividad: Es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria. El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, protección de la vida y predicción de huracanes.

Confidencialidad o privacidad: Es la necesidad de que la información sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño puesto que nadie vigila el uso adecuado de esta. El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, si hablamos de datos que se van a difundir en un momento determinado, como información personal e información comercial patentada.

El control: Permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información validando el emisor de la misma, para evitar suplantación de identidades.

Otros conceptos como protección a la réplica, no repudio, consistencia, aislamiento y auditoría, se desprenden de los antes citados, por lo que no abundaremos en estos.

3.2.3. Sistemas de Seguridad de la Información

Sistemas de seguridad
Son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de daño sobre: las computadoras de sus sistemas y los elementos físicos asociados con éstos (edificación, impresoras, discos, cables, dispositivos de interconexión, entre otros.), el software y la información almacenada en tales sistemas y los usuarios del sistema.

Objetivos
Informar al mayor nivel de detalle a los usuarios, empleados y gerentes de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización.

Proporcionar los criterios para adquirir, configurar y auditar los sistemas de computación y redes para que estén en concordancia con las políticas de los sistemas de seguridad.

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación.

Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos y este documento se centra en dichos principios.

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo vital de los sistemas. Las actividades que se describen en este documento suelen requerir actualizaciones periódicas o las revisiones correspondientes. Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian considerablemente o cuando hay que modificar las leyes y normas organizativas. Éste es un proceso interactivo. Nunca termina y debe revisarse y probarse con periodicidad.

Metodología para la definición de un sistema de seguridad

A continuación, se muestra una metodología para definir un sistema de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque. La metodología se basa en los distintos tipos de amenazas, métodos de ataque y puntos vulnerables.

Sistema de Seguridad

Fase 1. Predecir ataques y evaluar riesgos

Para cada tipo de amenaza
Para cada tipo de método de ataque

<u>Estrategia proactiva</u>
Predecir posibles daños
Determinar vulnerabilidades
Minimizar vulnerabilidades
Implementar plan y elaborar directivas y controles de seguridad
Elaborar planes de contingencia

<u>Estrategia reactiva</u>
Evaluar daños
Determinar la causa del daño
Reparar daños
Implementar plan y elaborar directivas y controles de seguridad
Documentar y aprender
Implementar plan de contingencia

Fase 2. Examinar resultados y hacer simulación

Fase 3. Examinar eficacia directiva
Fase 4. Ajustar directiva en consecuencia

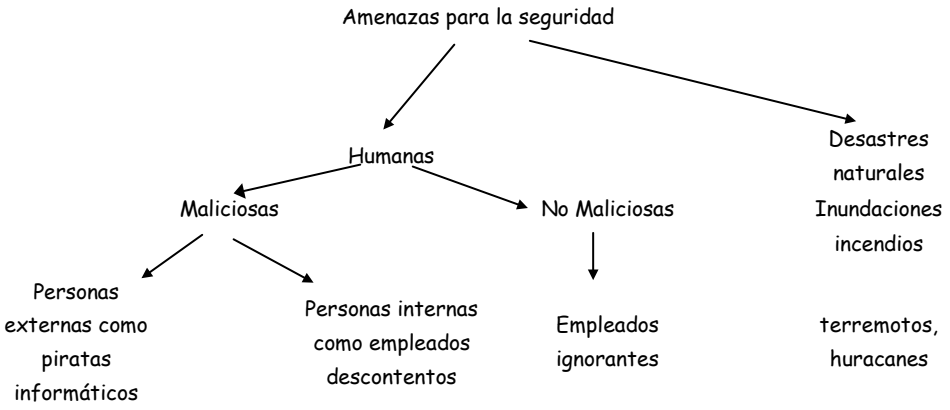
Con el objeto de describir cada una de las anteriores fases, se considera:

Fase 1. Predecir posibles ataques y analizar riesgos.
La primera fase de la metodología es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado.

Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para comprometer los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad. El conocimiento de estos tres elementos de los ataques ayuda a predecir su aparición e, incluso, su duración o ubicación. La predicción de los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas + Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

Para cada tipo de amenaza
Considere todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente ilustración clasifica las distintas amenazas a los sistemas.



Amenazas como empleados ignorantes o descuidados y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización.

Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias proactivas o reactivas.

Para cada tipo de método de ataque
Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los

agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza. De nuevo, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores.

La siguiente es una lista breve de estas técnicas:

- Ataques de denegación de servicio
- Ataques de invasión
- Ingeniería social
- Virus
- Gusanos
- Caballos de Troya
- Modificación de paquetes
- Repetición de paquetes
- Adivinación de contraseñas
- Interceptación de correo electrónico

Estrategia proactiva

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema y los puntos vulnerables que explota. Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques. Éstos son los tres pasos de la estrategia proactiva:

Determinar el daño que causará el ataque.

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, utilice un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques. Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales. No todos los ataques causan el mismo daño. Éstos son algunos ejemplos de las pruebas que hay que ejecutar:

Simular un ataque con virus a través de correo electrónico en el sistema del laboratorio y ver el daño que ha provocado y cómo recuperarse de la situación.

Utilizar la ingeniería social para adquirir un nombre de usuario y una contraseña de algún empleado ingenuo y observar cómo se comporta.

Simular lo que ocurriría ante un incendio en la sala de servidores. Mida el tiempo de producción perdido y el tiempo necesario para la recuperación.

Simular un ataque de virus dañino. Anote el tiempo necesario para recuperar un equipo y multiplique ese tiempo por el número de equipos del sistema infectados para averiguar el tiempo de inactividad y la pérdida de productividad.

También es aconsejable implicar al equipo de respuesta a incidentes ya mencionado ya que es más probable que un equipo, en lugar de una sola persona, consiga localizar todos los tipos distintos de daños que se han producido.

Establecer los puntos vulnerables y las debilidades que explotará el ataque.

Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes.

Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo ya que en los diferentes factores se superponen para diferentes ataques. Este modelo puede ser útil al determinar las áreas de vulnerabilidad que plantean el mayor riesgo para la empresa. También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. La ponderación de los riesgos y los costos forma parte de un análisis de riesgos del sistema que se explica en el documento técnico acerca del diseño de la seguridad.
Las directivas y controles de seguridad no serán, en ningún caso, totalmente eficaces al eliminar los ataques. Éste es el motivo por el que es necesario desarrollar planes de recuperación y de contingencia en caso de que se quebranten los controles de seguridad.

Implementar plan y elaborar directivas y controles de seguridad
El establecimiento de un conjunto eficaz de directivas y controles de seguridad requiere el uso de un método para determinar los puntos vulnerables que existen en nuestros sistemas y en las directivas y controles de seguridad que los protegen. El estado actual de las directivas de seguridad informática se puede determinar mediante la revisión de la siguiente lista de documentación. La revisión debe tomar nota de las áreas en las que las directivas son deficitarias y examinar los documentos que haya:

- Directiva de seguridad informática física, como los controles de acceso físico.
- Directivas de seguridad de la red (por ejemplo, las referentes al correo electrónico y a Internet).
- Directivas de seguridad de los datos (control de acceso y controles de integridad).
- Planes y pruebas de contingencias y de recuperación de desastres.
- Conocimiento y formación en seguridad informática.
- Directivas de administración y coordinación de la seguridad informática.
- Otros documentos que contienen información importante como:
- Contraseñas del BIOS de los equipos.
- Contraseñas para la configuración de enrutadores.
- Documentos de control de acceso.
- Otras contraseñas de administración de dispositivos.

Elaborar plan de 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 comerciales 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 (es el proverbial "Plan B").

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. El plan de contingencia debe:

- Determinar quién debe hacer qué, en qué momento y en qué lugar para que la organización siga funcionando.
- Ensayarse periódicamente para mantener al personal informado de los pasos de la contingencia actual.
- Abarcar la restauración de las copias de seguridad.
- Explicar la actualización del software antivirus.
- Abarcar el traspaso de la producción a otra ubicación o sitio.

Los siguientes puntos resaltan las distintas tareas que deben evaluarse para desarrollar un plan de contingencia:

- Evaluar las directivas y controles de seguridad de la organización para utilizar todas las oportunidades destinadas a reducir los puntos vulnerables. La evaluación debe tratar el plan y los procedimientos de emergencia actuales de la organización y su integración en el plan de contingencia.
- Evaluar los procedimientos actuales de respuesta ante emergencias y su efecto en el funcionamiento continuo de la organización.
- Desarrollar respuestas planeadas a ataques, integrarlas en el plan de contingencia y anotar hasta qué punto son adecuadas para limitar el daño y reducir el impacto del ataque en las operaciones de procesamiento.
- Evaluar procedimientos de copia de seguridad, que incluyan la documentación más reciente y pruebas de recuperación de desastres, para evaluar su adecuación e integrarlos en el plan de contingencia.
- Evaluar planes de recuperación de desastres para determinar su adecuación con el fin de proporcionar un entorno operativo temporal o a largo plazo. Los planes de recuperación de desastres deben incluir la prueba de los niveles de seguridad necesarios, con el fin de que el personal de seguridad pueda ver si siguen exigiendo la seguridad en todo el proceso de recuperación o en operaciones temporales y el traspaso de la organización otra vez a su sitio de procesamiento original o a un sitio nuevo.
- Redactar un documento detallado que describa los distintos señalamientos en las tareas anteriores. El documento debe mostrar:
  - Todos los casos para probar el plan de contingencia.
  - El impacto de las dependencias y la ayuda planeada fuera de la organización y, las dificultades que se tendrán para la obtención de los recursos esenciales en el plan.
  - Una lista de prioridades observadas en las operaciones de recuperación y el fundamento para establecerlas.

Estrategia reactiva

La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan.

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 él.

Evaluar el daño

Determine el daño causado durante el ataque.

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 puedan proseguir las operaciones comerciales y la productividad normales.

Determinar la causa del daño

Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Revise los registros del sistema, los registros de auditoria y las pistas de auditoria. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

Reparar el daño

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de restauración. El equipo de respuesta a incidentes también debe poder controlar el proceso de restauración y recuperación y ayudar en este último.

Documentar y aprender

Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

Implementar un plan de contingencia

Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrolle un plan apropiado basado de la documentación del paso anterior.

Fase 2. Examinar resultados y hacer simulación

El segundo paso importante en la estrategia de seguridad es revisar los descubrimientos establecidos en el primer paso (predicción del ataque). Tras el ataque o tras defenderse de él, revise su resultado con respecto al sistema. La revisión debe incluir la pérdida de productividad, la pérdida de datos o de hardware y el tiempo que se tarda en recuperarlos. Documente también el ataque y, si es posible, haga un seguimiento del lugar en el que se originó, qué métodos se utilizaron para iniciarlo y qué puntos vulnerables se explotaron. Para obtener los mejores resultados posibles, realice simulaciones en un entorno de prueba.

Fase 3. Examinar eficacia de directiva

Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros.

Fase 4. Ajustar directiva en consecuencia
Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia; las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes. Todas las directivas deben seguir las reglas e instrucciones generales de la organización. Por ejemplo, el horario laboral puede ser de 8 a.m. a 6 p.m. Podría existir o crearse una directiva de seguridad que permita a los usuarios conectarse al sistema solamente durante este horario.

3.3 Plan de Contingencia y su utilidad

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Hay dos ámbitos que vamos a analizar. El primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas. El segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está funcional y actualizado.

3.4. Plan de Contingencia: Origen, Elementos y Personal

Orígenes
Durante los últimos años los planes de contingencia se han transformado en un tema de "no interés ni actividad" a uno de los más importantes en el mundo del procesamiento de datos.
La pérdida del poder de cómputo puede ser causada por muchas cosas. Ocurrencia de desastres tales como incendio, inundación y falla de electricidad son representativas de las amenazas reales de un centro de cómputo. Ejemplos de otros desastres incluyen: sabotaje, descuido y disturbios civiles. La probabilidad de que ocurran tales eventos puede ser fuertemente reducida a través de un efectivo programa de seguridad. De cualquier forma ya no puede lograrse la seguridad total, es muy importante tener la capacidad de recuperarse de una contingencia. Sin esta capacidad una empresa dependiente del procesamiento de datos está asumiendo un gran riesgo de destrucción.

Se observa una tendencia permanente de crecimiento de desastres. Existen tres principales causas de la elevada y creciente gravedad de los desastres en los asentamientos humanos:

La primera surge de la diversificación de los tipos de peligros a los cuales está propensa la comunidad, así como del crecimiento de las intensidades de sus manifestaciones, que son consecuencia de nuevos fenómenos destructivos de origen tecnológico, típicos en asentamientos humanos con alta concentración de industrias y transporte

La segunda causa se relaciona con la notable vulnerabilidad de las grandes urbes, resultado de la alta densidad y del crecimiento de la población expuesta al peligro, así como de la enorme complejidad de los servicios humanos y sistemas de subsistencia que las componen.

La tercera consiste en la ineficiencia de la gestión o regulación de los desastres. Esto se detecta, por un lado, en la parcialidad y el carácter aislado de las medidas para el combate de los desastres, por el otro, se observa en la ineficiente ejecución de las medidas disponibles, debido principalmente a la falta de una adecuada organización de la sociedad, así como la insuficiente planeación para enfrentar los desastres.

No obstante, a pesar de que no se pueden prevenir algunos fenómenos destructivos de origen natural, la prevención de un desastre depende del esfuerzo de la sociedad.

Elementos
El diseño e implantación de un plan de contingencia, debe considerar los siguientes elementos:

- Los riesgos y los porcentajes de factibilidad a los que se está expuesta la organización
- La asignación de responsabilidades al personal
- La identificación de las aplicaciones de mayor importancia dentro de la producción de datos
- La especificación de alternativas de respaldo
- La definición de medidas y el tiempo previsto para la recuperación
- La integración de prácticas de mantenimiento y entrenamiento y pruebas del plan

Es importante destacar que un plan de contingencia no evita los desastres, sino que provee los medios para salvaguardar al máximo los recursos del área de procesamiento electrónico de datos y reducir así, las posibles pérdidas que resultan de estos desastres.

Una de las claves en el desarrollo de un plan de contingencia, estriba en la evaluación de posibles riesgos que envuelven el ambiente informático.

Personal
Para definir el personal que debe participar en el programa, existen dos opciones:
a) Contratar los servicios de un consultor externo
b) Que el plan de recuperación de desastres sea elaborado por el personal de la misma institución.

En ambos casos, existen ventajas y desventajas, como se lista a continuación.

Opción a) Contratar a consultores externos

Ventajas:

- Se dispone de una persona, incluso de todo un equipo dedicado exclusivamente al desarrollo de este proyecto.
- Los consultores externos, poseen conocimientos especializados que pueden facilitar el desarrollo del plan en menor tiempo.
- Los consultores saben como se hace un plan de contingencia y además saben quien es quien, dentro de la industria de seguridad de la información.

- Los consultores externos tienen otra perspectiva del proyecto y se percatan de requerimientos que podrían ser pasados por alto por una persona de la empresa.
- Los consultores generalmente, entregan el plan de recuperación con un acuerdo en mantenimiento que consideran las pruebas de entrenamiento y actualización del plan.

Desventajas:

- Una gran desventaja al contratar un consultor externo especializado en el tema, será el precio, mismo que no todas las empresas pueden pagar.

- El consultor al no contar con el conocimiento suficiente de la empresa, propondrá soluciones que podrían no considerar toda la problemática interna.

Opción b) Que el plan sea elaborado por el personal de la misma institución.

Ventajas:

- El desarrollador del plan de contingencia, al formar parte de la empresa, tendrá un acceso más rápido y completo a la información que necesite.
- El desarrollador del plan, como miembro del área de sistemas, tendrá más facilidad para la realización del inventario de hardware y software, así como para la etapa de clasificación de los sistemas de acuerdo a su importancia y consecuentemente para la definición de los procedimientos de respaldo.
- Podrá conocer todas las medidas de seguridad de información implementadas en la empresa sin ninguna reserva.
- Puede utilizar el conocimiento que tiene acerca de sus compañeros de trabajo, para tratar de definir quienes son las personas más adecuadas para la conformación de los diversos equipos de contingencia.

Desventajas:

Por lo que respecta a las desventajas de que el plan sea desarrollado por los empleados de la empresa, podemos mencionar las siguientes:

- La persona encargada, en la mayoría de los casos no contará con la experiencia necesaria en el desarrollo de este tipo de proyectos.
- Igualmente en la mayoría de los casos, a la persona encarga de desarrollar el plan se le asignará esta tarea como una adicional a las que ya venía realizando. Es decir, no contará con el tiempo completo para dedicarlo a este proyecto. Por lo tanto el tiempo de desarrollo del plan será excesivamente largo, o bien, será terminado en el límite fijado pero la calidad del mismo no podría ser completamente satisfactoria.

Una vez identificados los factores de riesgo a los que estamos expuestos por el entorno en el que nos desarrollamos, además de reconocer la necesidad de estructurar estrategias de prevención que nos permita superar situaciones adversas y de desastre, nos corresponde identificar los diferentes metodologías para establecer planes de recuperación de desastres y los pasos a desarrollar en la consecución del mismo, buscado hacer una adaptación adecuada a las necesidades de nuestra empresa, dentro de las políticas de operación de la misma. En consecuencia en el siguiente capítulo se tratarán las metodologías estudiadas y el método propuesto para nuestro caso práctico.

Capítulo 4

Desarrollo del plan de recuperación.

4.1. Introducción al plan de recuperación de desastre.

A lo largo del tiempo se han generado algunos cambios en la forma en que las empresas manejan sus recursos de cómputo. Antiguamente exponíamos nuestros centros de cómputo en un aparador para mostrar la alta tecnología que manejábamos en nuestras empresas. Con el tiempo se ha convertido en lo siguiente: en primer lugar, al madurar los proyectos de informática, las empresas han pasado a depender cada vez más de sus equipos de cómputo. Por otro lado, hoy está claro que en las instalaciones de procesamiento electrónico está mucha de la información vital para la empresa. Esta información es tan vulnerable como los centros de cómputo, lo que ha provocado que en lugar de exponerlos, en esta época se busque la manera de protegerlos. En otras palabras, hoy tenemos mucho más que perder.

En el mundo de hoy, las organizaciones dependen del procesamiento datos para el flujo de información esencial, imaginemos qué pasaría si se quedara sin procesamiento de datos durante dos días, o durante una o dos semanas. Las operaciones comerciales podrán limitarse de tal manera que afectarán los activos corporativos, los movimientos comerciales, el servicio al cliente, el flujo de dinero, las oportunidades de inversión y el margen de competencia. Toda la organización es vulnerable en caso de que las operaciones de cómputo no funcionen.

Las amenazas son reales y un desastre puede provenir de diferentes agentes. Pueden ocurrir desastres naturales, fallas prolongadas de energía eléctrica, incendios, sabotajes y hasta explosión de bombas. Supongamos que se descompone una computadora; inicialmente, esto es solo un problema, pero si no puede ser reparada en un tiempo razonable, el efecto puede ser un desastre, sin importar cual haya sido la causa, un tiempo prolongado de suspensión de procesamiento de datos puede ser devastador, por eso debemos estar preparados.

Un plan de recuperación en caso de desastre (DRP) es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quién hace qué y cómo. Los objetivos de dicho plan son los de establecer, lo más pronto posible, el procesamiento de aplicaciones críticas (aquellas necesarias para la recuperación) para posteriormente restaurar totalmente el procesamiento normal. Un plan de recuperación en caso de desastre no duplica un entorno comercial normal, pero si minimiza la pérdida potencial de activos y mantiene a la empresa operando, al tomar acciones decisivas basadas en la planeación anticipada.

Dicho de otra manera, un plan de recuperación en caso de desastre es un programa de recuperación de la organización. La base de este plan es la decisión del negocio sobre qué aplicaciones del procesamiento de datos son las más importantes de proteger y recuperar. En otras palabras, el plan de recuperación no es solo un problema del área de sistemas sino de todo el negocio.

Un DRP es un plan escrito en el que se detallan las acciones, procedimientos y recursos que deben usarse durante un desastre que cause destrucción parcial o total de los servicios de cómputo. En este plan se define qué tareas son críticas, quién es el responsable de todos los aspectos del proceso de recuperación y cómo va a funcionar la organización mientras los sistemas están siendo reparados o transportados a una nueva instalación.

Un plan de recuperación completo mitigará los efectos de los desastres y permitirá una respuesta rápida, una transparencia del procesamiento critico a otras instalaciones y una eventual recuperación. La probabilidad de que ocurra un desastre puede verse reducida aplicando programas

de seguridad muy estrictos, sin embargo, no se puede pensar en la seguridad total, por lo que es necesario pensar en un plan de recuperación.
La preparación de un plan de recuperación proporciona a los directivos de una empresa una excelente oportunidad para aliviar o minimizar problemas potenciales que, en un momento dado, podrían interrumpir el procesamiento de datos.

El diseño de un plan completo de recuperación en caso de desastres, debe contemplar:

- Los riesgos y la probabilidad de ocurrencia de estos, a los que se esta expuesta la organización.
- La asignación de responsabilidades al personal, tanto en las actividades que se realizan durante la emergencia como en las de preparación y las de recuperación.
- La identificación de las aplicaciones de mayor importancia dentro de la producción de datos, para darles la seguridad necesaria.
- La especificación de alternativas de respaldo.
- La definición de procedimientos y políticas a seguir durante el momento de la crisis.
- La definición de medidas y el tiempo previsto para la recuperación.
- La integración de prácticas de mantenimiento en el plan y pruebas del mismo.

Es importante destacar que un plan de recuperación no evita los desastres, sino que provee los medios para salvaguardar al máximo los recursos del área de procesamiento electrónico de datos y reducir así las posibles pérdidas que resultan de esos desastres.

4.2 Relación costo beneficio.

Vender la idea de desarrollar el plan de recuperación de desastres a la alta dirección de la empresa puede ser un problema muy serio, tanto como el propio desarrollo del plan. Algunos de los problemas a los que se pueden enfrentar los directores de sistemas para obtener el apoyo de la alta dirección para este tipo de proyectos son los siguientes:

- *Falta justificar los costos del plan*: Esta crítica puede deberse a que no se justifican adecuadamente los riesgos de no tener el plan. Existen dos estrategias para resolver este problema:
  La primera es asignar un costo a cada hora de tiempo fuera del sistema
  La segunda es demostrar los beneficios de tal plan. Por ejemplo, el desarrollo de un buen plan de contingencia puede reducir los precios de los seguros; cierta estructura contra contingencias puede tener usos permanentes.

- *Si ya tenemos seguros, ¿Para que necesitamos el plan?*: Aún si existe consenso para desarrollar un plan en papel, es posible que la gerencia se resista a gastar dinero en su implementación. Una forma de responder a la pregunta anteriormente formulada es hacerles entender que los seguros pueden cubrir el costo del daño a la instalación, al hardware y a los medios de almacenamiento de la información. Incluso, los aseguradores pueden ofrecer seguros para la información misma, pero esto no lo es todo: mucho dinero no puede reconstruir nuestra información.

También se debe explicar a la dirección que este es un proyecto que ahorra dinero. Hay que lograr que la dirección tenga en mente varias cosas como costo de oportunidad, imagen corporativa, competencia e imagen del negocio. También hay que tomar en cuenta los diversos impactos de la contingencia como el económico, operacional, legal, la baja del servicio, la pérdida del negocio, entre otros.

4.3 Metodologías de desarrollo de Planes de recuperación.

A continuación se describen dos metodologías de desarrollo de planes de recuperación de desastres para sistemas de información tecnológica: la de William Toigo y la de Hewllet-Packard.

4.3.1 Metodología de William Toigo.

A continuación se describen las ocho etapas que componen esta metodología y se enuncian las diferentes tareas que la componen.

Etapa 1.- Definición y arranque

- Definir los objetivos del plan.
- Seleccionar la metodología.
- Obtener la aprobación de la dirección.
- Diseño de cuestionarios.

Etapa 2.- Análisis de riesgos

Recolección de datos:

- Inventario de hardware, software, aplicaciones, bases de datos y telecomunicaciones.
- Se obtiene el grado crítico de los sistemas tanto desde el punto de vista de los usuarios como el de los técnicos.
- Se determina la tolerancia a una falla o desastre. En términos prácticos la tolerancia puede ser expresada como un valor en pesos: es la pérdida de ingresos de la empresa, debido a una suspensión del procesamiento de cierta duración.
- Identificación de amenazas al procesamiento normal. Estas amenazas se pueden clasificar por su origen (naturales o causadas por el hombre), o simplemente observando los fenómenos que pueden causar una perdida del funcionamiento normal de los sistemas.

Análisis de datos:

- Aquí se realiza un análisis de todos los datos y se formula un conjunto de objetivos específicos para guiar el desarrollo de la capacidad de recuperación. El objetivo es determinar los riesgos que puedan ser eliminados y minimizar los efectos de los riesgos que no se puedan eliminar.

Etapa 3.- Protección de la instalación.

Apartado en donde se tratan varias estrategias comunes de prevención de desastres y de protección que se pueden poner en práctica para proveer la capacidad de evitar desastres:

- Detección de agua
- Protección contra fuego
- Eliminación de contaminantes y disminución de su impacto
- Falla el suministro eléctrico
- Control de acceso físico.

El diseñador del plan de contingencia debe conocer estos temas y su aplicación en la empresa ya que son factor que comúnmente originan desastres.

Etapa 4.- Almacenamiento fuera del site.

El almacenamiento fuera del site♦ incluye el análisis y clasificación de los datos, la revisión de los procedimientos de respaldo existentes, la evaluación y selección de un proveedor de espacio de almacenamiento y la formalización de agendas para el mantenimiento actualizado de datos en el site externo.

♦ Término definido en el Glosario.

Se requiere que la información correcta sea identificada, para conseguir esto se deben realizar las acciones siguientes:

- Identificar los sistemas críticos y vitales
- Definir las entradas y salidas de esos sistemas
- Almacenar respaldos de los programas, sistemas y software de la base de datos de producción.
- Identificar la documentación requerida para restaurar los sistemas e información; esto incluye inventarios, manuales técnicos y de usuario, formas impresas, copias del plan de recuperación de desastres, entre otros

Etapa 5.- Estrategia de respaldo de sistemas.

Aquí se hace uso de los resultados de la etapa del análisis de riesgos. Hay que saber:

- Qué aplicaciones son críticas o vitales
- Cuál es la configuración mínima del hardware para correr los sistemas
- Cuántos usuarios tienen los sistemas
- Cuáles son los requerimientos de la empresa

Existen muchas estrategias de respaldo de los sistemas de computo, debe analizarse cada caso para determinar cuál es la más conveniente.

Etapa 6.- Estrategia de respaldo de redes.

El diseñador del plan debe entender las redes de comunicaciones que están alrededor de los procesadores.

Una actividad preeliminar consiste en revisar el análisis de riesgo para identificar dependencias en redes, el grado crítico de los servicios de red y el nivel mínimo de servicio requerido para la continuidad del negocio.

Existen varias opciones para recuperar las redes que han tenido fallas:

- Para sistemas de comunicación interna: es importante adquirir el software para diagnostico y reparación de problemas de redes, en caso de falla en el conmutador hay dos opciones: (1) instalar líneas directas para las funciones dependientes de las comunicaciones y (2) comprar un segundo conmutador y tenerlo de respaldo.
- Para equipo periférico de las computadoras: tener hardware redundante almacenado para reemplazo inmediato cuando falla un dispositivo crítico.
- Para redes de área local: para proteger estas redes contra pérdidas catastróficas debido a fallas de nodos, pérdida de la integridad de los medios de comunicación, o factores relacionados con el software, la solución reside en el software usado para crear y controlar la red.

Además de las fallas de redes, otro escenario de contingencia que puede ser considerado por el diseñador del plan de recuperación de desastres, consiste en la falla de la compañía telefónica. Las estrategias para la recuperación de esta contingencia son muy caras y consisten básicamente en instalar o contratar otros medios de comunicación alternativos al teléfono, u obtener los servicios de una segunda compañía telefónica.

Etapa 7.- Toma de decisiones en caso de emergencia.

Se refiere a tres proyectos fundamentales para la recuperación:

- Evacuación
- Recuperación
- Reinstalación de las actividades normales.

Se deben considerar los siguientes puntos:

a) Es imposible predecir todos los escenarios y tomar todas las decisiones por adelantado; por eso resulta inútil diseñar procedimientos muy rígidos.

b) El plan es necesario para coordinar las acciones de recuperación ya que sin él, sería más lenta y el desastre causaría daños mayores a las empresas.

c) En esta fase se deben diseñar los equipos que llevaran a cabo el plan de recuperación.

d) Se debe hacer un directorio telefónico de los equipos que componen el plan y de todas las que tengan relación con el plan.

e) Pueden identificarse uno o varios diagramas de flujo de manejo de emergencias que describan la secuencia en la cual se realizarán las tareas de recuperación

Etapa 8.- Mantenimiento y pruebas del plan.

El plan de recuperación de desastres es un documento vivo y cambiante, por lo que requiere mantenimiento.

Antes de probar el plan, se debe dar entrenamiento específico a todos los miembros de los equipos de recuperación en las tareas que se realizarán en caso de desastre. Los líderes de los equipos, en cambio deben recibir entrenamiento general sobre todo el plan completo.

Los objetivos principales de las pruebas son:

- Asegurar que el plan pueda aplicarse exitosamente recuperando lo que sea posible
- Las pruebas sirven como una herramienta de auditoria
- Las pruebas pueden revelar información útil acerca del desempeño de los sistemas a un nivel de emergencia. Entre otras cosas.
- Las pruebas son una forma de entrenar y además pueden utilizar sus resultados para corregir el plan o agregarle aspectos no considerados originalmente.

Para hacer la pruebas.

- Debe establecerse un escenario
- Deben definirse los objetivos de la prueba
- Deben definirse reglas
- Designar participantes y observadores
- Documentar resultados

4.3.2 Metodología de Hewlett-Packard

Esta metodología consta de once fases, como se muestra en la Figura 4.1 y posteriormente se describen las principales tareas que la componen.

Fase 1.-Administración del proyecto

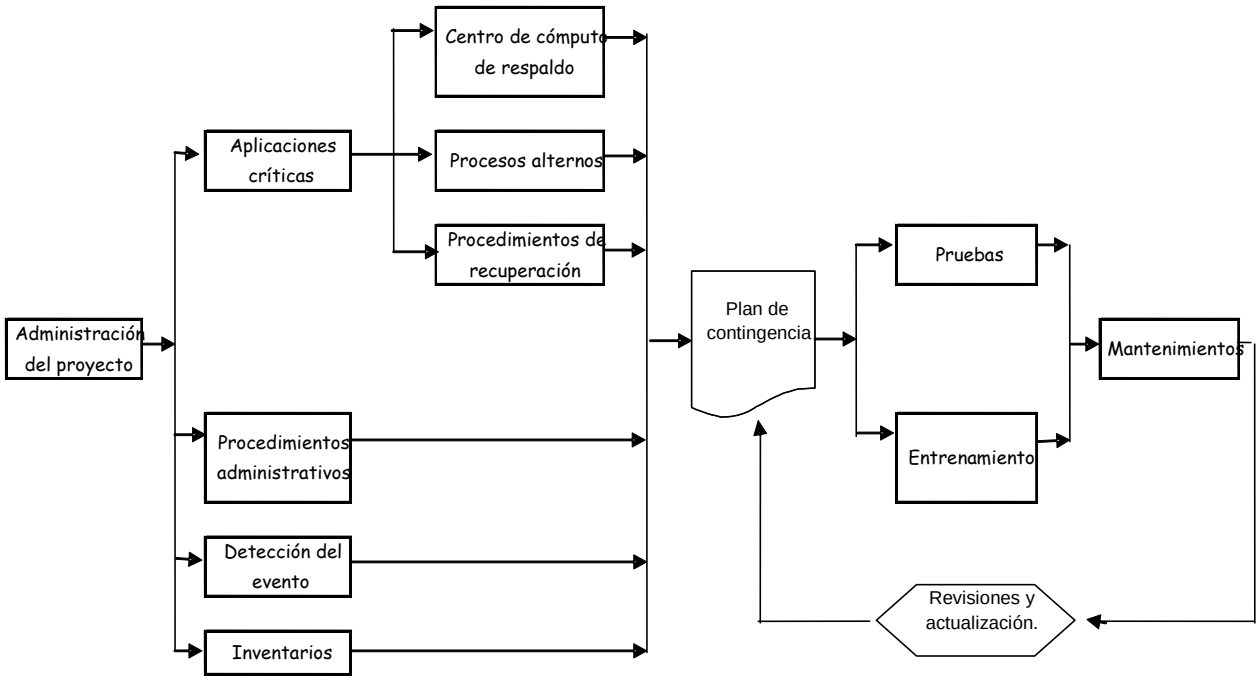
En esta fase se definen los siguientes objetivos:

- Obtener un compromiso de la gerencia: La dirección de la empresa debe comprometerse a desarrollar el plan de recuperación, de tal manera que los recursos necesarios puedan ser asignados al proyecto.
- Organizar el equipo de desarrollo del plan de recuperación de desastres: Identificar a los individuos de la administración, del procesamiento de datos y usuarios.
- Auditar el estado del plan de contingencia existente: Aprovechar aquello que ya se haya puesto en práctica e identificar aquello que falta por hacer.
- Desarrollar un plan administrativo para el proyecto: Realizar una estimación de la duración de las tareas, asignar recursos y desarrollar un calendario para el proyecto.

- Seleccionar las herramientas de documentación: Decidir que software se usará para la documentación del plan y los procedimientos generales.

Figura 4.1

Metodología de Hewlett-Packard para Desarrollo de Planes de Recuperación de Desastres



Fase 2.- Aplicaciones críticas.

Los objetivos de esta fase son:

- Establecer prioridades de las aplicaciones: Analizar todas las aplicaciones para establecer prioridades e identificar cuáles son las críticas. Esta metodología maneja tres categorías: crítica, importante y "todas las demás". Considera que la prioridad de una aplicación se basa en tres factores principales: valor monetario, limitaciones y prioridades y urgencia de tiempo.
- Especificar prioridades de procesamiento para recuperación de desastres: Listar las aplicaciones en orden de restauración durante la recuperación.
- Determinar los requerimientos del procesamiento: Analizar los recursos necesarios para procesar las aplicaciones con prioridad alta, de tal manera que se tenga suficiente capacidad de respaldo.
- Establecer propósitos de la recuperación de desastres: Especificar el nivel de procesamiento y tiempos de recuperación que se han de lograr en la restauración de desastres menores, mayores y catastróficos.

Fase 3.- Instalación de respaldo y procedimientos

Los objetivos de esta fase son:

- Seleccionar una localidad externa de almacenamiento (caja de seguridad): Los datos y documentos de respaldo deben almacenarse fuera de la instalación para que sobrevivan, aun cuando exista la destrucción total del equipo de cómputo.
- Determinar el contenido indispensable de la caja de seguridad externa: Identificar los archivos, software, documentos, materiales, entre otros.

- Especificar procedimientos de almacenamiento y actualización: Determinar los procedimientos, calendarios y responsabilidades de mantenimiento del contenido de la caja de seguridad externa.
- Identificar requerimientos del sistema para las instalaciones de respaldo: Determinar el equipo y la capacidad de procesamiento necesaria en la instalación de respaldo.
- Seleccionar una o más de estas instalaciones: Evaluar las instalaciones de respaldo y elegir una o más para hacer los arreglos necesarios.
- Producir una guía de respaldo de la instalación: Las diferentes instalaciones de respaldo se diferencian entre si sobre todo con el centro primario, por lo que debe documentarse una guía de la instalación de respaldo.
- Identificar al personal de respaldo: El personal del centro de cómputo estará disponible durante la recuperación pero debe tomarse en cuenta personal de respaldo en caso contrario.

Fase 4.- Procedimientos del procesamiento alterno.

Los objetivos de esta fase son:

- Identificar las aplicaciones críticas que requieran procedimientos del procesamiento alterno: Las aplicaciones críticas son por definición aquellas necesarias para la supervivencia de la compañía.
- Desarrollar los procedimientos de procesamiento alterno: Para las aplicaciones críticas seleccionadas, se debe crear el procedimiento de procesamiento alterno, que pueda usarse en caso de que las instalaciones del centro de cómputo no estén disponibles.

Fase 5.- Procedimientos de recuperación

Los objetivos de esta fase son:

- Definir grupos de recuperación y sus funciones: Las acciones que se deben tomar para efectuar el restablecimiento de un desastre son llevadas a cabo por equipos de recuperación, cada uno con su propia área de responsabilidad.
- Identificar a los miembros de cada equipo: Nombrar a las personas que servirán en cada equipo de recuperación.
- Especificar sus procedimientos: Establecer los pasos de acción que tiene que seguir los líderes y miembros del equipo. Se debe distinguir entre las funciones del líder y las funciones de los miembros.

Fase 6.- Procedimientos de detección de eventos

Los objetivos de esta fase son:

- Especificar los procedimientos de emergencia: Son las acciones que deben realizarse inmediatamente, en respuesta a un evento dañino o una situación amenazadora.
- Establecer los procedimientos de escalación: El propósito de estos procedimientos es definir la distribución de los pasos y del tiempo que llevan a la declaración de un desastre menor o catastrófico.

Fase 7.- Procedimientos del equipo de manejo de desastres

Los objetivos de esta fase son:

- Identificar al equipo de manejo de desastres: Este equipo tiene la responsabilidad de dirigir las operaciones de recuperación y restauración del procesamiento normal.
- Especificar las funciones y los procedimientos del equipo: El equipo de manejo de desastres esta orientado a los esfuerzos de recuperación dirigidos que siguen a un desastre. Las responsabilidades son establecidas en un estatuto formalizado, junto con sus funciones, además de los pasos necesarios para iniciar las operaciones de recuperación

- Seleccionar las ubicaciones de los centros de control: Elegir localidades internas y externas para usarse como centro de control. Las operaciones de recuperación de desastres deben dirigirse desde un centro de control y su propósito puede establecerse en una sola palabra. Comunicación
- Listar los recursos del centro de control: El centro de control debe estar bien equipado, especialmente con herramientas de comunicaciones (teléfonos, radios, directorios, entre otros.)
- Realizar un inventario de material necesario para aplicaciones críticas: La evaluación del daño y del impacto con actividades clave de la administración de desastres porque proporcionan la información necesaria para la toma de decisiones.

Fase 8.- Inventario

Los objetivos de esta fase son:

- Llevar un inventario de todos los recursos del procesamiento de datos: El inventario debe dividirse en categorías y después subdividirse en subcategorías, para hacer más fácil la recopilación, la actualización y el uso.
- Listar a los distribuidores de los recursos críticos: Las partidas dañadas en un desastre pueden ser reemplazadas rápidamente, especialmente aquellas usadas por aplicaciones críticas.

Fase 9.- Entrenamiento

Los objetivos de esta fase son:

- Diseñar un plan completo para el entrenamiento de recuperación de desastres: Es necesario un programa general del entrenamiento para asegurar que las personas correctas obtengan el tipo de adiestramiento adecuado
- Desarrollar actividades específicas de entrenamiento: El plan de instrucciones de cada una de las actividades en el programa de adiestramiento debe seguir cualquier formato acostumbrado o conveniente
- Desarrollar técnicas y herramientas de evaluación: El entrenamiento tiene como función primaria el desarrollo del conocimiento y habilidad. También es una buena fuente de información sobre la calidad del plan de recuperación en caso de desastre.

Fase 10.- Pruebas

Los objetivos de esta fase son:

- Diseñar un plan completo de pruebas del plan de recuperación: Las pruebas deben llevarse a cabo de manera cuidadosa y sistemática
- Desarrollar planes para pruebas específicas: Escribir un plan para cada prueba que ha de ser conducida
- Desarrollar técnicas y herramientas de evaluación de las pruebas: Las pruebas proporcionan información importante sobre la adecuación del plan y el entrenamiento

Fase 11.- Mantenimiento

Los objetivos de esta fase son:

- Asignar responsabilidades para la administración y el mantenimiento del plan de recuperación: El mantenimiento involucra varias funciones:
  - Recibir y controlar información de las revisiones necesarias
  - Mantener una lista de distribuciones de las copias del plan y controlar su circulación
  - Mantener la historia de las revisiones del plan
  - Asegurar que las revisiones se lleven a cabo puntualmente
  - Distribuir las actualizaciones como sea necesario

- Coordinar el ciclo de revisión con calendarios de entrenamiento y pruebas
- Coordinar con los auditores el calendario de las revisiones y mantenimiento.

• Establecer procedimientos y calendarios de revisión y mantenimiento: Los propósitos de esta tarea son proporcionar un calendario para la revisión regular y sistemática del contenido del plan y definir un procedimiento para los cambios sugeridos

• Crear listas de distribución y políticas para el programa de recuperación: El plan de recuperación contiene mucha información sensible sobre las operaciones de cómputo por lo que la distribución de este requiere una consideración importante

En la Figura 4.2 se presentan las principales diferencias entre los dos métodos expuestos en este capítulo y el método propuesto. Como se puede observar las diferencias son notables y los dos métodos que ya existen para la elaboración de un DRP tienen algunas deficiencias, las cuales tratamos de cubrir en el método propuesto.

Figura 4.2[1]

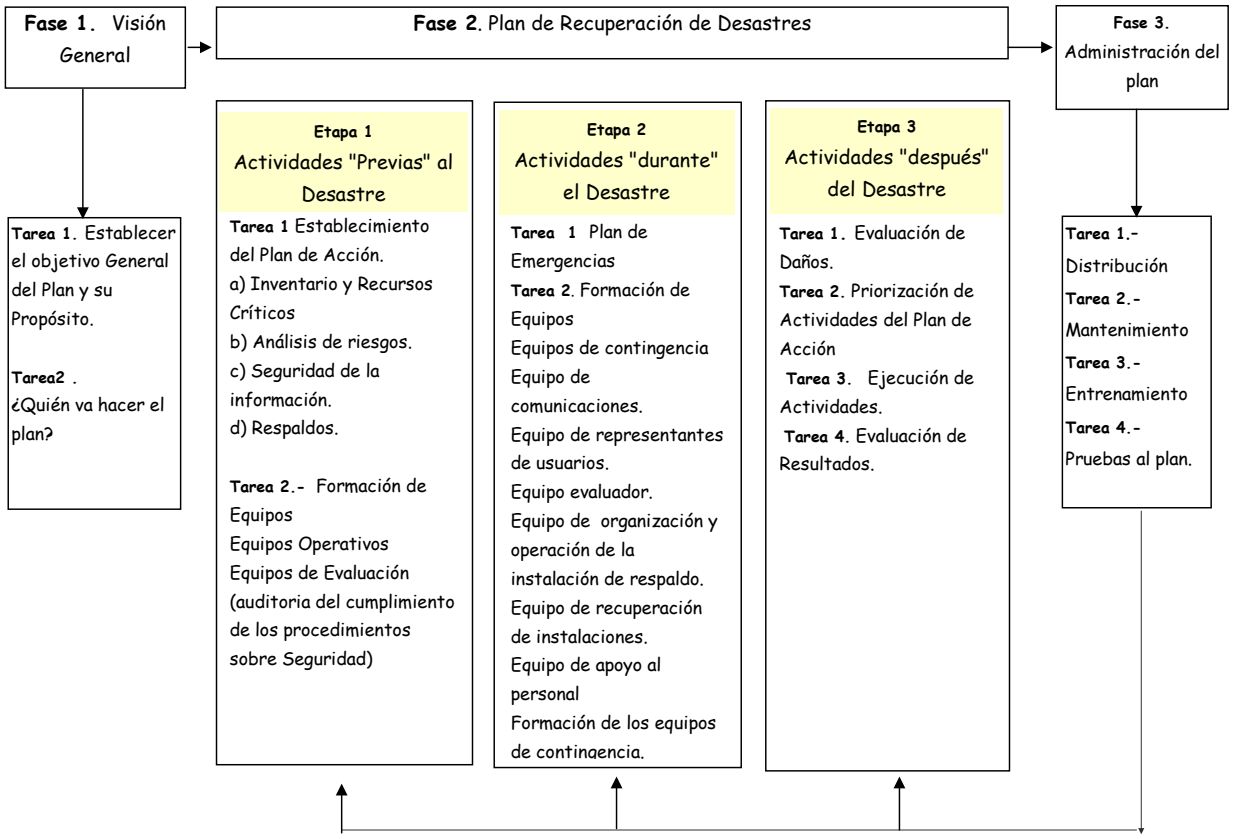
Cuadro comparativo entre metodologías expuestas y método propuesto para la elaboración de planes de recuperación de desastres			
Contempla:	**Metodología William Toigo**	**Metodología Hewlett-Packard.**	**Método propuesto**
Elección de personal que realizará el plan		Sí	Sí
Objetivos del plan	Sí		Sí
Revisión a planes existentes		Sí	Sí
Inventario de Recursos		Sí	Sí
Análisis de riesgos	Sí		Sí
Análisis de impacto en el negocio			Sí
Seguridad física	Sí		Sí
Seguridad lógica			Sí
Seguridad de redes			Sí
Almacenamiento de respaldo en sitio externo	Sí	Sí	Sí
Estrategias de respaldo	Sí		Sí
Manuales de procedimientos de respaldo		Sí	Sí
Planes de emergencias	Sí	Sí	Sí
Elaboración de equipos y asignación de responsabilidades		Sí	Sí
Mantenimiento al plan	Sí	Sí	Sí
Entrenamiento		Sí	Sí
Pruebas al plan	Sí	Sí	Sí
Administración del plan	Sí		Sí
Auditoría al plan			Sí

[1] Figura elaborada por los realizadores de la presente tesis

4.4 Método propuesto. Plan de Recuperación de Desastres.

Figura 4.3

Metodología Propuesta para el Desarrollo de Planes de Recuperación de Desastres



Luego de revisar otras metodologías para la elaboración de planes de recuperación de desastres, dos de las cuales se exponen en este capítulo (Hewlett-Packard y William Toigo), notamos que cada una tiene sus fortalezas y sus debilidades, sin embargo diseñamos un método que abarca algunos puntos mas que estas dos metodologías juntas.

El método que estamos proponiendo es una manera sencilla y de cierta forma práctica de visualizar el DRP (ver Figura 4.3). En este método tratamos de ubicarnos en el tiempo y detallamos las actividades de manera cronológica de la ocurrencia de las cosas, además que ofrece alternativas para empresas medianas y pequeñas que aunque no desarrollen este tipo de programas por cuestiones de falta de capacidad financiera, les sirva de ayuda para reducir la exposición a los riesgos, aplicando únicamente a manera de prevención las recomendaciones que aquí establecemos.

Este método está enfocado primordialmente a empresas cuya principal preocupación es disminuir el tiempo fuera de operación y realizar el restablecimiento de sus operaciones en el menor tiempo posible. Este plan se desarrolla a fondo, incluyendo todos los procedimientos detallados que se utilizarán, antes, durante y después de un desastre o contingencia.

Esta metodología se divide en tres fases fundamentales, las cuales a su vez se dividen en etapas y tareas que para mayor comprensión, describimos a continuación:

Fase 1: Visión General.

En esta fase, las acciones se orientan a la formulación de un marco general que permita establecer las bases conceptuales, aquí también se establece quien será el encargado de diseñar el plan; consta de dos tareas:

Tarea 1. Establecer el objetivo General del Plan y su Propósito.

Independientemente de los objetivos propios que establezca cada empresa para su plan de contingencia, los objetivos generales del plan son los siguientes:

- Restablecer el proceso de las aplicaciones críticas tan pronto como sea posible.
- Recobrar después el procesamiento total, restaurando completamente las operaciones afectadas por el desastre.
- Restablecer la capacidad total de procesamiento de la empresa (las condiciones normales).

Tarea 2. ¿Quién va hacer el plan?

Hay que decidir quién se encargará de desarrollar el plan. Las dos opciones principales son (1) que el plan sea desarrollado por un experto en la materia contratado especialmente para esto y (2) que el plan sea desarrollado por el personal de la empresa que probablemente será coordinado por un miembro del área de sistemas, un miembro del área de seguridad o ambos.

Consultor Externo

Si se decide que el plan sea desarrollado por un consultor externo, deben realizarse las siguientes actividades:

- Selección del consultor
- Negociación con el consultor: Tratar de llegar al acuerdo más conveniente para la empresa, en términos económicos.
- Obtener el plan de trabajo del consultor: de esta manera se podrá controlar que el plan este listo y funcionando en el menor tiempo posible.

Desarrollo en Casa

Si se decide que el plan de contingencia sea desarrollado en casa, deben realizarse las siguientes actividades:

- Investigación y selección de metodología. En la sección 4.3 de este capítulo se presentan dos metodologías: la de William Toigo y la de Hewlett-Packard. Está también la opción de utilizar la presente metodología propuesta.
- Identificar Aplicaciones identificadas como críticas
- Directorio telefónico
- Requerimientos mínimos por sistema
- Procedimientos de recuperación de la información, procedimientos de respaldo.
- *Site* alterno con disponibilidad de:
  - Espacio en disco
  - Líneas de comunicación
  - Espacio físico para el personal
  - Misma configuración del equipo (sistema operativo y software).

- Plan de trabajo: estimación de la duración de las tareas, ubicación de los recursos y elaboración de un plan de trabajo para el proyecto del plan de recuperación de desastres.

Fase 2: Plan de Recuperación de Desastres

Etapa 1: Actividades Previas al Desastre.

Aquí se definen las actividades de planeamiento, prevención, 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 y que consta de las siguientes tareas:

Tarea 1 Establecimiento del Plan de Acción.

a) Inventario y Recursos Críticos

Un centro de cómputo puede realizar cientos de operaciones que el personal y los usuarios consideren importantes, pero durante un desastre no puede hacerse todo porque los recursos clave no están disponibles. Por esto, durante un desastre, una corporación debe concentrarse en el procesamiento de cómputo que sea más importante para la supervivencia: sus aplicaciones críticas. Hay que entender que el objetivo de un plan de contingencia es minimizar la pérdida potencial de los activos, no el de duplicar un entorno normal del negocio.

Entonces, como parte del diseño de un plan de contingencia, las aplicaciones más críticas deben ser identificadas junto con los recursos necesarios para ejecutarlas.

A continuación se presentan las actividades que hay que realizar en esta tarea. Las dividimos de acuerdo con las posibilidades:

- Identificar los requerimientos mínimos de procesamiento de todos los sistemas
  En esta actividad, el objetivo estriba en identificar todos los recursos de hardware, software, equipo auxiliar, provisiones, entre otros, así como los archivos de datos que se requieren para procesar todos los sistemas de la empresa. Los aspectos que deben identificarse son los siguientes:
  - Usuarios: cuántos y cuáles (por puesto y nombre)
  - Requerimientos de ejecución: tiempo de ejecución, fechas críticas (si las hay), modelo del CPU, espacio en disco de las aplicaciones, memoria principal, comunicaciones y redes (es muy importante que el diseñador del plan de contingencia entienda la configuración e importancia de las redes de computadoras instaladas, especialmente si se hace un procesamiento distribuido), entre otros.
  - Archivos: archivos de datos, espacio en disco para estos archivos.
  - Software: sistema operativo, cualquier software que tenga que estar presente durante la "corrida". También es conveniente identificar el software necesario para la compilación de las aplicaciones ya que podría ser necesario recopilar antes de instalar en el centro de cómputo alterno.
  - Otros: impresoras, papel, formas especiales preimpresas, requerimientos de comunicación de datos, entre otros.
- Realizar un inventario de todos los recursos de cómputo: Es necesario tener un inventario completo y actualizado de los recursos del procesamiento de datos, por dos razones:

- Evaluación del daño: al usar el inventario como una lista de verificación, se puede determinar rápidamente qué recursos siguen operando y cuáles han sido dañados. Así podrá determinarse también si existe alguna capacidad de procesamiento después del desastre.
- Restauración de instalaciones: para restaurar los daños ocurridos al centro de cómputo por el impacto de un desastre, se utiliza el resultado de la evaluación del daño; se adquieren los dispositivos destruidos y se puede reproducir rápidamente (dependiendo de los proveedores) la instalación existente antes del desastre.

Por medio de la realización de este inventario, podremos identificar cuál es el sistema afectable que estamos tratando de proteger. En la tarea anterior ya identificamos el sistema perturbador; el sistema regulador que diseñemos posteriormente (recomendaciones sobre seguridad de la información y el plan de contingencia) será mejor.

En este inventario deben incluirse:

+ Software
+ Aplicaciones
+ Archivos de información
+ Medios de almacenamiento donde se contiene lo anterior
+ Hardware
+ Equipo de comunicaciones y redes

Documentación: manuales técnicos, de usuario, documentación de las aplicaciones, entre otros.

Equipo auxiliar: aire acondicionado, equipo contra incendios, dispositivos de seguridad, entre otros.

Diagramas de las configuraciones de redes, configuración de las computadoras, entre otros.

Otros: papel, formas preimpresas, entre otros.

Esta actividad podría permutarse con la anterior con respecto al orden de ejecución (determinar los requerimientos mínimos de procesamiento de los sistemas críticos y vitales), lo cual incluso podría facilitar la realización de la actividad anterior.

- Clasificar los Sistemas Según su Grado Crítico

Para determinar cuáles son las aplicaciones críticas, lo primero es hacer un "inventario" de aplicaciones. Esto es, hay que saber cuáles son todas las aplicaciones y formar un compendio, para después poder priorizarlas. Esta lista de aplicaciones se puede realizar con la ayuda del personal del área de sistemas.

Para determinar el grado crítico de cada sistema, se utiliza primordialmente información proporcionada por los usuarios.

Esta información se puede obtener por medio de cuestionarios o entrevistas (preferentemente) realizados a los empleados que utilizan los sistemas en forma cotidiana. El cuestionario o entrevista deben incluir preguntas para saber que sistemas usa, para qué y con qué frecuencia. También, para poder determinar el grado crítico del sistema, hay que preguntarles como manejarían la situación si el sistema no estuviera disponible durante determinado lapso.

La prioridad de una aplicación se basa en dos factores y un tercero derivado de esos dos:
Valor monetario: cantidad de ingresos producidos por la aplicación, o cantidad de pérdida en caso de que no se ejecute en determinado lapso. Esto se calcula equivalente a la cantidad de ingresos producida por la función que se esta automatizando.

Importancia: las aplicaciones pueden ser necesarias porque se usan para satisfacer ciertas prioridades del negocio (por ejemplo, dar servicio a clientes). Este factor de cada aplicación se conoce a través de las entrevistas con los usuarios y también en pláticas con la Gerencia o Dirección ya que ellos tienen una visión global del negocio y saben que es lo más importante.
Los dos factores anteriores derivan en un tercero que es la urgencia de tiempo, es decir, la necesidad de ejecutar una aplicación en un momento o con una frecuencia determinada. Ambos pueden variar según la hora del día, el día del mes, o el mes del año en que ocurra la falla. Por lo tanto, es importante no complicarse por esto; para nuestro propósito, hay que asumir que la falla ocurre en el peor momento posible.

El propósito de este análisis es asignar a cada aplicación una de las siguientes categorías (esta es la clasificación más común en la actualidad):
Crítica: estas funciones no pueden ser ejecutadas a menos que se consigan recursos con capacidades idénticas a las normales que reemplacen a las afectadas. No pueden ser reemplazadas por procedimientos manuales bajo ninguna circunstancia. La tolerancia a la interrupción es muy baja y el costo de la misma muy alto.
Vital: estas funciones no pueden ser ejecutadas por medios manuales o pueden ser manuales únicamente por un periodo muy breve. Tienen una tolerancia un poco mayor a la interrupción y el costo es un poco más bajo, siempre y cuando las funciones sean restauradas dentro de un cierto límite de tiempo.
Sensibles: estas funciones pueden ser ejecutadas con dificultad pero a un costo tolerable durante periodos más largos de tiempo.
No críticas: estas aplicaciones pueden ser interrumpidas por un lapso grande, a un costo muy pequeño o nulo para la compañía.

Después de haber clasificado los sistemas en esas cuatro categorías, es conveniente darles un orden de importancia dentro de cada categoría (un número que va del uno al número de aplicaciones). Este número servirá para determinar en que orden ir poniendo en operación los sistemas durante la recuperación de un desastre total con un centro de cómputo con recursos limitados, o cuáles sistemas dejar en operación en el caso de un desastre parcial que disminuya la capacidad de procesamiento. Por ejemplo, dentro de la clasificación "críticos" pueden quedar tres sistemas, ahora hay que numerarlos del 1 al 3 para saber cuál es el primero que se pondría a operar, cuál es el segundo y cuál el tercero en caso de un desastre.
En algunos casos, esta actividad de clasificación y ordenamiento de las aplicaciones es muy sencilla porque el grado crítico de cada aplicación será muy evidente y entonces los diseñadores del plan podrán ahorrar trabajo en el análisis formal anteriormente descrito. Cuando no sea así, tendrá que establecerse su importancia, valor monetario, entre otros., para poder clasificarlas.

Determinar los Requerimientos Mínimos de Procesamiento de los Sistemas Críticos y Vitales: En la actividad anterior se analizaron todas las aplicaciones para identificar cuáles eran críticas o vitales. En esta actividad, el objetivo estriba en identificar todos los recursos de hardware, software, información, equipo auxiliar, provisiones, entre otros., que se requieren para procesar los sistemas críticos y vitales de la empresa. Los aspectos que deben identificarse son los siguientes:

- Usuarios: cuántos y cuáles (por puesto y nombre)
- Requerimientos de ejecución: tiempo de ejecución, fechas críticas (si las hay), modelo del CPU, espacio en disco de las aplicaciones, memoria principal, comunicaciones y redes (es muy importante que el diseñador del plan de contingencia entienda la configuración e importancia de las redes de computadoras instaladas).
- Archivos de datos, espacio en disco para estos.
- Software: sistema operativo, cualquier software presente durante la ejecución. También es conveniente identificar el software necesario para la compilación de las aplicaciones ya que podría ser necesario recopilar antes de instalar en el centro de cómputo alterno.
- Otros: impresoras, papel, formas especiales preimpresas, requerimientos de comunicación de datos, entre otros.

• Realizar un Inventario de todos los Recursos de Cómputo.

Es necesario tener un inventario completo y actualizado, de los recursos del procesamiento de datos, por dos razones:

Evaluación del daño: al usar el inventario como una lista de verificación, se puede determinar rápidamente qué recursos siguen operando y cuáles han sido dañados. Así podrá determinarse también si existe alguna capacidad de procesamiento después del desastre.

Restauración de instalaciones: para restaurar los daños ocurridos al centro de cómputo por el impacto de un desastre, se utiliza el resultado de la evaluación del daño; se adquieren los dispositivos destruidos y se puede reproducir rápidamente (dependiendo de los proveedores) la instalación existente antes del desastre.

En este inventario debe incluirse:

- Software
- Aplicaciones
- Archivos de información
- Medios de almacenamiento donde se contiene lo anterior
- Hardware
- Equipo de comunicaciones y redes
- Documentación: manuales técnicos, de usuario, documentación de las aplicaciones, entre otros.
- Equipo auxiliar: aire acondicionado, equipo contra incendios, dispositivos de seguridad, entre otros.
- Configuración de las computadoras, diagrama de configuración de las redes, entre otros.
- Otros: papel, formas preimpresas, entre otros.

Esta actividad podría permutarse con la anterior (determinar los requerimientos mínimos de procesamiento de los sistemas críticos y vitales), lo cuál incluso podría facilitar la realización de la actividad anterior hasta cierto punto.

b) Análisis de riesgos.

El análisis de riesgo regularmente es más cualitativo que cuantitativo recomendamos realizarlo según lineamientos expuestos en el capítulo dos (análisis de riesgos). Recordemos que análisis de riesgo se refiere al estudio estructurado con que se revisa la probabilidad de que cualquier calamidad pueda ocurrir y lo que sucederá al sistema de procesamiento de datos de la organización en el caso de que ésta se enfrente con amenazas/riegos específicos, es decir, la pérdida esperada.

Al realizar este análisis de riesgo, el diseñador del plan de contingencia deberá identificar la dependencia de la continuidad del negocio en las redes de cómputo; esto, en el caso de las empresas que tengan redes de computadoras de cualquier tipo (LAN, Local Aerea Network; MAN, Metropolitan Area Network; WAN, Wide Area Network; entre otros.).

Cabe hacer notar que los resultados de esta etapa, además de cumplir la función que acabamos de señalar, servirán para justificar en forma realista la necesidad de contar con el plan y por ende de invertir en él. En este sentido, puede ser útil hacer el análisis de riesgos cuantificado ya que así pueden justificarse los montos de inversión necesarios para desarrollar el plan de contingencia. Si se diera el caso de que la alta dirección de la organización se mostrará renuente a invertir lo suficiente para asegurar la continuidad de la función de sistemas (aunque esto no debería suceder), entonces sería necesario convencerlos mostrándoles las cifras que representa la pérdida potencial por los desastres cuyos efectos no podrían prevenirse ni mitigarse debido a la ausencia o a la no adecuación del plan de contingencia. Entonces ellos podrían ver como una cantidad mucho menor, estarían asegurándose contra pérdidas mayores y de efectos desastrosos no sólo económicos sino legales, de imagen corporativa, entre otros.

A continuación se presentan las actividades que conforman este punto:

Identificación de riesgos

Identificación de Desastres Probables

El objetivo es conocer las principales amenazas que se ciernen sobre el procesamiento de datos de la empresa; así sabremos exactamente de qué queremos protegernos. Aunque el plan de contingencia debe servir para guiar la recuperación de cualquier desastre, resulta importante que estemos especialmente preparados para combatir los desastres que tienen una mayor probabilidad de ocurrencia; por ejemplo, en la Ciudad de México no tiene caso invertir en prepararse contra huracanes.

Identificación de Riesgos Externos e Internos

Una identificación de riesgos sistemática asegura que se han revisado y analizado todas las amenazas potenciales.

El resultado de esta actividad será la base para desarrollar los procedimientos de emergencia en una etapa posterior. Las actividades de prevención serán dirigidas a los riesgos que sean identificados en esta tarea.
Para facilitar y acelerar la realización de esta actividad, puede considerarse lo siguiente:
Consultar a los organismos locales de atención de emergencias y de protección civil. Ellos ya tienen definido cuáles son los desastres naturales de ocurrencia más probable en la Ciudad de México.
Finalmente, hay que mencionar que las empresas que cuenten con redes de área amplia (MAN o WAN, respectivamente), deben poner especial cuidado en la identificación de riesgos a las telecomunicaciones.

Técnicas de análisis
Como se expuso en la sección 2.3 del capítulo dos aquí se pueden utilizar los métodos cuantitativos y los cualitativos, el objetivo es determinar la probabilidad de que ocurra un desastre y cual sería su impacto.

Tratamiento del riesgo
Aquí se determina una vez identificado, analizado y proyectado el riesgo, de que manera se tratará, es decir si se asume, minimiza o se transfiere, en la sección 2.4 del capítulo dos se detallan estas formas de tratamiento del riesgo.

c) Seguridad de la información.
Sabemos que el plan de recuperación disminuye su eficacia al tiempo que se vuelve más complejo si no existe un buen plan de seguridad de la información. A su vez, este debe ser complementado con un buen DRP.

Este punto se divide en tres, seguridad física, seguridad lógica y seguridad en redes, en el capítulo uno sección 1.3 se muestran especificaciones relacionadas a estos tres tipos de seguridad.

Las actividades que conforman esta etapa son las siguientes:

- Identificar las Medidas de Seguridad de la información implantadas Actualmente.
  Hay que identificar y compilar todas las medidas de seguridad de la información funcionando actualmente en la empresa, medidas de seguridad lógica, física y de redes. Es necesario saber cuales son todas las medidas que pueden considerarse como de prevención de desastres. Es decir, en esta actividad hay que conocer el sistema regulador con que cuenta la empresa actualmente. Esto tiene dos objetivos:
  - Reinstalar estas medidas en caso de que los dispositivos que las realizan sean destruidas por un desastre.
  - Conocer la situación de la seguridad de la información dentro de la empresa y en especial para los sistemas de información automatizados. Así se podrá evaluar si esta es suficiente para proteger los sistemas de todos los riesgos identificados, especialmente los críticos y vitales.
  - Hacer recomendaciones sobre medidas que pueden ser implantadas

Una vez conociendo la situación actual de la seguridad de información en la empresa y tomando en cuenta que ya conocemos cuáles son los recursos críticos que hay que proteger, podemos elaborar una propuesta sobre medidas preventivas que no existen y que consideramos necesarias para mejorar las posibilidades de continuidad de la función de sistemas. Se trata aquí de mejorar el sistema regulador, haciéndolo más suficiente y adecuado a la organización y sus necesidades.

- Integrar al responsable de seguridad a los equipos de recuperación.

La visión que se forme el planeador de contingencia sobre el aspecto de seguridad de la información será muy útil para mejorarla ya que él tiene una perspectiva global de la exposición de los sistemas de información a riesgos, la gravedad del impacto de un desastre en estos sistemas, la importancia de los sistemas para la labor diaria de la empresa, entre otros. Por lo tanto, el coordinador y algunos otros miembros del plan de contingencia podrán realizar aportaciones importantes a la planeación de la seguridad de la información.

De la misma manera, es recomendable y necesario integrar al responsable permanente de la seguridad de información al personal de desarrollo del plan de contingencia, así como al equipo de manejo de desastres durante la recuperación, donde sus ideas y experiencia resultarán de la mayor relevancia. Así la relación establecida entre los equipos de contingencia y de seguridad, coadyuvará a hacer más efectivo el trabajo de ambos, complementándose en una forma más adecuada. Se trata pues, de que ambos equipos empiecen a trabajar coordinando y dirigiendo sus esfuerzos hacia un mismo objetivo, diseñando y poniendo en práctica su trabajo en forma conjunta.

d) Respaldos.

La importancia de esta sección radica en que la recuperación de un desastre depende de la disponibilidad de los recursos adecuados.

En general, se requieren respaldos de lo siguiente:

- Datos y documentación para aplicaciones
- Sistema de cómputo con los periféricos necesarios y las conexiones de comunicaciones de datos (hardware)
- Software, incluyendo sistemas operativos, utilerías y programas de aplicaciones junto con la documentación necesaria
- Materiales, tales como formas preimpresas, papel, cintas, toner
- Personal que realice el trabajo
- Una instalación alterna con el espacio de trabajo adecuado para el procesamiento de datos y para los usuarios (puede ser el mismo centro de cómputo de respaldo).

Esta etapa puede considerarse como una de las más importantes para el éxito del plan de contingencia y es importante tanto su diseño adecuado como su ejecución día a día. Podemos tener un excelente plan de contingencia, con el diseño mas adecuado, el personal mejor entrenado, entre otros., en fin, todos los recursos económicos y humanos disponibles, pero si no tenemos la información o los sistemas que la explotan, nada podremos hacer en el momento de una contingencia.

Las actividades que conforman esta sección son las siguientes:

- Definir lo que debe respaldarse y con qué frecuencia.
- Proveer la forma de restaurar las actividades del negocio y las funciones de sistemas usando la información almacenada fuera de la empresa, requiere que la información correcta sea identificada. Es decir, se necesita saber exactamente qué información es la que se va a usar en el procesamiento de sistemas posterior a una emergencia. Así podrá conformarse el contenido del site de almacenamiento externo.

El material guardado en el almacén externo debe incluir:

• Respaldos de software y documentación
• Respaldos de aplicaciones y documentación
• Respaldos de datos
• El inventario
• Otros materiales necesarios: formas preimpresas, papel, cintas, entre otros. (en especial los que sean difíciles de conseguir rápidamente).
Copia (s) del plan de contingencia.
• Si es necesario, algún listado de gran importancia que pueda consultarse para suplir la falta de otros sistemas que no puedan ejecutarse durante la contingencia
• Procedimientos de procesamiento alterno y sus formas o materiales.

En cuanto a la frecuencia con que deben hacerse los respaldos y ser transportados al almacén externo, dependerá de varios factores:

+ La importancia del recurso
+ La frecuencia con que éste es modificado.

En todas y cada una de las tareas de que se componen en esta actividad hay que tomar en cuenta no solo los recursos que están en el centro de cómputo sino los de todos los equipos de cómputo donde se procesen los sistemas críticos y todo lo necesario para la recuperación después de un desastre.

Algunas sugerencias respecto a la frecuencia con que deben hacerse los respaldos son las siguientes:

+ Cuando se adquiera un nuevo paquete de software o se instale una nueva versión de sistema operativo o algún software de base debe generarse una copia para el almacén de seguridad. También se puede almacenar una copia de los manuales.
+ Cada vez que se ponga una nueva aplicación en producción hay que almacenar una copia de ésta, así como de su documentación. Posteriormente se puede analizar el grado crítico de ésta aplicación y así se decide, puede o no eliminarse su respaldo.
+ Cada vez que se modifique el plan de contingencia se debe almacenar la copia actualizada.
+ Cada vez que se actualice el inventario del equipo de cómputo debe almacenarse la copia más actualizada.
+ Cuando se incluya un nuevo material, o se modifique el material existente requerido para el procesamiento de los sistemas críticos
+ Cuando se cuente con redes de computadoras deberá ponerse especial énfasis en la formulación de los procedimientos de respaldo, definiendo claramente con que frecuencia se harán los respaldos, que información se va a respaldar, dónde está

almacenada esta información, quién tendrá la responsabilidad de llevarla a cabo, donde se almacenarán los medios que contengan esos respaldos, entre otros.

Selección del *site* de almacenamiento externo

El local que se elija servirá para almacenar los datos y la documentación de respaldo en un lugar donde exista la posibilidad de que sobrevivan, aún en el caso de destrucción total del centro de cómputo o de la empresa completa.

Hay que reconocer que incluso la información que no requiera ser duplicada por razones de continuidad, no deberá permanecer dentro del centro de cómputo, sino en un almacén seguro en alguna parte del edificio de la empresa.

Dentro del centro de cómputo solamente deben permanecer un mínimo de registros de información necesarios para la operación eficiente.

Algunas consideraciones en la elección del almacén externo (de respaldo) son las siguientes:

- El almacén no debería ser dañado por un desastre que afecte al centro de cómputo (aunque en la práctica no puede estar muy lejos del centro de cómputo por que el transporte de los respaldos de información, con la frecuencia que éstos se hagan, podría representar un problema.
- El almacén no debe estar localizado en un área de alto riesgo,
- Debe tener un tamaño suficiente para albergar todo su contenido en una forma organizada.
- Debe cumplir con las medidas mínimas de seguridad.
- Debe cumplir con las medidas mínimas de condición ambiental como temperatura y humedad.

Hay varias opciones que sirven como almacenamiento externo:

- Cajas de seguridad contra incendios: existe una variedad de cajas de seguridad y gabinetes contra incendios disponibles para almacenar información.
- Almacenes: esta opción consiste en almacenar los datos en otra instalación que cuente con los mismos requerimientos de control de temperatura, humedad, protección contra incendios, detección de agua y seguridad física que el *site* de la empresa.
- Instalaciones comerciales de almacenamiento de información: ésta es una de las opciones más utilizadas en los Estados Unidos. Son empresas dedicadas al almacenamiento de información, que cumplen con todos los requerimientos de seguridad y medio ambiente. Una forma de justificar el gasto en esta instalación es el hecho de que el almacén puede no ser utilizado sólo por el área de sistemas, sino también para almacenar cualquier información vital de la empresa.

Obtener un centro de cómputo de respaldo

Después de que han sido identificadas las aplicaciones críticas y que se han identificado sus requerimientos de procesamiento, el planeador del plan de recuperación usa esta información para determinar la configuración mínima de hardware que podrá soportar el procesamiento de estas aplicaciones críticas. Ya con esto, el planeador extra listo para buscar un centro de procesamiento de datos de respaldo con capacidad para soportar el procesamiento de esas aplicaciones durante el estado de desastre.

A esta actividad es a la que algunos autores llaman estrategia de recuperación, que consiste en tener la habilidad para procesar información, antes de que se logre la recuperación completa del site primario de cómputo.
Tenemos varias opciones a considerar, aunque no todas son viables para todas las organizaciones, por lo que se debe examinar cada caso para determinar cuál es la más adecuada. Además, cada opción tiene sus ventajas y sus desventajas. Incluso, para diseñar una estrategia de recuperación, es posible que se requiera una solución múltiple.

• La primera estrategia es la "hermética", parte de la hipótesis de que es posible construir un centro de cómputo "ultraseguro" de manera que la probabilidad de una interrupción de funciones es insignificante o nula. Esta estrategia tiene un precio prohibitivo ya que implica máxima seguridad en hardware, suministro de energía, medio ambiente, acceso, seguridad lógica, entre otros.

• Instalación del proveedor: la mayoría de los vendedores de hardware tiene equipo de cómputo disponible para usarse y probarse en centros de demostración; por supuesto que esta opción ofrecerá al usuario un tiempo muy reducido de uso de máquina. También, algunos proveedores ofrecen el servicio del centro de cómputo de respaldo para sus clientes; en México, IBM y HP están dando este servicio.

• Convenio de ayuda mutua: a pesar de que a este tipo de convenios se les considera informales, han existido durante algún tiempo y han funcionado. En nuestro país representan una opción viable para la mayoría de las empresas ya que no se cuenta con servicios especializados de respaldo. Tal vez la principal ventaja de esta opción es el costo ya que con un gasto mínimo, se provee a la compañía de capacidad de cómputo en una máquina que funciona.

Este convenio se celebra con otra compañía que tenga una infraestructura de cómputo con características similares, es decir hardware compatible y, sobre todo, tiempo y capacidad de procesamiento disponible, o ambos. Además, se deben tener dispositivos de entrada y salida que permitan utilizar los respaldos que se han realizado y generar resultados que el usuario utilizará como siempre lo ha hecho. Hasta que los requerimientos de cada uno de los participantes han sido definidos, la viabilidad de este tipo de arreglos será cuestionable. Por supuesto, es necesario hacer notar que ninguna compañía que desee proporcionar soporte a otra que ha perdido su capacidad de procesamiento automatizado de datos, puede hacerlo sin impactar de alguna forma su propia operación.

Algunas condiciones para que se pueda llegar a este tipo de acuerdo son las siguientes:

- Cada parte debe tener su plan de contingencia, diseñado, puesto en práctica y probado.
- Cada una debe de estar preparada para soportar el procesamiento del afectado en cualquier momento.
- Los planes de crecimiento preferentemente han de ser similares.

Algunos de los problemas que presenta esta opción son los siguientes:

a) Muchas firmas no están dispuestas a proveer tiempo de máquina para verificar en los hechos la compatibilidad.
b) El crecimiento y la evolución de los sistemas de cómputo pueden causar que dos sistemas que eran compatibles dejen de serlo en un tiempo corto.
c) Los asuntos relacionados con seguridad del sistema deben aumentar y mejorar mucho durante la operación compartida.
d) La probabilidad de que su procesamiento de datos se vea impactado por alguna contingencia se ve incrementada ya que no sólo se verá afectado por lo que ocurra al centro de cómputo propio sino también por lo que pudiera pasar a los centros de cómputo de las demás compañías que suscriben el convenio.

- Centro de contingencia dedicado (hot site): es una instalación de cómputo totalmente equipada y disponible para usarse en el momento de que el sistema de un suscriptor quede fuera de servicio. Esta opción es recomendable para cualquier organización que no pueda estar sin procesamiento de sistemas de cómputo ni un día. Adicionalmente al equipo, la mayoría ofrece espacio listo para recibir otras computadoras que pueden utilizarse. Además, estas empresas dan cierto número de horas al año para hacer simulacros del plan (normalmente entre 24 y 72). En ocasiones también ofrecen espacio para documentos e información (esta podría ser la solución al almacenamiento externo), además de espacio con equipo de oficina.
- Otro centro de cómputo de la compañía: En las situaciones donde el procesamiento de información crítica crece muy rápidamente, o es susceptible de ser dividido sin pérdida de continuidad o funcionalidad, o que no pueden utilizarse las otras opciones, es apropiado considerar el establecimiento de un segundo centro de cómputo de la compañía.

Esta es la alternativa más obvia y natural para las compañías que tienen más de un centro de cómputo y con diferente ubicación geográfica. Es decir, si los centros de cómputo se encuentran dentro del mismo edificio, entonces no debe contarse con que estos centros de cómputo se encuentran dentro del mismo edificio, entonces no debe contarse con que estos centros de cómputo puedan respaldarse mutuamente ya que una catástrofe que afectara a uno seguramente afectaría al otro. Por otro lado, si se encuentran demasiado lejos, podría hacer que el procesamiento alterno fuera poco ágil y oportuno, por esa razón tampoco sería una buena opción. Este parámetro de distancia está en función del tamaño y recursos con que cuente la empresa, además de la infraestructura de telecomunicaciones y transporte con que se cuente en la región.

Esta alternativa tiene la ventaja comparativa de ofrecer un tiempo de transferencia rápido, un equipo humano familiarizado con la producción y seguridad y control del ambiente diseñado con los estándares de la compañía.
De cualquier manera, el establecimiento de un segundo centro de cómputo no hace que la compañía quede exenta de la planeación de contingencia a detalle, necesaria para su éxito adecuado.

- Mobile Hot o Cold Sites: Esta opción se esta volviendo muy popular en los Estados Unidos. Consiste en un trailer que contiene equipo de cómputo listo para operar y que

puede ser puesto en el estacionamiento de la empresa después de la ocurrencia de una contingencia. Normalmente contiene muy poco equipo de comunicaciones, pero traen unida una segunda caja con espacio para otras necesidades durante la recuperación, por ejemplo equipo de oficina. Este servicio esta diseñado para minimizar la necesidad de cambiar de sede durante la recuperación de las operaciones de cómputo (especialmente después de un desastre natural, cuando los empleados de la compañía no querrán moverse y dejar sus hogares o familias)

Finalmente, existen otras dos alternativas de estrategias de respaldo:

1.- El uso de microcomputadoras: usar microcomputadoras y encontrar una localización para operarlas es generalmente más fácil que hacer esto con una computadora central ya que aquellas no requieren de todo el acondicionamiento ambiental que requieren las computadoras centrales. Además, los distribuidores generalmente pueden proveer microcomputadoras en un solo día. Obviamente esta alternativa solo puede realizarse en el caso de que las aplicaciones críticas puedan ser procesadas en equipo de computación personal

2.- Respaldo manual: el grado de dependencia de los sistemas automatizados, al igual que la capacidad de la organización para poner en práctica los procedimientos manuales, determinan la extensión en que las operaciones manuales puedan reemplazar las funciones automatizadas en el momento de un desastre. Si el grado de dependencia de los sistemas automatizados es bajo, entonces la conversión a procedimientos manuales es una alternativa muy viable. Esta alternativa resultará muy útil en lugares donde existen interrupciones breves muy frecuentemente. Puede resultar una alternativa cara; dado que podría ser necesario considerar personal adicional, además de que todos deben de estar suficientemente entrenados en dichos procedimientos. Una condición necesaria es que el registro de las transacciones en papel debe seguir la misma estructura de campos utilizada en el subsistema de captura del sistema que este respaldando. De esta manera, será más sencilla la utilización del sistema de respaldo manual, así como el regreso al sistema automatizado, cuando este se restablezca. Finalmente, hay que recordar que esta alternativa involucra mucho a las áreas usuarias en la planeación y la recuperación misma del desastre.

Al seleccionar una instalación de respaldo se deben tomar en cuenta muchos factores, pero indudablemente el más importante es que sea suficiente para soportar los objetivos de recuperación que han sido previamente establecidos.

Para determinar esto con exactitud, deben utilizarse los siguientes criterios para definir las necesidades específicas del *site* y para determinar las alternativas de procesamiento más apropiadas:

- Disponibilidad y confiabilidad de la instalación alterna.
- Compatibilidad del hardware
- Compatibilidad del software
- Dimensión física de la instalación alterna.
- Apoyo para las instalaciones ambientales
- Apoyo para las comunicaciones
- Apoyo de personal
- Consideraciones logísticas
- Suficientes periodos para pruebas

- Seguridad
- Costo-efectividad
- Requisitos contractuales

No debemos olvidar que aunque lo ideal sería reproducir en un 100% el ambiente de cómputo con el que se contaba previamente al siniestro, esto no puede realizarse en la mayoría de los casos debido al alto costo que representa. Por lo tanto, se debe encontrar un equilibrio entre el presupuesto de la empresa y el poder proporcionar la capacidad de procesamiento para que la empresa pueda continuar operando en un nivel establecido por esta misma.
Para terminar esta etapa, se puede decir que hasta que no exista un balance de los requerimientos bien preparado y aprobado por los usuarios, técnicos y alta dirección, no habrá una decisión correcta. Finalmente, es importante recordar que no existe necesariamente una solución correcta. La planeación de contingencia es un costo necesario de estar en el negocio si uno quiere permanecer en pie después de un evento de contingencia.

Tarea 2.- Formación de Equipos

Equipos Operativos
Sus labores serán:
- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, entre otros., para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, modem, otros aditamentos para comunicaciones.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres.

Equipos de Evaluación (auditoria del cumplimiento de los procedimientos sobre Seguridad)
Esta función debe ser realizada de preferencia por personal de auditoria, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:
- Revisar que las Normas y procedimientos con respecto a *Backups* y seguridad de equipos y datos se cumpla.

- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la Institución y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

Etapa 2. Actividades durante el Desastre.

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

Tarea 1 Plan de Emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas (Declaración de Desastre).

Es conveniente prever los posibles escenarios de ocurrencia del siniestro:

- Durante el día.
- Durante la Noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- Vías de salida o escape.
- Plan de Evacuación del Personal.
- Plan de puesta a buen recaudo de los activos de la Institución (incluyendo los activos de Información si las circunstancias del siniestro lo permiten)
- Ubicación y señalización de los elementos contra el siniestro (extintores, cobertores contra agua, entre otros.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

Tarea 2. Formación de Equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, entre otros.) con funciones claramente definidas a ejecutar durante el siniestro.

<u>Equipos de contingencia.</u>

El objetivo de esta tarea es definir los equipos de contingencia.

Las acciones que se deben tomar para efectuar el restablecimiento de un desastre, son llevadas a cabo por equipos de recuperación, cada uno con su propia área de responsabilidad.

Al realizar esta tarea, debemos recordar que estamos planeando para el peor de los casos, la destrucción total de la instalación de cómputo; también hay que considerar que la definición de los equipos debe ser en términos de responsabilidades del equipo y de su membresía, es decir, las áreas que estarán representadas en el equipo, así como sus funciones específicas durante la recuperación en caso de desastre.

Obviamente, se deben adaptar los equipos a las circunstancias existentes, dependiendo de factores tales como número, tamaño y sofisticación del centro de cómputo e importancia de la función de sistema en la empresa.
Lo que se presenta a continuación constituye tan solo una recomendación sobre la forma en que podrían organizarse los equipos de contingencia, así como las funciones que se les asignarían.

Coordinador del plan de contingencia.
Sus funciones son las siguientes:

- Decidir si se declara la contingencia o no, si únicamente se establecen medidas temporales de seguridad.
- Vigilar que el plan permanezca actualizado y adecuado (actualización, mantenimiento y pruebas)
- Se encarga de la administración y el manejo del presupuesto que se ejerza durante la puesta en marcha del plan
- Vigilar que la instalación de respaldo seleccionada se mantenga con las condiciones necesarias para cumplir las especificaciones.

Sub-coordinador del plan de contingencia.
Sus funciones son las siguientes:

- Obtener las provisiones y servicios generales necesarios durante la contingencia hasta el restablecimiento de operaciones normales.
- Autorizar y vigilar el acceso a la caja de seguridad externa
- Mantener el contenido e inventario de la caja de seguridad actualizado y completo. La decisión de alguna nueva inclusión o exclusión será en conjunto con el coordinador.
- Notificar a la compañía de seguros.

Equipo de comunicaciones.
Sus funciones son las siguientes:

- Dotar de todas las comunicaciones y telecomunicaciones necesarias a la instalación de respaldo, tratando de evitar la discontinuidad en el funcionamiento de los sistemas a causa de problemas en las telecomunicaciones, de manera especial, las comunicaciones entre la instalación de respaldo y las entidades con las que normalmente tiene comunicación frecuente la empresa. A este respecto, la telefonía celular como posible respaldo para comunicaciones. Los teléfonos celulares constituyen una inversión inicial, así como un gasto constante, pero las organizaciones que han estado en un desastre y los han usado pueden testificar que ese costo es pequeño en comparación con el enorme beneficio que se obtiene.
- Realizar todo lo necesario para instalar la infraestructura de comunicaciones en el nuevo centro de procesamiento de datos o reinstalarla en el centro en reparación.

Equipo de representantes de usuarios.

Sus funciones son las siguientes:

- Comunicar a sus respectivas áreas los procedimientos de operación durante la contingencia, además de supervisar a las personas de sus respectivas áreas que van a trabajar en la instalación de respaldo.
- Ver que el lugar en la instalación de respaldo en donde llegarán los usuarios a trabajar, cuente con todo lo necesario.
- Ellos constituirán el puente entre la instalación de respaldo y el local donde se encuentra la empresa.
- En el caso de un desastre natural de alcance regional, los directores de cada área deben enterarse bien de la situación de los subordinados.

Equipo evaluador.

Sus funciones son las siguientes:

- Debe evaluar el daño al centro de cómputo y en general a todo el equipo y redes de cómputo con que cuenta la empresa, así como el daño a los sistemas, a la información, entre otros. Para esto, debe servirse del inventario que realizó previamente. También es su deber rescatar lo que aún puede servir.

Equipo de organización y operación de la instalación de respaldo.

Sus funciones son las siguientes:

- Llevar la información (cintas y discos) pertinente, de acuerdo con lo establecido al plan de recuperación y las indicaciones del coordinador del plan
- Llevar e instalar todo el software y hardware necesario para que puedan procesarse los sistemas críticos.
- Operar el sistema y llevar a cabo todos los procesos necesarios de acuerdo con el plan de producción en contingencia diseñado por ellos mismos.

Equipo de recuperación de instalaciones.

Sus funciones son las siguientes:

- Con base en el inventario y en el diagnostico del equipo de evaluación, deberá concentrarse en la reconstrucción de todas las instalaciones de cómputo, obedeciendo las indicaciones del coordinador del plan.
- También debe asegurar la disponibilidad del hardware necesario en la instalación de respaldo. Esta tarea la realiza en forma conjunta con el equipo de organización y operación de la instalación de respaldo.

Equipo de apoyo al personal.

Finalmente consideramos la creación de otro equipo que, aunque no es propiamente operativo del plan de recuperación, es posiblemente el más importante ya que si no actúa en forma eficiente y expedita todo el plan de recuperación podría haberse paralizado por falta de personal que lo ejecute.

Sus funciones son las siguientes:

- Proveer asistencia y primeros auxilios al personal herido.
- Alertar a los servicios médicos para que concurran en auxilio del personal afectado.
- Debe proveer apoyo para los requerimientos personales de los empleados.

- Se debe tratar de resolver cualquier necesidad de la familia del empleado.
- Además, debe formarse un equipo de denominaremos "manejo de desastres", el cuál esta formado por el coordinador y el sub-coordinador del plan de recuperación, así por los lideres de los demás equipos de contingencia. Este equipo se constituye como el órgano máximo de decisión durante la recuperación, así como en las revisiones de las pruebas y el mantenimiento del plan. Entre otras, tiene la función, de diseñar el plan de regreso a la instalación de cómputo de la empresa, fijando tiempos, acciones, entre otros. También tiene la función de dar coherencia y organización a las acciones durante la recuperación.

Formación de los equipos de contingencia.

Una vez que se han definido los equipos, es necesario integrarlos con las personas más adecuadas. Por lo tanto, formar los equipos requiere de la identificación del personal que tiene las habilidades y conocimientos necesarios para desempeñar las tareas que les son asignadas. Hay que tener en cuenta que debido a que cada equipo tiene su función, sus miembros solo necesitan la capacidad para realizar los procedimientos correspondientes a sus funciones.
Se propone que cada equipo de contingencia cuente con los siguientes integrantes:

Líder: debe coordinar las actividades del equipo, posee un conocimiento global de todo el plan de contingencia y es miembro del equipo de manejo de desastres.
Líder suplente: suplirá al líder en todas sus funciones en caso de éste falte.
Miembros: los integrantes del equipo (el número de ellos depende de la complejidad y extensión de las tareas) conocen únicamente las funciones de su equipo en la recuperación de desastres. Algunas personas pueden ser miembros de más de un equipo.
Con el fin de evitar la deserción de los integrantes de los equipos de contingencia en el momento de un desastre, la empresa debe proveer soporte a las necesidades personales de los empleados si espera que estén disponibles para llevar a cabo las operaciones de recuperación. Esto se debe a que si una calamidad destruye el centro de cómputo, es posible que también haya dañado los hogares o las familias de los empleados. En este caso, los empleados no querrán dejar a su familia a menos que tengan la seguridad de que recibirán protección y ayuda. Este es el objetivo del equipo de apoyo al personal.

Un plan de contingencia realista reconoce que no puede ser mejor que la gente que lo ejecuta. Especialmente en esta metodología, se confía mucho en las personas que desempeñarán las tareas requeridas para la recuperación, muchas de las cuales tendrán que ser por iniciativa propia. Por eso, resulta muy importante la selección del personal adecuado para los equipos de contingencia.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, entre otros.), deberán de existir al menos dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de

prioridades, minimizando la suspensión o pérdida completa del procesamiento de cómputo.

Etapa 3. Actividades después del Desastre.

También se conoce esta fase como "ponerlo en marcha". Es decir, pasarlo de la teoría a la práctica, dejándolo listo para activarse en cualquier momento que se necesite. Para esto, el plan ya debe ser conocido por todas la personas que deban conocerlo y los miembros de los equipos de recuperación deben tener la capacidad de llevar a cabo sus asignaciones en la mejor forma.

Tarea 1. Evaluación de Daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar y en cuanto tiempo, entre otros.
Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

Tarea 2. Priorización de Actividades del Plan de Acción

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.
Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

Tarea. 3. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

Tarea 4. Evaluación de Resultados.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, entre otros.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

Fase 3. Administración del plan

La administración del plan de recuperación de desastres se divide en 4 tareas fundamentales:

- Distribución
- Mantenimiento
- Entrenamiento
- Pruebas al plan.

Tarea 1. Distribución del Plan de Recuperación de Desastres.
El procedimiento para la distribución del plan debe informar de dicho plan a los equipos participantes y al resto de la organización. En la lista de contactos se podrá encontrar los nombres de todas las personas a las que se debe distribuir el documento del Plan de Recuperación de Desastres.

La adecuada distribución y promoción del plan determinarán finalmente su buen éxito. Es por ello indispensable, que el líder de cada uno de los equipos debe asegurarse de que todo su equipo, esté perfectamente enterado de la visión global del plan, de su papel y de la responsabilidad que se le esta encomendando.

El líder puede tomar ventaja de toda la diversidad de medios informativos disponibles a su alcance para distribuir el plan a su equipo, pero los medios usados deben alcanzar a todo el universo posible de participantes.

Tarea 2. Mantenimiento del Plan de Recuperación de Desastres.
Como toda organización cambia, el plan constantemente debe someterse a una revisión y adecuación constante, que lo mantenga vigente para todos los cambios de tecnología y de estructura organizacional.

Básicamente se pueden definir dos tipos de actividades de mantenimiento:
Mantenimiento programado.- Este esta dirigido a comprobar la validez de la información que por no ser relevante para el desarrollo de tecnologías pueden pasar desapercibidas, tal puede ser el caso de un número telefónico particular de uno de los líderes o de algún proveedor.
Mantenimiento eventual.- Corresponde a las modificaciones disparadas por eventos suscitados, como puede ser cambios de plataforma, liberación de nuevas aplicaciones, cambios en la estructura organizativa, entre otros.

El mantenimiento del plan es un requisito indispensable para garantizar su efectividad. Como referencia cabe mencionar que las empresas aseguradoras en Estados Unidos, consideran, para ciertos sectores industriales, que un plan que no se ha revisado en más de seis meses esta desactualizado y por lo tanto no garantiza la continuidad del servicio.

Las siguientes preguntas ayudan a evaluar el plan:

¿Es adecuado el plan, para los casos de desastre presentados hasta ahora?
¿Soporta el plan, cambios a futuro de crecimiento y desarrollo?

¿Han surgido nuevas vulnerabilidades o amenazas no contempladas hasta ahora en el plan?
¿Se están repitiendo con frecuencia eventos similares de desastre?
¿Se detectaron fallas o "huecos" en el plan durante los ensayos?
¿Es clara la información escrita en el plan?
¿Se están cumpliendo los objetivos originales del plan?
¿Se están respaldando y recuperando adecuadamente los registros vitales?
¿El equipo DRP esta respondiendo a casos específicos de recuperación de desastres?
¿Es correcta la secuencia de tareas, propuesta por el plan para la recuperación de desastres?
¿Están todas las aplicaciones críticas incluidas en el plan?
¿Está actualizada la lista de datos de todos los equipos del DRP?
¿Se están administrando correctamente los datos almacenados fuera de sitio?
¿Se han cambiado los contratos con los proveedores, para ajustarse al plan?
¿Se ha cambiado el software o hardware, para cumplir las demandas del plan?

Tarea 3. Entrenamiento para la Recuperación de Desastres

El plan de entrenamiento, tiene la función de mejorar la capacitación, preparación y coordinación de los equipos de recuperación, proveedores, operadores y áreas involucradas con el fin de minimizar la toma de decisiones y retrasos ocurridos antes, durante y después de un desastre.

Premisas

Todos los miembros de los equipos de recuperación, usuarios o proveedores, requieren ser entrenados en el plan de recuperación de desastres.

El entrenamiento debe incluir, sesiones de información y discusión de actividades y responsabilidades, notificación y declaración de desastres, procedimientos de recuperación, pruebas de escenarios y regreso a operaciones normales.

A continuación, se describen los aspectos fundamentales que pueden considerarse cuando se impartan cursos de entrenamiento del plan de recuperación:

Enfoque del entrenamiento.

Las siguientes preguntas ayudan a determinar el enfoque que deben tener las sesiones de entrenamiento:
¿Quién será entrenado?
¿Quién hará el entrenamiento?
¿Qué temas serán discutidos o mostrados en el entrenamiento?
¿Cuándo y en donde tendrán lugar las sesiones de entrenamiento?
¿Cómo será evaluada y documentada la sesión?

Actividades de entrenamiento.

El entrenamiento puede tener diferentes actividades:
Sesiones de orientación y educación: Estas sesiones son para dar a conocer a cada miembro sus responsabilidades y funciones dentro del plan de recuperación.
Sesiones de revisión: Son sesiones donde todos los miembros discuten y revisan sus funciones responsabilidades, bajo diversos escenarios de desastre.
Sesiones de simulación: Son sesiones, donde se involucra a todas las áreas a participar en las pruebas de ejecución del plan de recuperación de desastres.

Sesiones de evaluación: Son sesiones donde se evalúa el resultado de las pruebas y simulacros de desastre.

Los tópicos a considerar para los entrenamientos son los siguientes:
Información de funciones individuales y responsabilidades.
Información acerca de amenazas, vulnerabilidades y evasión de desastres.
Notificación y declaración de desastres.
Respuestas concretas para casos específicos de desastre.
Procedimientos de recuperación en los sitios de respaldo.
Procedimientos para regresar a la operación normal

Tarea 4. Pruebas al Plan de Recuperación de Desastres.
Las pruebas al Plan de Recuperación en caso de desastre son la única manera confiable de asegurar que el plan funciona y es efectivo en el caso de un desastre real. Mientras más real una prueba simule los efectos de un desastre sobre los recursos de Información Tecnológica, más útil y concluyente será esta. Las pruebas deberán validar por lo menos una vez al mes que los registros vitales se encuentran disponibles y que estos pueden ser recuperados y utilizados.

Las pruebas de Recuperación en caso de desastre son una responsabilidad compartida entre el equipo DRP y los usuarios finales y ambas partes deben estar de acuerdo con los objetivos de las pruebas. El equipo DRP normalmente se encargará de la simulación de la recuperación mientras que el usuario deberá validar junto con el equipo DRP, los resultados de las pruebas. El usuario final será el encargado de dar la aprobación final de los resultados de las pruebas. Debe tomarse el debido cuidado al asegurarse de que la totalidad del plan es probado.

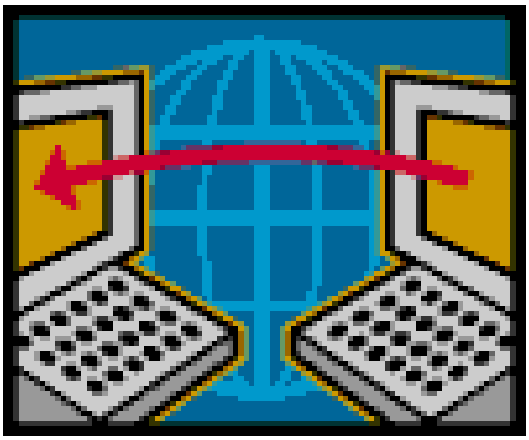
Cuando se analizan los posibles eventos que pueden crear situaciones de contingencia, lo que se está haciendo en realidad es simular eventos que generen desastres, para proceder a prevenirlos o en su caso corregirlos oportunamente cuando se presenten.

Frecuencia de Pruebas:
Para ser útil, un Plan de Recuperación en caso de desastre debe mantenerse actualizado. Cambios en la tecnología, requerimientos del negocio y cambios en las regulaciones de gobierno pueden causar un continuo cambio en el ambiente de sistemas. Cuando estos cambios tienen lugar, la evaluación del riesgo, los requerimientos para la planeación de recuperación en caso de desastre y los planes de recuperación en caso de desastre necesitan ser revisados para determinar si se requiere hacer cambios a estos.

Durante las pruebas de recuperación en caso de desastre es frecuente que los equipos identifiquen errores en los diferentes supuestos o procesos que necesitaran ser corregidos o cambiados en la Planeación de Requerimientos de Recuperación en caso de desastre y/o en el Plan de Recuperación en caso de desastre. Estas correcciones o cambios deben realizarse antes de la preparación del reporte final de la prueba.

En este capítulo se trataron los temas teóricos para la elaboración de planes de recuperación de desastres, culminando con la propuesta de un método el cual es un resultado del trabajo de investigación expuesto a lo largo de los capítulos anteriores. Para terminar con nuestro trabajo en el capítulo siguiente utilizamos este método propuesto para la realización de un caso práctico de un DRP para una empresa de Telecomunicaciones que depende 100 % de su información tecnológica.

Capítulo 5



Caso práctico de un DRP en la compañía de telecomunicaciones "Directv México"

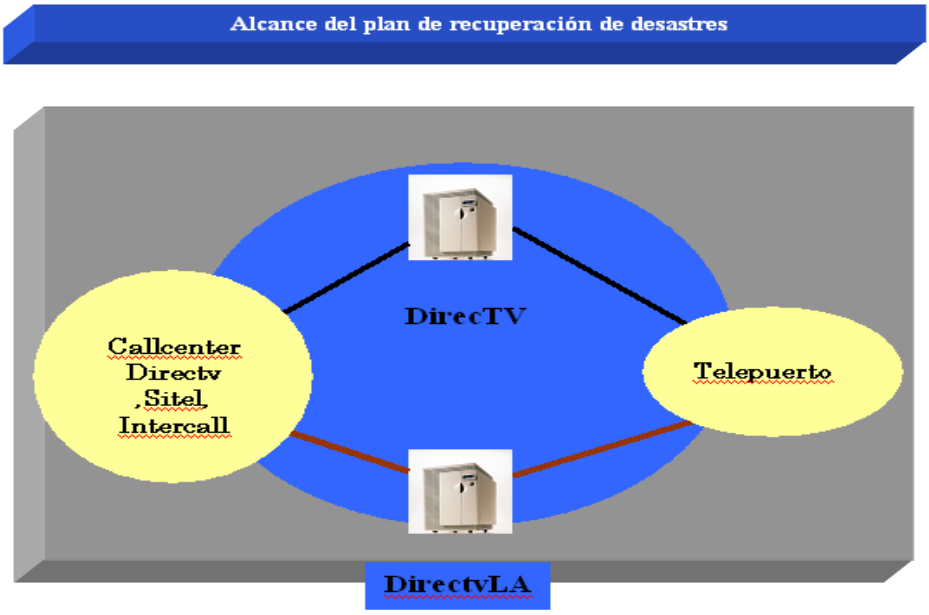
5.1 Visión General

Introducción al Plan de Recuperación de Desastres.
Grupo Galaxy Mexicana (Directv), es una empresa especializada en servicios de comunicación y de entretenimiento vía satélite, ha mostrado en los últimos años un aprovechamiento importante de tecnología moderna, incrementando fuertemente sus operaciones diarias. Ante este hecho, no ha dudado en proteger sus operaciones más importantes y los servicios de cómputo más críticos, de la interrupción no programada de sus operaciones por un desastre. Dado que cualquier interrupción podría inclusive afectar el cumplimiento de su operación comercial y causar grandes pérdidas monetarias, ha desarrollado un plan de recuperación de desastres para el área de Tecnología de Información.

Este plan de recuperación de desastres es el resultado de un esfuerzo conjunto de ideas, análisis y experiencias obtenidas durante el estudio y desarrollo de este tema de tesis por lo que se elaboró de acuerdo a los lineamientos del método propuesto en el capítulo 4.

Tarea1.- Establecer su objetivo general y su alcance
Este plan de recuperación de desastres esta desarrollado para cubrir el alcance que detalla la Figura 5.1, la cual muestra la operación actual de los sistemas de Directv y en caso de que ocurriera un desastre de tal manera que no se contara con acceso al site, como nuestro centro de respaldo será sustituido por un hot-site conocido como DirectvLa (Directv Latinoamérica) ubicado en Miami Florida.

Figura 5.1[1]



Este plan de recuperación contempla los siguientes objetivos:
- La restauración del sistema IBS y la recuperación de sus datos.
- La recuperación del centro de cómputo principal de Directv, ubicado en Blvd. Manuel Ávila Camacho No. 1-101, edificio "INVERLAT", Piso 1, Colonia Lomas de Chapultepec, México D.F.

[1] Figura elaborada por los realizadores de la presente tesis.

- El uso del centro operativo en Directv Latinoamérica, con domicilio en Fort Lauderdale, Florida USA.
- La recuperación de enlaces de comunicación de Directv México, DirectvLa y los centros de atención.
- La designación de gente para la logística y operación del plan de la recuperación.

Los objetivos del plan de recuperación de desastres, están enfocados a prevenir y corregir la interrupción de la aplicación que más impacto tiene para el negocio.

Tarea 2.- Personal que realizará el plan

El plan en original fue realizado por un despacho de consultoría externa, sin embargo el presente fue diseñado por los realizadores de esta tesis.

5.2 Plan de Recuperación de Desastres.

5.2.1 Etapa 1.- Actividades previas al desastre.

Tarea 1.- Establecimiento del plan de acción

a) Inventario y recursos críticos.

De acuerdo al estudio "análisis de impacto en el negocio" como se verá en el inciso b) se determina que la actividad o aplicación crítica del negocio es el sistema IBS.

En la figura 5.2 se presenta un inventario de equipos de cómputo, los cuales mantienen la operación diaria de la empresa, sin embargo los equipos de mayor riesgo son los servidores de bases de datos donde reside la aplicación IBS y que cubre el presente DRP.

b) Análisis de riesgos

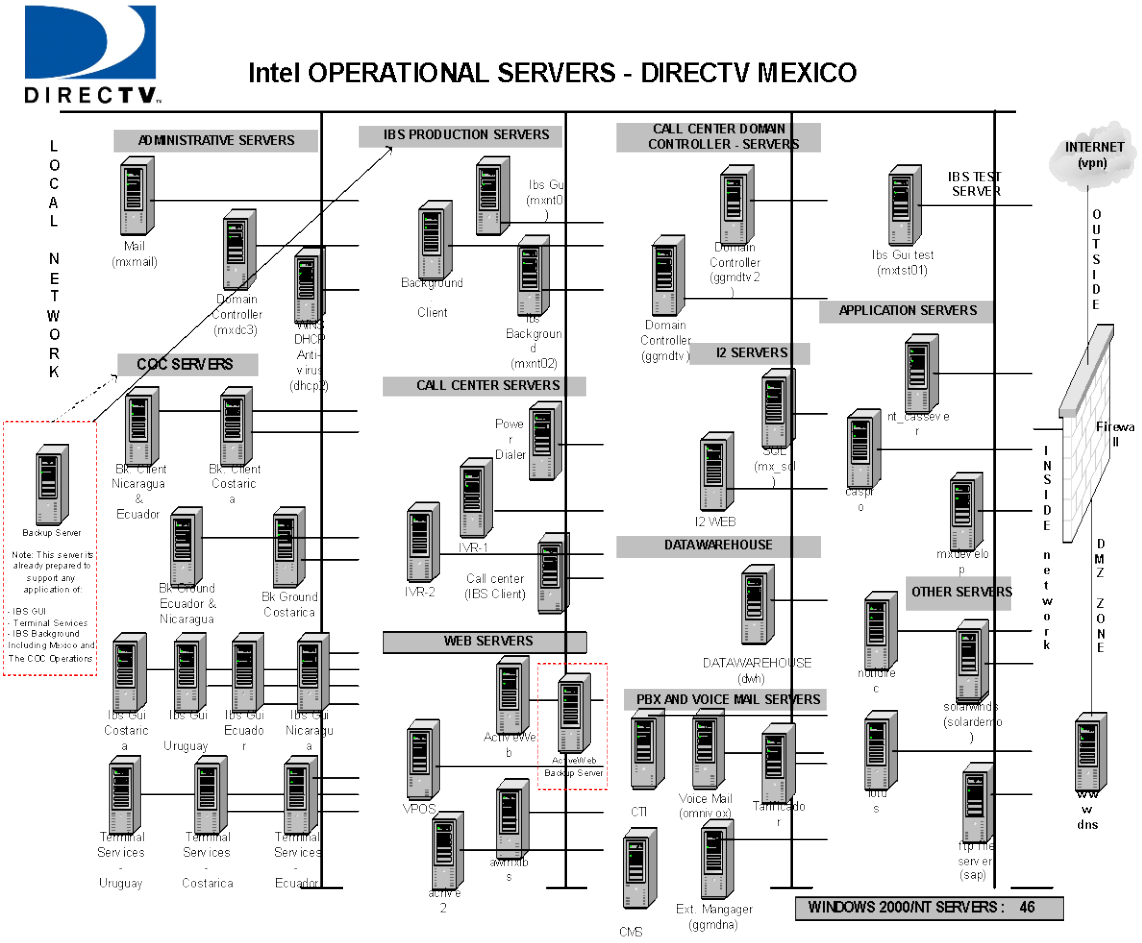
<u>Identificación de riesgos.</u>

Las vulnerabilidades y amenazas que contempla este plan son las siguientes:

- ✓ Rayos y/o truenos
- ✓ Huelgas y/o paros sindicales (que afecten el edificio o instalaciones de Directv)
- ✓ Interrupciones de suministro eléctrico (que afecten el edificio o instalaciones de Directv)
- ✓ Choque de aeronave, cerca o en el edificio
- ✓ Amenaza de bomba o explosivo (que afecten el edificio o instalaciones de Directv)
- ✓ Derrame y/o fuga de químicos
- ✓ Desalojo sorpresivo de edificios u oficinas
- ✓ Disturbios sociales y/o manifestaciones (que afecten el edificio o instalaciones de Directv)
- ✓ Estructura endeble del edificio
- ✓ Fuego y/o incendio
- ✓ Inundaciones (que afecten el edificio o instalaciones de Directv)
- ✓ Fugas de agua
- ✓ Fuga de gas o material tóxico
- ✓ Sabotaje externo (hackers, ciberterrorismo)
- ✓ Sabotaje interno de empleados disgustados
- ✓ Líneas dedicadas afectadas
- ✓ Accidentes en construcciones vecinas

- ✓ Explosión cerca o en el edificio.
- ✓ Fallas de hardware que el proveedor no pueda resolver en los tiempos pactados
- ✓ Terremoto
- ✓ Erupción volcánica

Figura 5.2 Infraestructura de los sistemas[2]:



Las vulnerabilidades y amenazas que no contempla este plan son las siguientes:

- ✓ Epidemias y/o enfermedades (que afecten el edificio o instalaciones de Directv)
- ✓ Nevada / Tormenta de hielo
- ✓ Sequía
- ✓ Tormenta de arena
- ✓ Temperaturas extremas
- ✓ Hambruna
- ✓ Huracán
- ✓ Paro masivo de tráfico
- ✓ Tornado
- ✓ Tifón
- ✓ Derrame de desperdicios

[2] Autor: Gerente de telecomunicaciones y administrador de servidores de Directv

El siguiente listado menciona amenazas, las cuales se esperan sean solucionadas a través de procedimientos normales de operación y no requieren ser incluidos dentro de un Plan Recuperación de Desastres.

- Humedad extrema
- Error humano
- Uso indebido de usuarios finales
- Errores de procedimientos
- Errores en la programación
- Utilización de datos erróneos
- Disfunción de software
- Virus de software
- Acceso no autorizado a los datos
- Acceso no autorizado para el manejo del respaldo de datos

Riesgos identificados para la ejecución del Plan:
En el desarrollo del presente plan hemos detectado algunos riesgos potenciales que ponen en peligro la ejecución efectiva del DRP. A continuación enumeramos los que consideramos más significativos:

La configuración del equipo con el que cuenta el centro alterno de procesamiento no tiene las mismas características del equipo localizado en el centro de procesamiento central por lo que la operación en este centro será degradada.

Al momento de recuperar los datos en el centro de procesamiento alterno, habrá una pérdida de datos por la operación que haya transcurrido entre el último respaldo trasladado fuera de sitio y el momento en que ocurre el desastre.

Al momento de declarar el desastre el equipo de respaldo DirectvLa, puede estar en uso por otro cliente que notificó primero el desastre y por lo tanto ocupo primero el servidor de respaldo.

Técnicas de análisis.

a) Análisis cuantitativo.

Cálculo de pérdida probable

Para realizar el cálculo de la pérdida probable nos apoyamos en el modelo de regresión lineal expuesto en la sección 2.3.1.1 del capítulo 2. De esta manera obtendremos una proyección de las necesidades futuras del sistema y se destacará la importancia de mantenerlo en línea las 24 horas del día.

La figura 5.3 muestra la estadística de llamadas durante el periodo Enero-Junio del año 2004 para las áreas Customer Care, Recuperación de Cartera y Activaciones, áreas potenciales de fuente de ingresos de la compañía , no se muestran estadísticas del departamento de Telemarketing por razones que se exponen en la siguiente sección denominada "Análisis de impacto en el negocio".

Figura 5.3[3]

	Histórico de llamadas mensuales durante el periodo Enero-Junio 2004					
Area	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**
Customer Care	119,050	119,975	120,325	120,100	119,900	120,650
Recuperación de Cartera	18,975	21,250	23,550	19,975	23,800	24,450
Activaciones	8,400	7,050	9,450	8,400	8,800	11,900

Aplicando Regresión Lineal al área Customer Care tenemos:

Customer Care	**X**	**Y**	**X²**	**XY**	**Y²**
	1	119,050	1	119,050	14,172,902,500
	2	119,975	4	239,950	14,394,000,625
	3	120,325	9	360,975	14,478,105,625
	4	120,100	16	480,400	14,424,010,000
	5	119,900	25	599,500	14,376,010,000
	6	120,650	36	723,900	14,556,422,500
Suma	**21**	**720,000**	**91**	**2,523,775**	**86,401,451,250**
Promedio	**4**	**120,000**	**15**	**420,629**	**14,400,241,875**

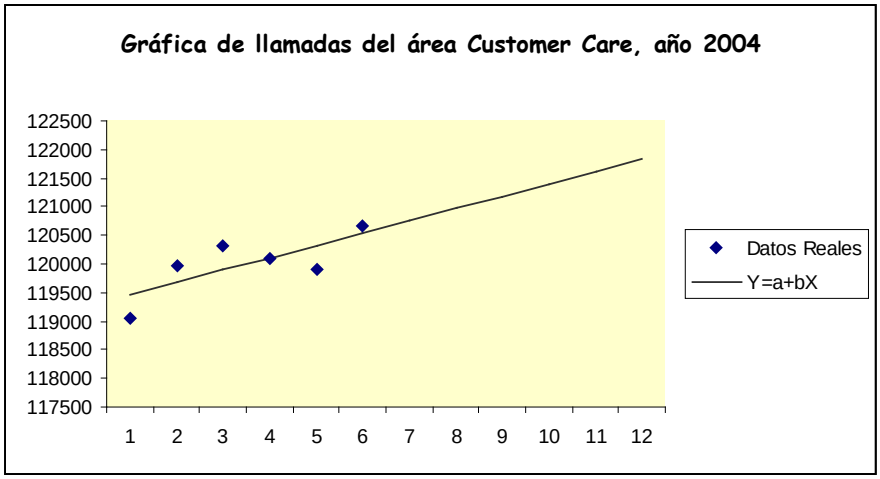
Sustituyendo las fórmulas:

$$b = \frac{\sum XY - \frac{\sum X * \sum Y}{n}}{\sum X^2 - \frac{(\sum X)^2}{n}} \quad \text{y} \quad a = \overline{Y} - b\overline{X}$$

$\Longrightarrow$ b= 215.71 y a= 119245

Por lo tanto la función lineal aproximada para estimar el comportamiento de las llamadas durante el siguiente semestre del año es: $\hat{Y} = a + bX$ $\Longrightarrow$ $\hat{Y} = 119245 + (215.71 * X)$ quedando gráficamente de la siguiente manera:

Figura 5.4



[3] Estadística proporcionada por Gerente de Call Center de DirecTV

Aplicando Regresión Lineal al área de Recuperación de Cartera tenemos:

Recuperación de cartera	X	Y	X²	XY	Y²
	1	18,975	1	18,975	360,050,625
	2	21,250	4	42,500	451,562,500
	3	23,550	9	70,650	554,602,500
	4	19,975	16	79,900	399,000,625
	5	23,800	25	119,000	566,440,000
	6	24,450	36	146,700	597,802,500
Suma	**21**	**132,000**	**91**	**477,725**	**2,929,458,750**
Promedio	**4**	**22,000**	**15**	**79,621**	**488,243,125**

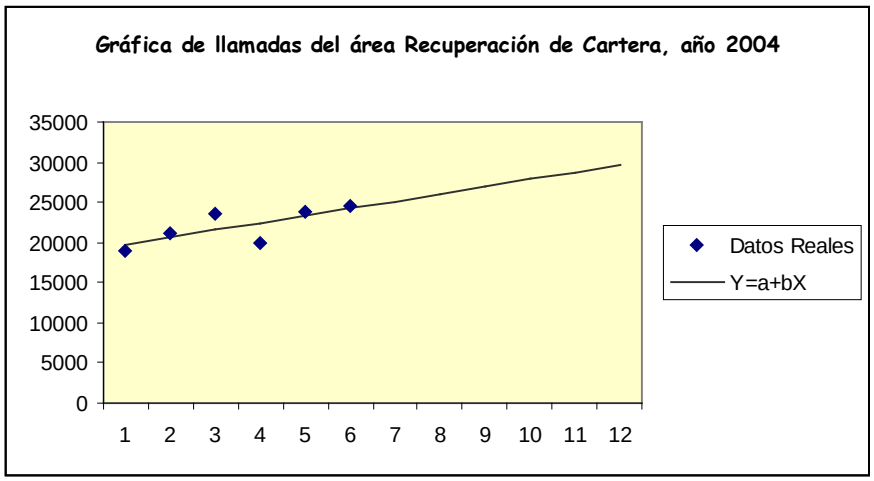
Sustituyendo las fórmulas:

$$b = \frac{\sum XY - \frac{\sum X * \sum Y}{n}}{\sum X^2 - \frac{(\sum X)^2}{n}} \quad \text{y} \quad a = \overline{Y} - b\overline{X}$$

⟹ b= 898.57 y a= 18855

Por lo tanto la función lineal aproximada para estimar el comportamiento de las llamadas durante el siguiente semestre del año es: $\hat{Y}$ = a + bX ⟹ $\hat{Y}$ = 18855 + (898.57 * X) quedando gráficamente de la siguiente manera:

Figura 5.5



Aplicando Regresión Lineal al área de Activaciones tenemos:

Activaciones	X	Y	X²	XY	Y²
	1	8,400	1	8,400	70,560,000
	2	7,050	4	14,100	49,702,500
	3	9,450	9	28,350	89,302,500
	4	8,400	16	33,600	70,560,000
	5	8,800	25	44,000	77,440,000
	6	11,900	36	71,400	141,610,000
Suma	**21**	**54,000**	**91**	**199,850**	**499,175,000**
Promedio	**4**	**9,000**	**15**	**33,308**	**83,195,833**

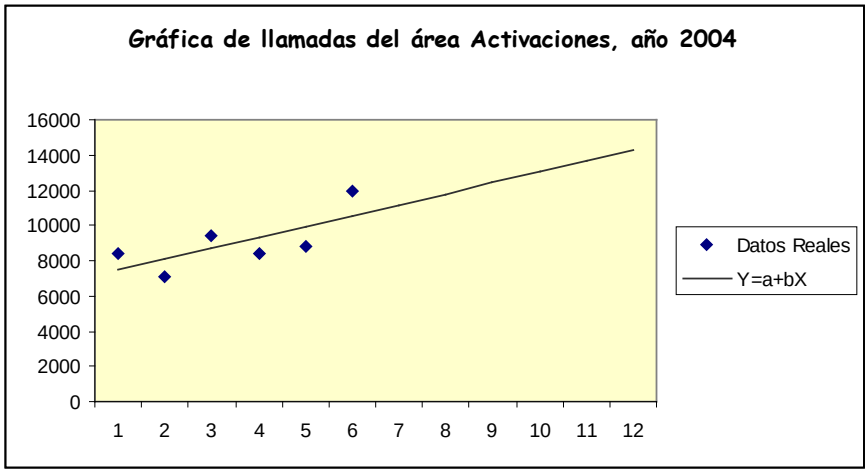
Sustituyendo las fórmulas:

$$b = \frac{\sum XY - \frac{\sum X * \sum Y}{n}}{\sum X^2 - \frac{(\sum X)^2}{n}} \quad \text{y} \quad a = \overline{Y} - b\overline{X}$$

⟹ b= 620 y a= 6830

Por lo tanto la función lineal aproximada para estimar el comportamiento de las llamadas durante el siguiente semestre del año es: $\hat{Y}$ = a + bX ⟹ $\hat{Y}$ = 6830 + (620 * X) quedando gráficamente de la siguiente manera:

Figura 5.6



Ahora aplicando el coeficiente de correlación para las distintas áreas se tiene la formula:

$$R^2 = \frac{\left[\sum XY - \frac{\sum X \sum Y}{n}\right]^2}{\left[\sum X^2 - \frac{(\sum X)^2}{n}\right] * \left[\sum Y^2 - \frac{(\sum Y)^2}{n}\right]}$$

Sustituyendo obtenemos los siguientes resultados:

Coeficiente de correlacion		
Area	**R^2**	**%**
Customer Care	0.561	56.1117
Recuperación de Cartera	0.555	55.5017
Activaciones	0.511	51.0588

Como se puede observar en todos los casos, el porcentaje del coeficiente de regresión es mayor al 50% el cual indica la representación bajo la regresión lineal del comportamiento de las llamadas. En general podemos observar la tendencia de las llamadas es positiva, por lo que en función del tiempo, las áreas pronosticadas son cada vez más dependientes del sistema de cómputo. Para visualizar una aproximación en unidades monetarias se recomienda ver la Figura 5.7

Figura 5.7[4]

Función	Impacto en la calidad del servicio	Impacto Económico	Pérdida mínima esperada en valores monetarios
* Cancelaciones	Sí Provoca mayor irritación en los clientes	Sí	No es posible determinarlo exactamente, se estima en la última linea de este cuadro
* Reportes de problemas en Audio y Vídeo	Sí	Sí Puede producir cancelaciones	No es posible determinarlo exactamente, se estima en la última linea de este cuadro.
* Información General	No	No	No es posible determinarlo exactamente, se estima en la última linea de este cuadro
Explicación y ajustes de saldos de clientes	Sí 25 % de las llamadas en promedio por hora	Sí Puede producir cancelaciones	Si suponemos que al menos el 50% de las llamadas cancelara el servicio y estos clientes tuvieran la programación básica, es decir el paquete plata, Directv dejaría de percibir una cifra aproximada $ 13 615 por hora en este rubro
* Requisición de facturas	Sí	Sí Oportunidad en la recuperación de cartera	No es posible determinarlo exactamente, se estima en la última linea de este cuadro
Problemas en el equipo del cliente	Sí 25% de las llamadas en promedio por hora	Sí Puede producir cancelaciones	Si suponemos que al menos el 50% de las llamadas cancelara el servicio y estos clientes tuvieran la programación básica, es decir, el paquete plata, Directv dejaría de percibir una cifra aproximada $ 13 615 por hora en este rubro
Venta de servicios como NFL Directv, NBA Directv, BOX Directv, Baseball	Sí 5 % de las llamadas en promedio por hora (promedio durante temporada)	Sí Representa un costo significativo por hora de servicio	Si suponemos que el 50% de las llamadas contrataran un PPV y el otro 50% contratara la temporada completa. Directv dejaría de percibir una cifra aproximada de $ 3039 por hora en ese rubro
Información y venta de Pagos por Evento (PPV)	Sí 12.5 % de las llamadas en promedio por hora	Sí Representa un costo significativo por hora de servicio	Asumiendo que el 100% de las llamadas contratara un PPV del precio mínimo, Directv dejaría de percibir una cifra aproximada de $ 673 por hora en este rubro
* Problemas técnicos	Sí	Sí Puede producir cancelaciones	No es posible determinarlo exactamente, se estima en la última linea de este cuadro
* Programación (Activación de productos/paquetes)	Sí	Sí Puede producir cancelaciones	No es posible determinarlo exactamente, se estima en la última linea de este cuadro
Pagos	Sí 5 % de las llamadas en promedio por hora	Sí	No es posible determinarlo exactamente, estos pagos se puede aplicar posteriormente
* Problemas en Pagos por Evento	Sí	Sí Puede producir cancelaciones	No es posible determinarlo exactamente, se estima en la última linea de este cuadro
* Incluye los rubros marcados con (*)	27.50%	Suponiendo que el 50% de cancelara el servicio.	Si estos clientes tuvieran la programación básica, es decir, el paquete plata, Directv dejaría de percibir una cifra aproximada $ 14 977 por hora en la suma de estos rubros.

[4] Figura elaborada por los realizadores de la presente tesis.

Análisis de impacto en el negocio (Business Impact Analysis)

El BIA provee la base para las prioridades de planeación, recuperación y la selección de las estrategias que reflejen un balance óptimo entre las inversiones y los riesgos.

El objetivo principal del BIA es proveer un análisis de los costos asociados con la interrupción de las operaciones en el centro de operación de Directv. Como resultado de este análisis, la estrategia de recuperación ha sido identificada y se espera que reduzca el impacto en la continuidad de las operaciones de Directv en caso de que ocurra un desastre.

Las actividades para lograr esto han sido:

- Identificar las funciones críticas del negocio
- Estimar el impacto económico y operacional de un desastre en el centro de operación de Directv.

Directv ha establecido que las funciones soportadas por la aplicación IBS son críticas para la operación del negocio por lo que desde un principio se determinó esta aplicación como la única crítica.

Pérdida de ingresos

En el caso de una interrupción en el centro de operación de Directv, hay cuatro fuentes potenciales de pérdida de ingresos que deben ser consideradas y protegidas:

- Customer Care
- Recuperación de Cartera
- Activaciones
- Telemarketing

Directv actualmente maneja su propio Centro de Atención a Clientes, cuenta con más de 190 operadores que ofrecen servicios de atención telefónica cubriendo las áreas mencionadas anteriormente.

Directv Customer Care.

Las Funciones del Negocio soportadas por Directv Customer Care son:

- Cancelaciones
- Reportes de problemas en Audio y Vídeo
- Información general
- Explicación y ajustes de saldos de clientes
- Requisición de facturas
- Problemas en el equipo del cliente
- Venta de servicios como NFL Directv, NBA Directv, BOX Directv, Baseball
- Información y venta de Pagos por Evento (PPV)
- Programación (Upgrade/Downgrade a paquetes de programación))
- Problemas técnicos
- Programación (Activación de productos/paquetes)
- Pagos
- Problemas en Pagos por Evento

Basados en el reporte de Directv Customer Care acumulado a Junio de 2004, el número de llamadas que recibe este centro de atención, es aproximadamente de 120,000 llamadas promedio por mes (datos reales de Enero a Junio de 2004), lo que significa un promedio aproximado de 4,000 llamadas diarias. Si determinamos el número de llamadas por hora obtenemos un promedio aproximado de 308 llamadas.

Impacto económico y en el nivel de Servicio.
De las funciones descritas anteriormente, presentamos en la Figura 5.7 la forma en la que impactan en el negocio tanto económicamente como en la calidad del servicio prestado a los clientes.

Recuperación de Cartera.
Este proceso consiste en la programación de llamadas para recuperar saldos vencidos por clientes que no han cubierto sus adeudos. Aún y cuando este proceso puede seguir operando sin la aplicación IBS, los operadores encargados de seguir este programa de cartera accesan constantemente a IBS para la actualización o consulta de datos de los subscriptores.

Basados en el reporte de Recuperación de Cartera acumulado a Junio de 2004, el número de llamadas que realiza este centro de atención, es de aproximadamente 22,000 llamadas promedio por mes, lo que significa un promedio aproximado de 733 llamadas diarias. Si determinamos el número de llamadas por hora obtenemos un promedio aproximado de 56 llamadas.

Impacto económico y en el nivel de Servicio.
Debido a que los operadores pueden seguir trabajando siguiendo el plan de recuperación, el principal impacto es en la calidad del servicio por no tener datos en línea y económicamente el impacto es en la perdida de la oportunidad de una actualización en línea de los datos de los subscriptores como domicilio actual, cambio de forma de pago de cheque o efectivo a cargo automático.

Activaciones.
En este proceso se registran todas las activaciones de nuevos subscriptores del servicio de Directv por lo que representa la principal fuente de incremento en la participación de mercado de la empresa.

Basados en el reporte de Activaciones a Junio de 2004, el número de llamadas que realiza este centro de atención es de aproximadamente 9,000 llamadas promedio por mes, lo que significa un promedio aproximado de 300 llamadas diarias. Si determinamos el número de llamadas por hora obtenemos un promedio aproximado de 23 llamadas.

Impacto económico y en el nivel de Servicio.
Aún y cuando la venta haya sido realizada por el representante de Ventas o Distribuidor, el impacto puede ser en el retraso para activar la señal vía el sistema IBS, si consideramos que el cliente ya pago su contratación por medio del distribuidor, el impacto económico puede ser bajo, sin embargo, la calidad del servicio se ve disminuido puesto que no se atiende con oportunidad la activación del nuevo cliente.

Telemarketing.
En este proceso se registran todas las ventas por nuevas campañas de promociones de Directv por lo que representa la principal fuente de incremento en la participación de mercado de la empresa.

El número de llamadas promedio por hora depende del impacto que tenga la promoción en el mercado por lo que es difícil determinar un número aproximado.

Impacto económico y en el nivel de Servicio.
El impacto económico puede ser bajo, sin embargo, la calidad del servicio se ve disminuida puesto que no se atiende con oportunidad la solicitud de la promoción o servicio.

El objetivo principal del Plan de Recuperación de Desastres (DRP), es por lo tanto, la recuperación de la aplicación IBS después de que un desastre ha sido declarado.

Cálculo de pérdida probable expresada en valores monetarios:
Apoyados de la regresión lineal, el BIA y en la fórmula de la pérdida probable expuesta en el capítulo 2.3.1.4 podemos estimar la pérdida mínima que representaría para Directv el hecho de no contar con su DRP y se presentara un desastre derivado de alguno de los riesgos previamente identificados.

Para estimar el impacto cuantitativo que pudiera causar un desastre, suponemos que la probabilidad de que ocurra uno de los riesgo identificados es P= 100%, de esta manera asumimos que en algún momento estaremos fuera de operación y así estimamos el impacto en el negocio.

$R = P * C$

Donde:
R: Riesgo
P: Probabilidad de que ocurra un evento
C: Perdida operacional en el periodo

Figura 5.8[5]

	Pérdida probable expresada en valores monetarios		
Rubros del área Customere Care	**Pérdida por hora (C)**	**Pérdida por día (C)**	**Pérdida por Semana (C)**
Explicación y ajustes de saldos de clientes	$13,615.00	$176,995.00	$1,238,965.00
Problemas en el equipo del cliente	$13,615.00	$176,995.00	$1,238,965.00
Información y venta de Pagos por	$673.00	$39,507.00	$276,549.00
Venta de servicios: NFL Directv, NBA Directv, BOX Directv, Baseball	$3,039.00	$194,701.00	$1,362,907.00
Suma de rubros marcados con (*) en la gráfica 5.7	$14,977.00	$596,947.00	$4,178,629.00
Total:	**$45,919.00**	**$1,185,145.00**	**$8,296,015.00**

[5] Figura elaborada por los realizadores de la presente tesis.

b) Análisis cualitativo.

Para efectos de análisis cualitativo, en esta tesis se utilizó el método generalizado llamado "What if?", cuya teoría fue desarrollada en el capitulo 2.3.2.2 y aportó información importante para minimizar la exposición al riesgo.

Figura 5.9[6]

¿Qué pasaría si…?	Consecuencia	Recomendaciones
Se presentara humedad extrema en el centro de cómputo	Los equipos no funcionarían correctamente, pueden presentar fallas o hasta quedar completamente inservibles.	Adecuar las para que a través de aire acondicionado se mantenga una temperatura promedio que permita el optimo funcionamiento del equipo
Un error humano	Lo peor que puede pasar es que se borren registros, tablas o la base de datos completa, así como alteración de la información.	Respaldar la información crítica cada determinado tiempo para no perder en su totalidad los datos importantes
Uso indebido de usuarios finales	Alteración de datos o eliminación de los mismos.	Establecer políticas para otorgamiento de permisos, así el usuario final solo podrá realizar únicamente su trabajo.
Errores de procedimientos	Mala ejecución de un proceso.	Contar con un departamento especializado en procedimientos cuyo objetivo sea la auditoria de estos.
Errores de programación	Problemas en tiempos de ejecución.	Contar con un ambiente de desarrollo para las realizaciones de las pruebas necesarias.
Disfunción de software	Problemas en tiempo de ejecución.	Contar con personal experto para atacar los problemas inmediatamente.
Virus de software	Bloqueo total del sistema	Contar con un antivirus de actualización en línea y establecer políticas de seguridad.
Acceso no autorizado a los datos	Alteración, eliminación o mal uso de la información.	Establecer políticas de seguridad rígidas, así como permisos de usuarios.
Acceso no autorizado para el manejo de respaldos	Realización de respaldos no autorizados, mala ejecución o mal uso de información.	Establecer políticas de seguridad rígidas, así como permisos de usuarios.

Tratamiento del riesgo.

Directv pone en práctica la teoría del tratamiento del riesgo expuesta en la sección 2.4, puesto que utiliza las tres maneras de tratarlo como es el asumir, minimizar y transferir.

Asumir.- Directv asume el riesgo operacional.

[6] Figura elaborada por los realizadores de la presente tesis.

Disminuir.-Directv cuenta con mecanismos de prevención de riesgos como los mencionados en el siguiente inciso denominado *"Seguridad de la Información"*, de esta manera minimiza su exposición al riesgo.
Transferir.- Además cuenta con diversas pólizas de seguros, con las que puede hacer frente a sus perdidas físicas y monetarias en caso de algún desastre. Otra forma de transferir el riesgo que utiliza Directv es a través de contratos con proveedores, los cuales se responsabilizan si hay alguna falla o desperfecto en algún equipo o aplicación.

c) Seguridad de la información

Estos sistemas han sido diseñados para minimizar la posibilidad de que un desastre ocurra en las instalaciones de Directv México.

Seguridad Física.- Actualmente el área de sistemas cuenta con diversos sistemas de protección para garantizar la continuidad del negocio, entre ellos tenemos:

Sistemas de enfriamiento
Sistema de aire acondicionado, 2 aparatos Liebert (cap. 15 tons), en caso de falla uno de los aparatos mantendrá el ambiente deseado, mientras se repara el dañado.

Sistemas de energía ininterrumpida (ups)
Se cuenta con dos UPS, Sistema de Energía Ininterrumpible ubicado en el piso 1 y en un lapso de 35 segundos aproximadamente permite la llegada de corriente de la planta de emergencia, manteniendo con esto la alimentación de corriente regulada ubicada en cada estación de trabajo con contactos de color Naranja.
Se ha puesto especial interés en que las instalaciones eléctricas en los edificios ocupados por Directv sean seguras minimizando el riesgo de incendios por corto circuito.

Se cuenta también con un Generador "Automotores" de planta de emergencia que trabaja con diesel ubicado en el sótano 1.

Sistemas de prevención de incendios.
Se tiene instalado en los edificios sistemas de ataque a incendios tales como extintores, hidratantes, gas FM-200 en el centro de cómputo y agua almacenada en cisternas suficiente para combatir un incendio en sus inicios, sistemas de alarma y voceo.
Entre los sistemas implementados se encuentran:

- 8 detectores de fuego, humo o gas o sustancias volátiles.
- 4 detectores bajo el piso falso (2 por cada sección del site)
- 4 detectores en el techo (2 por cada sección del site)
- 2 expulsores de gas FM-200 (1 por cada sección del site). El modo de operar se muestra en el Anexo IV.

Control de acceso.
Se controla el acceso de visitantes al edificio con el fin de minimizar riesgos esta actividad se realiza con detectores de metales instaladas en las entradas, además de que se deben identificar con documento oficial. Los inquilinos cuentan con tarjetas magnéticas.

Control de acceso electrónico

- Para acceso al piso de las instalaciones existen torniquetes los cuáles sólo abren con la tarjeta electrónica personalizada. Las visitas se reciben en el área de recepción, nunca entran a las instalaciones.
- Lector de tarjetas magnéticas y teclado numérico para tener acceso al área de sistemas ya sea con gafete o con la introducción de una clave personal.
- Teclado numérico para acceder al site (centro de cómputo).

Se realizan chequeos periódicos de los sistemas y equipo de emergencia a fin de verificar su buena operación.

Los medios son revisados por el proveedor de servicios diariamente y se lleva una Bitácora de registro, el mantenimiento es planeado en los siguientes periodos:

Equipo	**Periodicidad**
Equipo contra incendio Gas FM-200	Trimestralmente
Aire acondicionado Liebert	Mensualmente
Planta de Emergencia Sotano 1	Trimestralmente
Banco de Baterias UPS	Trimestralmente
Tableros de distribución corriente regulada	Semanalmente

Se tiene definido un plan de emergencia para estar en contacto con bomberos, policía, grupo antibombas y hospitales de emergencia y se cuenta con algunos suministros en sitio, para contingencia y mantenimiento como filtros, fusibles, aceite entre otros.

Seguridad lógica.- El sistema operativo del sistema de producción es UNIX, lo que permite una buena administración de usuarios. Se tiene establecidas políticas de seguridad muy rígidas como lo son cambio de password una vez al mes, acceso restringido a aplicaciones, configuración de permisos según actividad, cambios periódicos de password de usuarios administradores, auditorias a logs de actividades realizadas en el sistema, entre otras.

Seguridad de Redes.- Esta se divide en dos, seguridad en red local (LAN) y red externa (WAN). Directv cuenta con un firewall el cual permite bloquear o filtrar el acceso entre las dos redes, la privada y otra externa. El firewall permite que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Además de que la administración de accesos es muy rigurosa, puesto que es necesario contar un password y usuario con los permisos necesarios para acceder a determinada aplicación.

d) Respaldos

Políticas y procedimientos de backup

Nuestro Administrador de Base de Datos (DBA) cuenta con un proceso automático de envió de información (logs) al servidor IBM RS6000 ubicado en las oficinas de nuestro corporativo DirectvLa en florida, aunado a esto se envía un respaldo general en cintas magnéticas los días lunes.

Los respaldos diarios de las Bases de Datos del sistema critico IBS, se registran en bitácora de operación y son obtenidos en cintas magnéticas las cuales son resguardadas

en una caja de seguridad blindada ubicada en el centro de cómputo de Directv.
Se envía una copia al Sitio Alterno de respaldos, contamos con una caja de seguridad blindada ubicada en Telepuerto, todos los días se mandan respaldos de la B.D. de IBS.

Respaldos críticos:

Respaldo de la base de datos ibs.

Respaldo de informix: archive nivel 0
Descripción: Se realiza un respaldo de nivel 0, en donde se respalda todo el ambiente de informix, se copia en cartuchos tipo "LTO", el software de informix, con todos los datos almacenados hasta esa hora.
Tipo de respaldo: base de datos.
Frecuencia: Semanal (El respaldo se realiza el día domingo por la noche a las 21:00 p.m.).
Duración aproximada de respaldo: 150 minutos.
Procedimiento:

- Abrir sesión telnet al server unix MXCSCA
- Insertar el cartucho LTO en la cartuchera LTO modelo 3580
- Cambiar el dispositivo de respaldo para Informix a través de la utilería "onmonitor"
- Teclear el comando " sudi ontape –s –L 0"
- Cuando el respaldo llega al 100% de realización, el respaldo ha terminado. Retirar la cinta y etiquetarla.
- Realizar el envío de la cinta las instalaciones de DirectvLa.

Responsable: Operador del centro de cómputo en turno supervisado por el DBA.

Respaldo de Informix: Logs
Descripción: En este nivel de respaldo, se guardan los logical logs de Informix a disco .
Los pasos que comprende el proceso de respaldo de los logical logs son los siguientes :

- Respaldo de las transacciones de las bases de datos (logical logs) a disco.
- Compresión del archivo de logical log.
- Copia del archivo del logical log al servidor DRP en el site de Disater Recovery.
- Proceso de reenvío de logical logs en caso de algún problema de comunicación con el server DRP.

El respaldo se realiza a un filesystem llamado "/usr/local/inflog " en el server de producción "MXCSCA".
Se respalda cada transacción realizada en la base de datos.

Después de realizar el respaldo en disco de manera local se realiza el envió del log al server DRP earth a Florida. Si por algún motivo existe algún problema de comunicación existe un programa que en cada media hora realiza reintentos de reenvió y se notifica el problema vía correo electrónico al DBA, al Admón. Unix y a los operadores.
Tipo de Respaldo: Respaldo de Archivos de Logical Logs
Frecuencia: Siempre, cada vez que se llena un Logical Log.
Procedimiento:
El respaldo de logs se realiza de manera automática a través de programas a los que hace referencia el script "alarmhandler" de Informix cada vez que se llena un log
Responsable: Es un proceso que se realiza de manera automática.

Selección del Centro de Almacenamiento Alterno

Centro de almacenamiento externo
Almacenamiento fuera del sitio (Información general acerca de proveedor(es), ubicaciones, personal autorizado, contactos de información, etc.)

El almacenamiento de respaldos fuera de sitio se encuentra en Telepuerto (Centro de Operaciones satelitales de Directv ubicado en Boulevard Puerto Aéreo).

Las cintas de respaldo se encuentran dentro de las oficinas designadas para Directv, en una caja de seguridad con 2 llaves de acceso que se encuentra en poder de Operadores del Site y de Directv, respectivamente. La figura 5.10 muestra una imagen de la caja de seguridad con las cintas de respaldo debidamente identificadas, la cual es a prueba de fuego, terremoto, explosión, inundación, etc.

Figura 5.10[7]

Para guardar las cintas los mensajeros de Directv se identifican con gafete de la empresa y acceden a la caja de seguridad y realizan el resguardo o recolección de cintas según sea el caso.

Para el almacenamiento y recopilación de cintas de respaldo, Directv cuenta con una carta memorándum la cuál autoriza la entrada a quien la porte las 24 horas del día los 365 días del año, para recoger las cintas de respaldo o almacenarlas previa identificación.

[7] Fotografía tomada por los realizadores de la presente tesis.

Site de Recuperación

Obtener un centro de cómputo de respaldo.

Grupo Galaxy Mexicana (Directv) cuenta para casos de desastre en su centro de cómputo con un centro de operaciones de respaldo en la modalidad de Hotsite. El Hotsite está equipado con:

- Hardware: 1 Server IBM RS6000, cuya ubicación Física es: Directv Latinoamérica, Fort Lauderdale, Florida USA.

- Software: Unix, Informix, Magic, IBS.

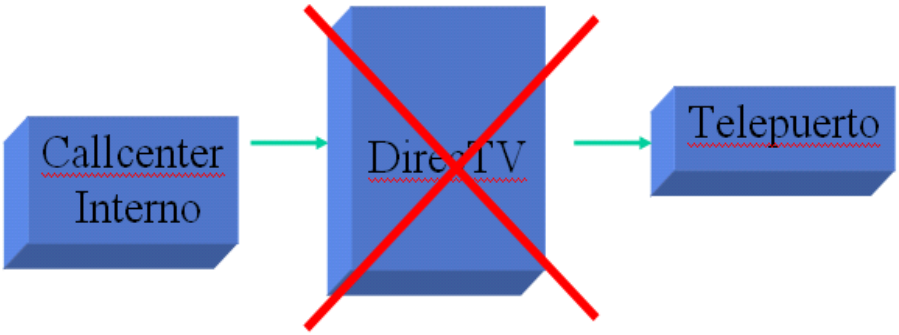
Si en un desastre, los contratos con proveedores de servicio para la reparación o sustitución de los servidores, equipos de comunicación y ambientación del site, resultan ser insuficientes para establecer las condiciones de operación normales, se procederá a la recuperación inmediata de activar el DRP, trasladando la operación al centro operativo de respaldo.

Esta estrategia tiene un tiempo estimado de restauración de 2 horas.

La recuperación en el centro de computo de respaldo, se debe considerar cuando el tiempo estimado para la recuperación de la operación en el centro de computo de Directv, es mayor a 6 horas y las condiciones del centro de computo han rebasado toda posibilidad de pronta reparación o restauración.

Como referencia al marco donde se efectúan las operaciones en Directv y su recuperación en el centro de respaldo considérense los esquemas que se muestran en la Figura 5.11.

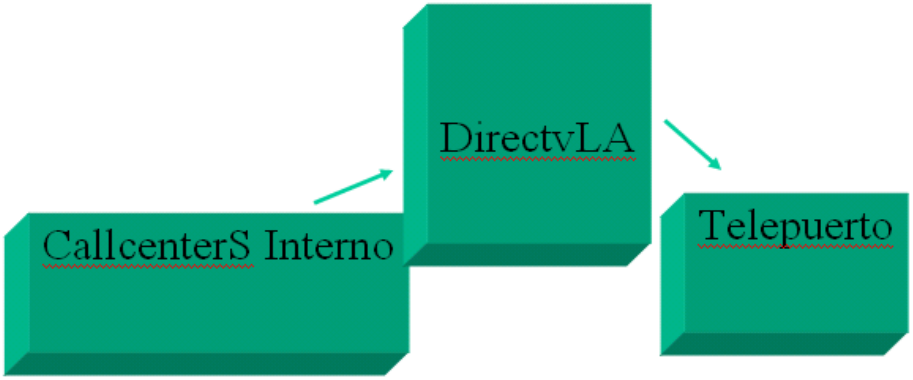
Figura 5.11[8]



En la Figura 5.11 se observa la operación actual de Directv, en donde Directv es el centro de cómputo de producción. Si durante un desastre el centro de computo de Directv pierde toda posibilidad de operación con el Call Center interno y Telepuerto, por lo que se procede a cambiar el flujo de la operación hacía el nuevo centro de computo (Hotsite) ver Figura 5.12.

[8] Figura Elaborada por los realizadores de la presente tesis.

Figura 5.12[9]



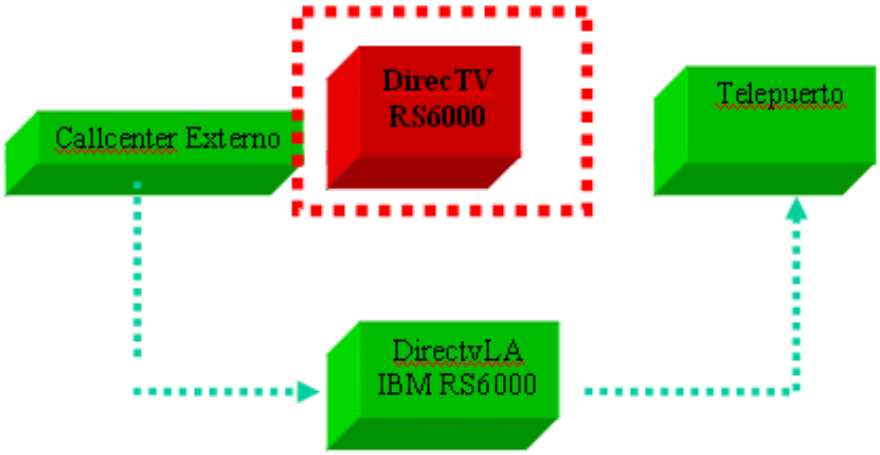
La Figura 5.12 ilustra la operación de Directv después de la recuperación en el site alterno, la operación de recuperación abarca únicamente el cambio del centro de operación actual, por lo que el cambio será transparente para el Callcenter y Telepuerto.

Supuestos del Plan de Recuperación de Desastres.

Este plan de recuperación de desastres se ilustra en la Figura 5.13 y funciona bajo las siguientes condiciones:

- Cuando el perímetro de desastre afecte únicamente la operación el centro de computo en Directv y no afecte la operación normal de los centros de atención a clientes y Telepuerto (centro de transmisiones).
- Cuando el desastre no impida al equipo de gente encargado de la recuperación de desastres de Directv estar disponible para ejecutar el plan.
- Cuando los enlaces de comunicación entre los sitios funcionen adecuadamente.

Figura 5.13 [10]



[9] Figura Elaborada por los realizadores de la presente tesis.

[10] Figura Elaborada por los realizadores de la presente tesis.

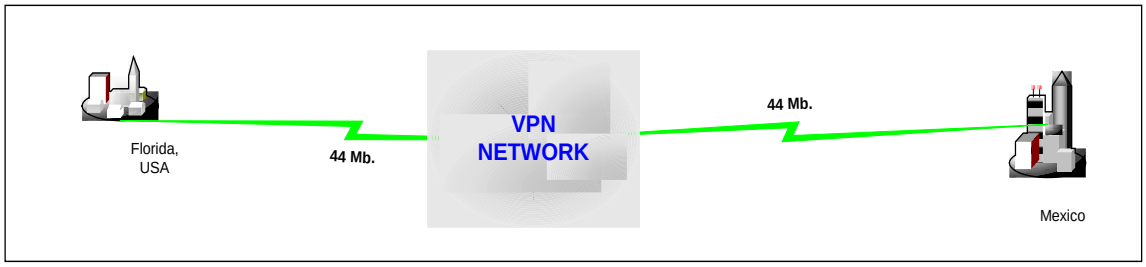
Conectividad de Redes del DRP

Para asegurar la continuidad del negocio en caso de desastre, Directv ha planeado un DRP para sus redes de comunicación y para sus centros de atención a clientes (*Call center*♦), a continuación de expone brevemente en que consiste cada uno de ellos.

a) DRP de Redes

El DRP de las redes de comunicación entre el site de México y Florida funciona actualmente como lo ilustra la Figura 5.14 y trabajo a través de una VPN (Red Privada Virtual) DRP del centro de operaciones.

Figura 5.14[11]



El plan DRP entra en operación si el equipo Unix RS-6000 M80 no puede operar en el site de operaciones de México o el site de México se encuentra en estado inoperante. Un equipo Unix de respaldo con características similares entra a operar remotamente desde Florida, USA. Este equipo se mantiene actualizado periódicamente con bases de datos de respaldo enviadas en línea durante el día.

Para mantener la comunicación con el sitio en Florida USA, se requiere tener una comunicación VPN a Internet y un Firewall PIX de Cisco o, inclusive un cliente de VPN Cisco client en cada máquina, es suficiente para tener la comunicación sobre Internet.

b) DRP para el Call Center.

El *call center* local cuenta con un DRP para la atención de clientes en Sitel México. En Sitel México se encuentran disponibles estaciones de trabajo para agentes emergentes que sostendrían la operación temporalmente, en tanto se recupera la operación del centro de atención telefónico local. (Figura 5.15)

Los agentes emergentes en Sitel, se conectarían al servidor UNIX del centro de operaciones de México, lo que permitirá correr la aplicación vital de esa operación. En caso de que el servidor UNIX de México no se encuentre disponible, utilizaríamos el esquema explicado en la figura 5.12

La llamadas de los clientes se encaminarían desde el PBX del centro de operaciones de México hacía el número directo del centro de atención de respaldo sitel (DID) destinado para este fin.

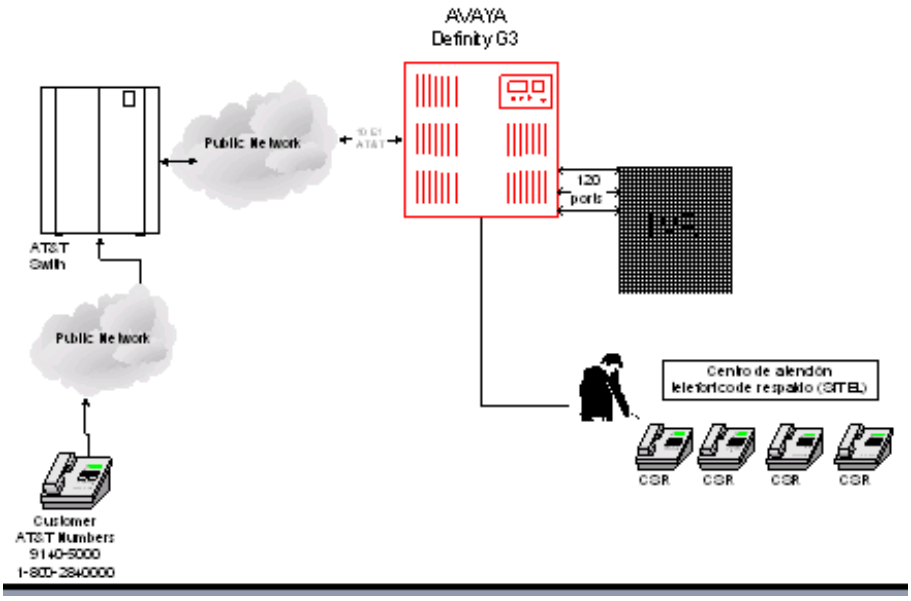
♦ Término definido en el Glosario

[11] Figura Elaborada por los realizadores de la presente tesis.

El número 01-800 dirigido actualmente al número local ##-##-##-## se cambiaría para terminar en el número local DID de sitel.

Con este esquema se atendería tanto el tráfico local de llamadas como el de larga distancia.

Figura 5.15[12]



Tarea 2.- Formación de Equipos

<u>Equipos Operativos</u>

En esta sección se nombran las principales áreas y departamentos responsables de mantener la operación normal de la empresa; cada uno esta formado por un equipo de trabajo determinado, la figura 5.16 desglosa estos departamentos.

<u>Equipos de Evaluación (auditoria del cumplimiento de los procedimientos sobre Seguridad)</u>

Directv México cuenta con equipo denominado "Comité de seguridad" el cual se encarga de realizar las revisiones necesarias para asegurarse que se cumplan las normas y procedimientos establecidos.

La organización de Directv México al ser parte de un grupo de empresas transnacionales es auditada por empresas extranjeras especialistas en tecnología de información, a fin de detectar las posibles fallas en la aplicación de las políticas y procedimientos, entre ellos su plan de recuperación de desastres.

[12] Figura Elaborada por los realizadores de la presente tesis.

Figura 5.16[13]

Area	Departamentos	Responsabilidades
Sistemas	Operaciones	Mantener los servidores funcionando y el sistema en línea las 24 hrs del día
	Bases de datos	Administrar las bases de datos
	Desarrollo	Elaboración de nuevas aplicaciones y administración de las existentes
	Telecomunicaciones	Soporte técnico a usuarios del sistema
	Telefonía	Administración de conmutadores
Call Center	Customer care	Atención a usuarios, problemas técnicos, subir y bajar de Paquete, pagos por evento, entre otros
	Recuperación de cartera	Realización de llamadas para recuperar saldos vencidos
	Activaciones	Activar nuevos suscriptores
	Telemarketing	Ventas por teléfono

5.2.2 Etapa 2.- Actividades durante el Desastre.

Tarea 1.- Plan de Emergencias

Procedimiento para evacuar los edificios oficinas Directv y Telepuerto con apoyo de la brigada de emergencia ante cualquier amenaza.

Disparo de alarma.

- Cuando se detecta una contingencia (incendio, terremoto, amenaza de bomba, etc.), se da una señal a los miembros de la brigada por el sistema de sonido y se alertan las sirenas. En ese momento se inicia el procedimiento con el apoyo de los miembros de la brigada de emergencia.

+ Los elevadores se detienen en la planta baja y se corta la energía eléctrica de ellos.
+ Los miembros de la brigada de emergencia se aseguran que nadie quede dentro del edificio revisando baños, salas de junta, oficinas privadas y cualquier lugar donde pudiera estar personal.
+ Los miembros de la brigada también asisten a las personas que por condiciones físicas tengan dificultades para usar las escaleras.
+ En la recepción permanece la brigada de primeros auxilios en espera de llamadas de auxilio.

Una vez dada la voz de alarma contingencia, la brigada de emergencia se divide en dos actividades, una para tratar de sofocar el incendio y otra para evacuar al personal de las Instalaciones en

[13] Figura Elaborada por los realizadores de la presente tesis.

problemas o del edificio. La brigada de primeros auxilios, permanece en la recepción en estado de alerta para ayudar a empleados en problemas.
El jefe de seguridad permanece en la recepción para ayudar al cuerpo de bomberos cuando se presenten al edificio.
En caso de incendio, si se produce fuera de horas de oficina o en día no hábil, el personal de seguridad reporta el siniestro a los bomberos y después llama al Gerente de Personal y Jefe de Servicios Generales.

Los vigilantes de seguridad, se encargan de mantener las puertas de salida abiertas, detener el transito en la avenida y ayudar al personal a cruzar la calle o dispersarse en la banqueta.

- No se permite el reingreso del personal hasta tener un edificio revisado y seguro.
El Gerente de Personal y Jefe de Servicios Generales avisará a los empleados que pueden entrar al edificio cuando existan las condiciones de seguridad en el edificio.
-Procedimiento para cortar la energía eléctrica ante una emergencia.
El personal de mantenimiento corta la energía eléctrica del edificio incluyendo elevadores.

-Protección de información valiosa producida por la computadora, por la vía de mantener copias de respaldo fuera del edificio.

Tarea 2.- Formación de equipos

Centros de Comando
En un desastre, se considera que el centro de operaciones principal de Directv, se encuentra en estado inoperante y que los medios definidos de comunicación puedan estar seguramente averiados, por lo que es menester, definir un centro de comando, fuera de las instalaciones, desde donde se indique y giren instrucciones precisas de recuperación.

Es conveniente que este centro de comando esté precisamente donde se encuentran los equipos de comunicación para garantizar la conectividad al equipo de contingencia.

Dado que es muy probable que la comunicación con los miembros del equipo sea difícil, es necesario que los miembros de los equipos se mantengan en comunicación constante con el equipo de administración en este centro de comando.

La comunicación hacia el centro de comando es muy importante ya que con ello se esta asegurando la coordinación de las actividades a la par de los demás miembros del equipo.

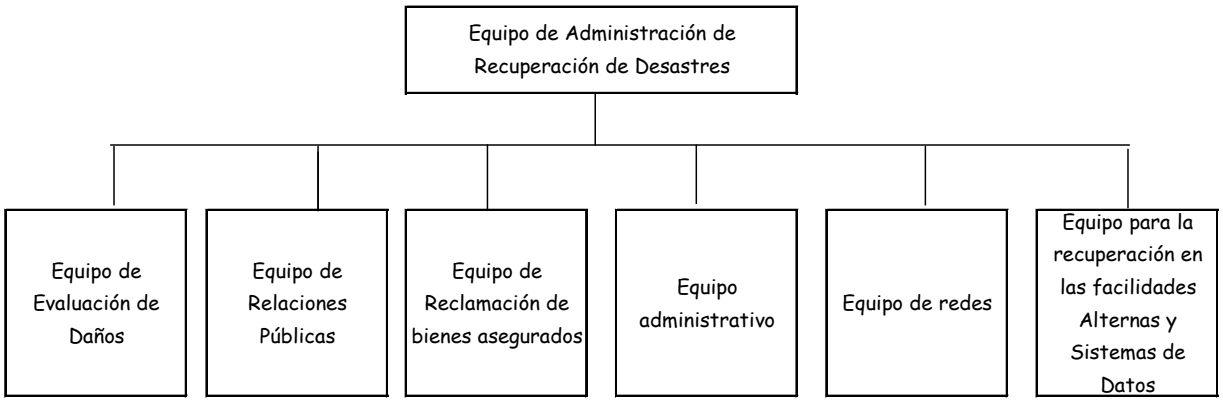
Listado de ubicaciones y direcciones actualizadas de centro de comando en caso de desastre

El centro de comando se encuentra en el área de sistemas de Directv, en caso de que el área no garantice la permanencia del personal el centro de comandos se traslada a un centro de atención a clientes externos (Sitel México).

Organización en la recuperación de desastres

Figura 5.17[14]

Estructura Organizacional



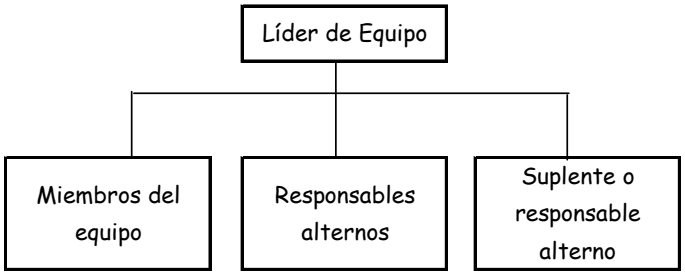
Responsabilidades y deberes por equipo:

Formación del equipo (Cadena de mando, figura 5.18):

Líder de equipo:
El líder deberá estar totalmente familiarizado con todo el DRP, formar un equipo de apoyo con los miembros más adecuados de acuerdo a la experiencia y desarrollo de cada uno, entrenar constantemente al equipo en la ejecución del plan y mantener siempre actualizada y al alcance de todos, una lista con todos los datos generales, necesarios para la localización oportuna del equipo.

Figura 5.18[15]

Cadena de mando



Miembros del equipo:
Son todos aquellos individuos que participan directamente en la ejecución del DRP. Tienen la responsabilidad de ejecutar una tarea especifica, de acuerdo al plan y de hacerlo en el momento exacto, es decir, ajustar su intervención a la sincronía propia del plan, indicada por el líder, con el fin de no actuar a destiempo en comparación con el resto del equipo.

[14] Figura elaborada por los realizadores de la presente tesis.
[15] Figura elaborada por los realizadores de la presente tesis.

Responsables alternos:
Para cada miembro del equipo, incluyendo al líder, se debe buscar un sustituto que tome la responsabilidad de asumir la función que resulte vacante por ausencia o incapacidad. La recomendación en este sentido, es "rolar" a los miembros del equipo durante los entrenamientos y pruebas, en todas y cada una de las actividades y responsabilidades, de manera que, al estar familiarizado, mantengan un buen control sobre la función heredada, en caso de requerir su participación al presentarse un desastre.

Nuevos miembros:
Toda persona, que por su función o actividad deba agregarse al equipo, será sometida a entrenamiento y evaluación, por parte del líder del equipo, que entregará copia del plan. Una vez autorizada y firmada su colaboración, será identificada y reconocida por todo el equipo, para su participación en el plan.

Descripción de los equipos de DRP.
Los equipos de recuperación de desastre se han identificado para administrar y desempeñar todas las operaciones de recuperación de desastre. Los equipos siguientes dirigirán el proceso de recuperación y proveerán apoyo:

Equipo de Administración de Recuperación de Desastre:
Líder: Director de Sistemas
Miembros: Dirección de sistemas.
Responsabilidad: El equipo de Recuperación de Desastre es responsable de la administración y control global de las operaciones de Recuperación de Desastre que comienzan con evaluar el daño y termina hasta que el sistema de cómputo esté operando normalmente y los empleados hayan recuperado totalmente las operaciones normales del negocio. El equipo de Administración de Recuperación de Desastre se compone de un líder de equipo y un líder de cada uno de los otros equipos de recuperación.
Su responsabilidad incluye determinar:

-Autorizar los gastos de la operación de recuperación que se requieran para el personal.
-Restauración del centro operativo principal.
-Dar la notificación inicial a los equipos de usuarios (tanto el grupo clave como a los usuarios que no constituyan parte del grupo clave) así como la constante comunicación durante el proceso de recuperación de las operaciones.
-Durante las actividades para recuperar el procesamiento y operaciones de sus unidades de negocio, informa la situación del Equipo de Administración de Recuperación de Desastre.

Equipo de evaluación de daños
Líder: Jefe de Sistemas Operativos
Miembros: Jefatura de Operación.
Responsabilidad: El equipo de Evaluación de Daños será responsable de complementar los informes de evaluación de daños.
Su responsabilidad incluye determinar:

-La condición del cuarto de cómputo, a través de complementar un informe preliminar de la situación;
-El alcance de daño a la máquina (IBM RS6000 M80) y los sistemas de la red afectados por el desastre, a través del llenado de una lista de comprobación de evaluación de daños.

-El estado del procesamiento al momento del desastre a través de la identificación de documentación que se haya podido rescatar y de cintas de respaldo y ubicar esos respaldos almacenados fuera de las oficinas.
- La condición del equipo y las facilidades de oficina, evaluar el alcance inicial de daños.
- Un informe completo, preciso y rápido de la situación del desastre.

Equipo de Relaciones Públicas:
Líder: Gerente de relaciones públicas
Miembros: Gerencia de Relaciones Públicas
Responsabilidad: El manejo de toda información pública, prensa, proveedores y de la preparación de comunicados de prensa.

Equipo para la reclamación de Bienes Asegurados:
Líder: Gerente de finanzas
Miembros: Dirección de Finanzas
Responsabilidad: El equipo para la reclamación de bienes asegurados es responsable de determinar el alcance del daño, complementar y presentar la reclamación correspondiente a la póliza de seguros existente.

Equipo Administrativo:
Líder: Gerente de Presupuestos
Miembros: Gerencia de Administración y Presupuesto.
Responsabilidad: El Equipo Administrativo es responsable de todos los asuntos administrativos tales como:

-Proveer abastecimiento al Centro de Comando de Emergencia
-El establecimiento de un fondo de caja chica
-Notificar al servicio postal de la dirección del Centro de Comando de Emergencia
-Desempeñar deberes secretariales, tales como notificar al personal cómo comunicarse con el Equipo de Administración de Recuperación de Desastres al Centro de Comando de Emergencia y tomar mensajes telefónicos para cada uno de los miembros del Equipo de Recuperación de Desastres
-Coordinar el transporte y cualquier alojamiento necesario para los miembros del Equipo de Recuperación de Desastre
-Proveer otros servicios incidentales al Equipo de Administración de Desastre tales como comidas, servicios de fotocopiado y otros deberes administrativos.

Equipo de redes:
Líder: Gerente Telecomunicaciones.
Miembros: Gerencia de telecomunicaciones y administración de servidores.
Responsabilidad: Realizar cambios en configuraciones de VPN, red, enrutamiento de llamadas y realizar pruebas de comunicación.

Equipo para la recuperación en las facilidades Alternas y Sistemas de Datos:
Miembros: Jefe de sistemas operativos y Gerente de negocios
Responsabilidad:
Este equipo es responsable de recrear un apropiado ambiente para la computación y la marcha del negocio así como la restauración de todos los sistemas en las ubicaciones alternas. Además, los Equipos de Recuperación de Facilidades Alternas y Sistemas son también responsables por el

movimiento de los sistemas o equipos desde la ubicación alterna a las nuevas facilidades construidas, una facilidad temporal o el regreso a las instalaciones principales en Blv. Manuel Ávila Camacho # 1-101, Col Polanco, México, D.F. Se requerirá de comunicación extensiva entre los equipos.
Recuperar los datos de los sitios de almacenamiento, acudir al centro operativo de respaldo, recuperar el servidor de respaldo si es necesario (Sistema operativo, manejador de base de datos, magic e ibs) y actualizar los datos del ultimo respaldo disponible en caso de no estar actualizados los logs a la base de datos global.

5.2.3 Etapa 3.- Actividades después del Desastre.

Tarea 1.- Evaluación de Daños.

Declaración de Desastre
La declaración del desastre es el primer aviso formal dirigido a un grupo especifico de personas, informándoles sobre el evento o grupo de eventos que han causado daño considerable en alguna o en todas las aplicaciones críticas del negocio, afectando o poniendo en riesgo su funcionamiento y cuya recuperación requiere de la ejecución inmediata del Plan de Recuperación de Desastres.

Notificación de Desastre

Pasos para notificar un desastre:

Paso	Equipo o Responsable	Actividad	Descripción
1.	Administración	Notifique a directores	Avise a Directores de GGM y GLA,
2.	Relaciones Públicas	Publique Notificación	Prepare publicación a medios de información. Publique en medios de información y prensa el desastre y su recuperación.

Tarea 2.- Priorización de Actividades del Plan de Acción.
A continuación se muestra un esquema del plan de acción y las actividades que lo conforman.

Paso	Equipo o Responsable	Actividad	Descripción
1.	Operador o Vigilante en turno	Avise desastre	Localice en la lista de contactos los datos del equipo de administración. Intente hasta tener comunicación. Avise el desastre al equipo de administración.
2.	Administración	Solicite evaluación de daños	Avise al equipo de evaluación de daños y solicite el diagnóstico del desastre en el centro de cómputo.

3.	Recuperación	Evalúe daños	Revise daños del desastre. Reporte al equipo de administración los daños del centro de cómputo. Mencione tiempo estimado de recuperación del centro de cómputo.
4.	Administración	Declare o cancele desastre	Localice equipos de recuperación. Declare o cancele declaración de desastre.
5. *	Administración	Reúne equipos	Pide a los equipos de recuperación se presenten en el Site de Directv.
6. *	Administración	Declare contingencia DirectvLa	Avise al centro de cómputo de respaldo DirectvLa, notifique desastre.
7. *	Redes y Comunicaciones	Avise a los Callcenter	Avise desastre a Callcenter externos que ejecute plan de Recuperación de red de respaldo.
8. *	Redes	Avise a Telepuerto.	Avise desastre a Telepuerto que ejecute plan de Recuperación de red de respaldo.
9. *	Administración	Avise a Proveedores.	Contacte proveedores y solicite soporte si lo requiere.
10.	Administración	Organice centro de comando	Organice centro de comando. Comience estrategia de recuperación.
11.	Recuperación	Avise a Callcenter externo y Telepuerto	Avise a Callcenter externo y Telepuerto inicio de operación desde sitio de respaldo
12.	Recuperación	Inicie operación En sitio de respaldo.	Comience operación de IBS.
* Estas actividades pueden hacerse en paralelo. Cuando se habla de actividades de equipos, se refiere a las actividades que debe realizar el líder de ese equipo o su suplente.			

Tarea 3.- Ejecución de Actividades.

Estás actividades deben realizarse según el orden establecido en el paso anterior, aquí también interviene el equipo de reclamo de bienes asegurados.

Seguros.

Directv tiene un plan de seguros y administración de riesgos que ha sido preparado e implementado por el departamento de Tesorería para proteger a la empresa de pérdidas significativas de dinero como resultado de un desastre.

Este plan ha cumplido los siguientes objetivos: es factible en costos, ha reducido la carga administrativa (menor número de pólizas) y provee buena protección a nuestros activos y utilidades.

Tarea 4.- Evaluación de Resultados.

Para un caso real, este sería un punto importante ya que se mide que tan bien se realizaron las cosas y las posibles necesidades o exposiciones al riesgo, para el caso de Directv afortunadamente no ha sido necesario realizar una recuperación total de nuestro centro de cómputo. Sin embargo se muestran algunas observaciones en la tarea de ejecución de pruebas en la sección denominada "Administración del plan".

5.3 - Administración del plan

La administración del plan de recuperación de desastres se divide en 4 tareas fundamentales:

Tarea 1.- Distribución.
Un plan de recuperación no sería útil si no se da a conocer a su gente de que existe, así que ha distribuido a toda su gente una serie de manuales para dar a conocer su plan de recuperación de desastres, entre las actividades de distribución están:
Platicas informativas.
Manuales impresos por área.
Manuales por correo electrónico.
Publicación de manuales en la *web* con la finalidad de poder acceder a ellos aún no estando en la oficina.

Tarea 2.- Mantenimiento.
El plan original de recuperación de Directv mostraba un número considerable de fallas, sin embargo, se han realizado modificaciones significativas recomendadas por los realizadores de la presente tesis y cuyas se exponen en el siguiente cuadro comparativo:

Diferencias significativas entre DRP anterior y el diseñado con el método propuesto.		
	Plan anterior	**Plan Método Propuesto**
Metodología	Hewlett-Packard.	Método propuesto
Tiempo de recuperación	Mínino se llevaba 4 hrs.	Se lleva aprox. 1/2 hora
Site alterno	El hot-site se encontraba a 5km. a la redonda	El hot-site se encuentra en otro país
Análisis de riesgos	Muy básico, solo se realizo de manera cualitativa	Análisis de riesgos cuantitativo
Seguridad	Enfocado a la seguridad física	Cubre seguridad física, lógica y redes
Mantenimiento	Básico, no se retroalimentaba	Hay retroalimentación
Auditoria	No se auditaba	Es auditado por despacho externo

Tarea 3.- Entrenamiento
Este paso se ha realizado en conjunto con las pruebas del plan ya que cuando existe alguna rotación de personal se capacita mediante manuales y se trata de que participe en la ejecución de la siguiente prueba del plan.

Tarea 4.- Pruebas al plan.

Registro de Pruebas

Sistema IBS Magic.

Resultado de las pruebas del DRP de México realizadas el 24 de Febrero de 2004 hacia el servidor "earth" ubicado en las oficinas en Fort Lauderdale.

Los ambientes que se probaron fueron IBS Magic e IBS GUI con los siguientes usuarios:

Coordinador del centro de atención a clientes
Operador telefónico 1
Operador telefónico 2
Supervisor del centro de atención a clientes

Prueba poder realizar la prueba se levanto un Service Request a DirectvLa a fin de que la Base de Datos que se está replicando y funciona para DRP se cambiara su estatus para poder accesarla.

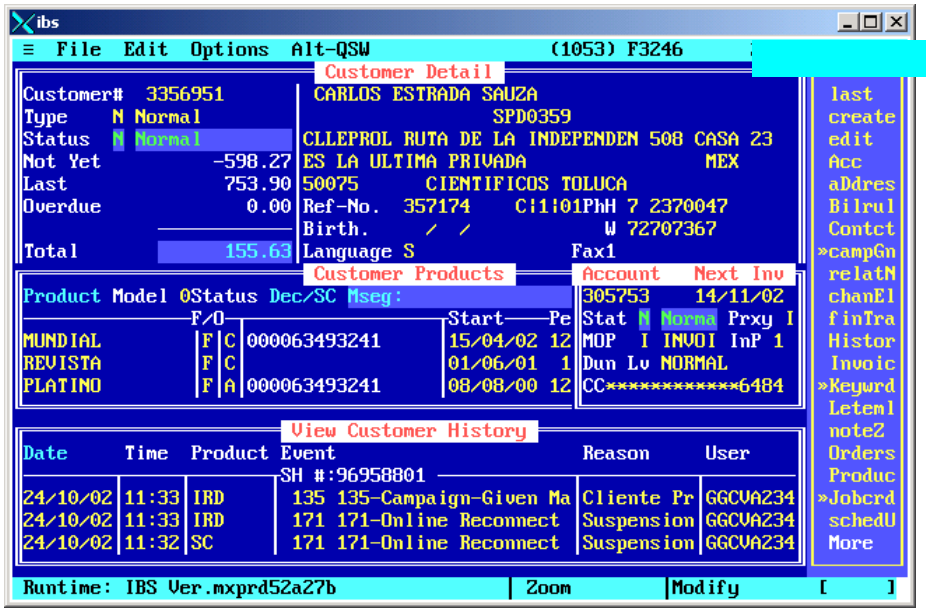
Una vez que la Base de Datos estuvo "on-line" en las dos PC en las que se realizaron las pruebas se cambio el archivo de configuración como a continuación se muestra:

El primer parámetro que se cambió fue el IP hacia XXX.XXX.XXX.XX que es el servidor "earth" de DRP y el segundo fue el script "mxprd01".

Una vez que se realizaron los cambios se procedió a realizar modificaciones a la Base de Datos de DRP y a verificar el tiempo de respuesta del sistema.

La Figura 5.19 muestra una pantalla del sistema IBS de producción *IBS Magic* estando operando desde el sitio alterno.

Figura 5.19[16]



Los movimientos que se realizaron a través de IBS Magic fueron:
Reconexiones
Cancelaciones
Ajustes de renta
Eliminación de campañas
Upgrades de Platino a Familia
Mes sin costo

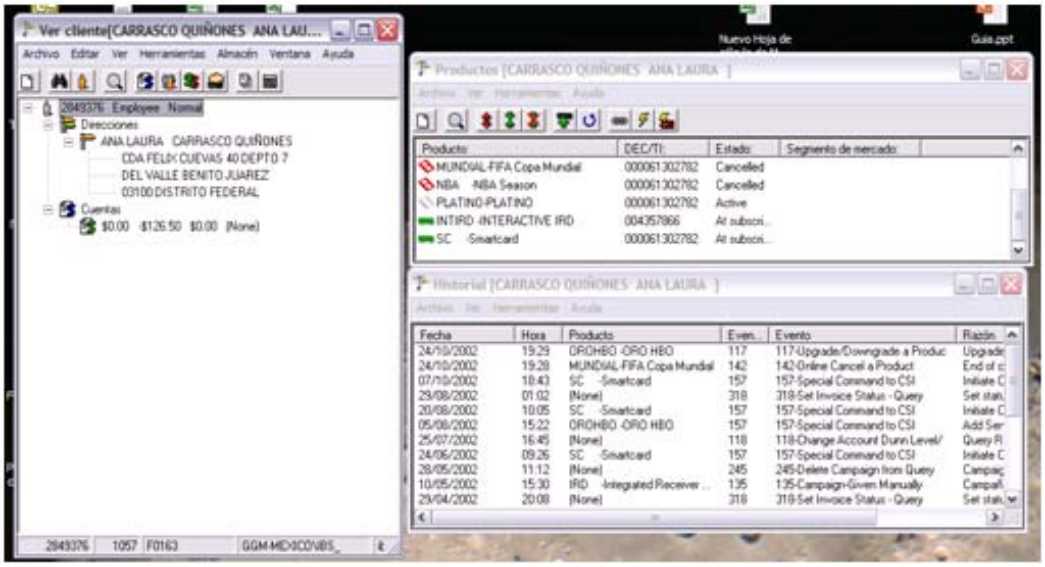
[16] Figura proporcionada por Gerente de Negocios de DirecTV

El coordinador del *Call Center* verificó el tiempo de respuesta afirmando que es muy bueno y que en una contingencia se podría trabajar sin problemas.

Sistema IBS GUI (Interfase gráfica).

Por lo que respecta al IBS GUI, (interfase gráfica del sistema) figura 5.20, el Gerente de negocios, realizó algunos movimientos.

Figura 5.20[17]



A pesar de que se utilizó como servidor de GUI una PC de escritorio el tiempo de respuesta fue bueno por comentario del Gerente de Negocios, sin embargo en una contingencia se utilizaría el servidor que actualmente está en producción para IBS GUI.

Los parámetros para conexión de ODBC para GUI son:

SERVERNAME	name.soc
HOST NAME	earth
HOST IP	XXX.XXX.XXX.XXX
SERVICE NUMBER	643
SERVICE NAME	name.soc
PROTOCOL NAME	onsoctcp
DATA BASE NAME	ibs

La prueba de DRP para IBS Magic e IBS GUI fueron exitosas y con un buen tiempo de respuesta.

Próxima prueba DRP en el mes de Octubre del 2004.

[17] Figura proporcionada por Gerente de Negocios de DirecTV

5.4 Manuales

Directv cuenta con algunos manuales elaborados con la finalidad de que el personal este enterado y preparado para algunos casos de contingencia, los detalles de los mismos se muestran en el Anexo IV;

- Sismo o temblor.
- Amenaza terrorista o sabotaje.
- Incendio.
- Medidas de prevención de fuego
- Falla del aire acondicionado.
- Erupción del volcán

Conclusiones

Debido a que las empresas de energía y telecomunicaciones son las más afectadas por los ataques a la seguridad de sus sistemas informáticos, el contar con un plan de Recuperación en Caso de Desastre (DRP) se hace indispensable para lograr la continuidad del negocio.

A pesar de los daños que pueda haber sufrido una empresa a consecuencia de desastres de tipo natural o debido a fallas del equipo y/o humanas, finalizamos este proyecto con la elaboración de un plan de recuperación de desastre que permite continuar las actividades normales de una empresa que depende en un gran porcentaje de su información tecnológica, dicho plan esta basado en un método propuesto y facilita el actuar con prontitud ante cualquier dificultad, organizar la reiniciación provisional de las labores más importantes y posteriormente reestablecer en forma integral todas las actividades.

Con la finalidad de ser una propuesta que cumpla con su cometido a través de fases claras y sencillas, incluso fácil de detectar dependiendo del factor tiempo, nuestro método propuesto combina, complementa y adiciona, dos de los métodos más completos existentes en el mercado.

La retroalimentación que este plan aporta a la empresa, permite la detección de problemas en los sistemas de seguridad y de organización para proteger y respaldar el elemento más importante de toda empresa de este tipo; la información.

La posición en el mercado de la empresa de telecomunicaciones DIRECTV, la situación actual, el prestigio que tiene, el análisis de impacto en el negocio y la lista de vulnerabilidades y amenazas a la que está expuesta, motivan y justifican el costo de la aplicación de un DRP. Los resultados obtenidos en nuestro caso práctico, muestran mejoras al confirmar que las expectativas de seguridad han sido optimizadas y los tiempos para lograr la reanudación de la operación se han visto reducidas, considerando la organización del personal de la empresa en equipos de trabajo y con la práctica de simulacros, en donde cada quien sabe que hacer llegado el momento desde su posición y responsabilidad.

Una empresa con información tecnológica no debe ignorar la necesidad de mantener un alto nivel de vigilancia en sus instalaciones. Los administradores de seguridad no deben olvidar las medidas de prevención como la identificación de los empleados, la separación de las responsabilidades de IT y las auditorias que son aspectos clave de una estrategia de seguridad efectiva. En la medida en que las fisuras internas a menudo son ignoradas principalmente debido a su inherente dificultad para detectarlas, trae como consecuencia estos tipos de incidentes que suelen ser los más costosos para las empresas tecnológicas y DIRECTV no es ajena a estos riesgos.

Deseamos que el lector de esta tesis sea alentado a recapacitar e implementar medidas de prevención y mejor aún, establecer planes de seguridad para lograr la permanencia de las empresas y por ende de fuentes de trabajo. Un seguro de daños, resarcirá las pérdidas económicas o materiales provenientes de un evento adverso pero no garantizará el que la empresa siga operando.

Si además del seguro se establece un DRP, podemos tener la seguridad que la empresa continuará funcionando normalmente. El primer paso es justificar ante los altos directivos de las organizaciones el valor de la prevención y convencerlos que la implantación del proyecto de este tipo, no es un gasto sino una inversión.

Glosario

Backups (Respaldo de Archivos):
En la actualidad el respaldo de archivos, es una de las principales actividades a desarrollar por una empresa o individuo ya que la perdida total de sus datos puede llegar a ser catastrófico para la misma. Generalmente la pérdida total de datos, se puede llegar a dar en el caso de la rotura de un disco rígido, algún accidente que de alguna manera destruya la maquina, o lo que es más común aun, la infección de su P.C. con un virus informático. Estas y muchas otras posibilidades, que surgen a diario pueden llegar a acabar con sus archivos.
Recuperación de Datos. La mejor manera de recuperar sus datos es si usted. tiene respaldo de sus archivos, de lo contrario se puede intentar recuperar los datos de su disco dañado, la recuperación puede llegar a ser parcial o en el mejor de los casos total.

Call Center:
Centro de atención a clientes vía telefónica.

Cluster:
En su parte central, la tecnología de Clusters consta de dos partes. La primera componente, consta de un sistema operativo confeccionado especialmente para esta tarea (modificaciones al kernel de Linux), un conjunto de compiladores y aplicaciones especiales, que permiten que los programas que se ejecutan sobre esta plataforma tomen las ventajas de esta tecnología de Clusters. La segunda componente es la interconexión de hardware entre las máquinas (nodos) del Cluster. Se han desarrollado interfaces de interconexión especiales muy eficientes, pero comúnmente las interconexiones se realizan mediante una red ethernet dedicada de alta velocidad. Es mediante esta interfaz que los nodos del Cluster intercambian entre si asignación de tareas, actualizaciones de estado y datos del programa. Existe otra interfaz de red que conecta al Cluster con el mundo exterior. Cuando se habla de resolver un problema en paralelo, se refiere a dividir un trabajo en varias tareas que se pueden desarrollan en paralelo.

Degaussing:
Se le conoce así al proceso de desmagnetización que siguen los medios de almacenamiento y grabación de datos, dichos medios generalmente están constituidos por óxidos férricos, dióxido de cromo, etc.

Downsizing:
Este término se aplica al proceso de traspasar los sistemas de información desde sistemas centralizados y costosos basados en grandes ordenadores y miniordenadores a sistemas más pequeños, flexibles y potentes y además menos costosos, al menos en lo que se refiere a su coste de adquisición: ordenadores personales y estaciones de trabajo conectados en red.

DRP:
Disaster Recovery Planning: Plan de Recuperación de Desastres.

Eavesdropping:
Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un

gateway de Internet y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.
Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Encriptación (Criptografía):
La encriptación es un software que le permite proteger la privacidad de sus archivos, directorios y mensajes sensibles, encriptándolos con hasta cuatro algoritmos de encriptación robustos. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o transmitido por una red insegura, como Internet y aún así permanecer secreta. Luego, la información puede ser desencriptada a su formato original.

Es la conversión de datos o mensajes en una sucesión de caracteres ilegibles y difíciles de descifrar por extraños, a partir de algoritmos que funcionan como llaves y sin los cuales simplemente es imposible decodificar los datos a su forma original. Este concepto es ampliamente utilizado en la parte de telecomunicaciones, sobretodo inalámbrico, donde se encuentran en continua evolución para proteger información que, a comparación con los envíos a través de cables, viajan al alcance de todos por aire.

Existe distintas soluciones de software para encriptar, incluso hay sistemas mixtos que combinan un programa con un dispositivo (llave) para poder correr la información. La encriptación puede integrarse a distintos tipos de transferencia de información desde el correo electrónico.
Ethernet
A finales de 1972, Metcalfe y sus colegas de Xerox PARC desarrollaron el primer sistema experimental de Ethernet para interconectar el alto de Xerox, un sitio de trabajo personal con un interfaz utilizador gráfico. Ethernet experimental fue utilizada para ligar los altos a uno otros y a los servidores y a las impresoras laser. El reloj de la señal para el interfaz experimental de Ethernet fue derivado del reloj del sistema del alto, que dio lugar a una tarifa de la transmisión de datos en Ethernet experimental de 2,94 Mbps.

La primera red experimental de Metcalfe fue llamada la red de Aloha del alto. En Metcalfe 1973 cambiante el nombre a "Ethernet," hacerle el claro que el sistema podría apoyar cualquier computadora altos no justos y precisar que sus nuevos mecanismos de la red se habían desarrollado bien más allá del sistema de Aloha. Él eligió basar el nombre en la palabra "éter" como manera de describir una característica esencial del sistema: el medio físico (es decir, un cable) lleva pedacitos a todas las estaciones, muchas la misma manera que el viejo "éter luminiferous" fue pensado una vez para propagar ondas electromagnéticas a través de espacio.

Firewall (Barreras de protección):
Por lo general un firewall es un enrutador: los sistemas abajo del Firewall lo ven como la gateway a la red externa y los enrutadores que están sobre el Firewall lo ven como una gateway de una red protegida. Ahora, un puente es simplemente una pieza de hardware que permite que dos --o más-- segmentos de una red sean conectados y permitan el paso de paquetes de un lado a otro sin que nadie en la red este preocupado por ello. En otras palabras, un enrutador es como un intérprete entre dos -

-o más redes-- y un puente es más parecido a un simple cable conectando dos segmentos de red. Así que un Puente Firewall es como un Puente que filtra los paquetes que pasan por él.
Te puedes conectar a cualquier firewall sin tener que modificar la configuración de tu red. Puedes proteger parte de una red en la que no tienes control de los enrutadores externos que pueden entrar a tu red.

Hacker :
Pirata que de la informática, persona que se dedica a sabotear equipos de computo, en busca de cómo dañar equipos o extraer información con fines de lucro

IP, Protocolo de identificación en Internet
La telefonía IP ya se considera una tecnología madura; cada vez más hombres de negocios saben que les ayuda a ser productivos y competitivos; sin embargo, es tan sólo una de las aplicaciones sobre el protocolo Internet (IP).

Los costos de mantenimiento de centrales telefónicas se ha disparado en los últimos años, por lo cual "resulta cada vez más costoso para las empresas mantener redes de voz y datos separados, "actualmente la única desventaja de la telefonía IP frente a la telefonía tradicional es el costo de los aparatos IP, que aún es elevado; sin embargo, cuando se ve la solución total, las facilidades, los ahorros en costos de comunicación, eso deja de tener importancia; la calidad y la seguridad del servicio, hoy son prueba superada para la telefonía IP". En los próximos años se espera una importante adopción de comunicaciones IP y redes privadas virtuales (IP VPN).

El networker de la casa usa un Protocolo de Internet típico (IP) el router, IP que es el OSI más común, se conecta a una red de computadoras. Un router de IP como un DSL o el router de módem de cable une la red del área local en la casa (Lan) a la red de área-ancha (WAN) del Internet. Manteniendo información de la configuración en un pedazo de almacenamiento llamado la "ruta de mesa," los routers también tienen la habilidad de filtrar tráfico, entrante o saliente, basada en las direcciones de IP de remitente y receptores.

Mainframes
Es el término en inglés con que se designa a las computadoras de grandes dimensiones.

Passive wiretapping
Véase eavesdropping.

Password
Generalmente para ingresar a cualquier sistema, programa, a una terminal de usuario, como usuario de un correo electrónico, o sitios en la Red, se requiere una identificación de usuario y una contraseña (password), necesarias para tener acceso y evitar que cualquier individual hago uso de los mismos, poniendo en riesgo la información.

Ploters
De manera general, un plotter (o más correctamente, un trazador) es un aparato, que, conectado a un ordenador, traza sobre papel aquellos dibujos que se le envían desde el ordenador. Tradicionalmente los trazadores se han utilizado para dibujar planos arquitectónicos, de ingeniería, topográficos y todo tipo de dibujos de tipo técnico. Hoy en día, sin embargo, gracias a la proliferación de los programas de diseño artístico, también hemos instalado varios para realizar el

dibujo de líneas de diseños artísticos complejos, como son las impresiones denominadas gigantografías.

Los plotters son periféricos que efectúan dibujos de gran tamaño, usados principalmente en los campos de ingeniería y diseño gráfico.

Router
Es un dispositivo físico que une redes múltiples juntas. Técnicamente, un router es una "capa de 3 entradas", significa que se conectan redes (como entradas) y que opera a la capa de la red del modelo de OSI.

El ruteador realiza 2 funciones básicas: Es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente, de esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retrazo y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

Algunos routers permiten que el networker de la casa sirva para poner al día la mesa de asignación de ruta para una interfase vista por la Web. Definición: Una WAN de área geográfica grande, como un estado, provincia o país. WANs conectan a menudo redes más pequeñas múltiples, como LANs o WANs. El más popular WAN en el mundo hoy es el Internet. Muchas porciones más pequeñas del Internet, como intranets, también son WANs.
Una organización instala una línea- de arrendamiento típicamente WAN para apoyar una Intranet a largas distancias. Además comparte los archivos y el e-mail. Estas WAN's proporcionan acceso a los sitios de Web de intranet y sistemas de videoconferencias. Además, algunas organizaciones abren selectivamente el acceso a las WAN para que los compañeros proporcionen servicios de extranet.

Site
Se designa de esta manera a un lugar de almacenamiento de información, como centro de respaldo de datos, (incluso puede integrarse en él un Call Center alterno), también se le conoce así a los sitios web.

Warm site: Un centro de datos o espacio para oficinas parcialmente equipado con hardware, interfaces de comunicación, suministro eléctrico y condiciones ambientales capaz de proporcionar soporte operativo de apoyo. (términos asociados: "hot site", "cold site").

Hot site: Un centro de datos o un espacio acondicionado para oficinas equipado con unos niveles mínimos de hardware, interfaces de comunicación y espacio con atmósfera controlada capaz de proporcionar un soporte de procesamiento de datos de copia de seguridad con relativa inmediatez. (Términos asociados: "warm site", "cold site").

Cold site: Uno o más centros de datos o espacios acondicionados para oficinas equipados con unos niveles mínimos previamente fijados de condiciones ambientales, conectividad eléctrica, acceso a las

comunicaciones, espacio y acceso configurable para permitir que el personal a cargo de la misión pueda proceder a la instalación y a la puesta en marcha del equipamiento, necesarias para reiniciar las operaciones comerciales.

Sniffing Packet: en concreto "Sniffing" (a los que lo realizan se les denomina "Sniffers") es precisamente lo primero que viene a la cabeza, cuando se habla de robo de información. Se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet.

Esto se hace mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red, así como la interactuación con otros usuarios y ordenadores. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios, etc.).

Por ello, cada vez es más importante enviar encriptada la información. Por ejemplo, los mensajes de correo electrónico y archivos delicados deben enviarse encriptados con PGP o GnuPG. La transferencia de archivos mediante FTP, debe evitarse en lo posible, utilizando SSH.

Cómo funcionan los Sniffers: El modo más sencillo de comprender su funcionamiento, es examinándola forma en que funciona un sniffer en una red Ethernet. Se aplican los mismos principios para otras arquitecturas de red. Un sniffer de Ethernet es un programa que trabaja en conjunto con la tarjeta de interfaz de red (NIC, Network Interface Card), para absorber indiscriminadamente todo el tráfico que esté dentro del umbral de audición del sistema de escucha.

Para ello, el sniffer tiene que conseguir que la tarjeta entre en modo "promiscuo", en el que como indica la propia palabra, recibirá todos los paquetes que se desplazan por la red. Así pues, lo primero que hay que hacer es colocar el hardware de la red en modo promiscuo; a continuación el software puede capturar y analizar cualquier tráfico que pase por ese segmento.
Esto limita el alcance del sniffer, pues en este caso no podrá captar el tráfico externo a la red (o sea, más allá de los routers y dispositivos similares) y dependiendo de donde este conectado en la Intranet, podrá acceder a más datos y más importantes que en otro lugar. Para absorber datos que circulan por Internet, lo que se hace es crear servidores de correo o de DNS para colocar sus sniffers en estos puntos tan estratégicos.

Telepuerto
Se le conoce así a las instalaciones acondicionadas por Directv cuya función principal es, brindar, gestionar y mantener un servicio de acceso satelital bidireccional a Internet desde usuarios puntuales en todo el territorio de la república mexicana.
Toda la información intercambiada entre el Usuario final y el Telepuerto se realiza a través de un enlace satelital simétrico. Para esto, el Telepuerto deberá ser capaz de realizar, entre otras funciones:

- Todas las tareas y acciones necesarias para enviar y recibir, vía satélite, flujos de información IP desde Internet hacia usuarios ubicados en todo el territorio nacional y viceversa, o sea desde estos usuarios hacia Internet.
- Todas las tareas y acciones necesarias para gestionar y mantener la información de los usuarios, sus perfiles de tráfico y toda otra información relevante.
- Deberá contar con todo el equipamiento necesario para estas funciones antes descritas.

Características del Telepuerto:

- Disponibilidad
- El Telepuerto deberá contar un nivel de disponibilidad mínimo de 99,99% Conexión a Internet.
- El Telepuerto deberá estar conectado a un proveedor TIER ONE de Internet a través de un enlace que no incluya ningún salto de satélite.
- Se deberá indicar el número máximo de hops al core de Internet.

Administración remota del sistema:
Se deberá contar con algún sistema de supervisión que permita monitorear el estado de los enlaces de los abonados y el tráfico cursado, así como la calidad de servicio que se está brindando (delays entre Internet y el usuario y viceversa, etc.). Este sistema podrá ser accedido mediante una terminal remota, una página Web o similar.

Escalabilidad de la solución:
Se deberá indicar el procedimiento mediante el cual se amplía la capacidad contratada de usuarios y ancho de banda, para los servicios y el impacto en los servicios comercializados.

Upsizing: se utiliza para designar la integración de aplicaciones y ordenadores aislados en entornos de red, de forma que se permita la compartición de datos. Un ejemplo sería la integración de bases de datos aisladas en un entorno cliente / servidor, con un potente servidor de bases de datos. En lugar de hablar de downsizing o de upsizing, la estrategia es utilizar la herramienta adecuada para cada tarea. Esto es lo que se denomina rightsizing.

VPN
Un VPN's proporciona conectividad de la red por encima de una distancia física posiblemente larga. Un VPN (red privada virtual) es una forma de Red de Área Ancha (WAN).

VPNs para Acceso Remoto, puede apoyar al mismo Intranet/Extranet como servicio de una tradicional WAN, pero VPN también ha crecido en popularidad por su habilidad de apoyar el servicio de acceso remoto.

Anexos

Anexo I.- Legislación en México Sobre Delitos Informáticos

Reformas al Código Penal Federal en materia de Delitos Informáticos publicadas en el Diario Oficial de la Federación el 17 de Mayo de 1999.

Exposición de Motivos

Delitos informáticos:

El uso de la tecnología informática es un instrumento que facilita a la sociedad su desarrollo económico y cultural, mediante su empleo en todas las áreas del desarrollo nacional.

La Ley de Información Estadística y Geográfica, define en su artículo 3 a la informática, como la tecnología para el tratamiento sistemático y racional de información mediante el procesamiento electrónico de datos.

El avance logrado en los últimos años en este sector, ha permitido que un creciente número de personas tengan acceso a esta tecnología y la utilicen cotidianamente para realizar actividades de muy diversa índole, como las educativas, culturales, comerciales, industriales, financieras o de comunicación, entre muchas otras. Hoy en día tiene tal importancia, que muchas de esas actividades no podrían realizarse sin el uso de equipos y sistemas informáticos.

Paralelamente al avance tecnológico han surgido nuevas formas de conducta antisocial que han hecho de los equipos y sistemas informáticos instrumentos para delinquir. Adicionalmente, se presentan conductas en las que dichos equipos o sistemas constituyen el objeto o fin en si mismo de la infracción.

Dentro de las conductas ilícitas más comunes que constituyen los llamados por la doctrina jurídica como "delitos informáticos", se encuentran: el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos.

En el contexto internacional, la Organización de las Naciones Unidas ha reconocido que los delitos por computadora constituyen un grave problema ya que las leyes, los sistemas de impartición de justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos. La propia Organización instó a los Estados miembros a intensificar sus esfuerzos para combatir este tipo de conductas, entre otras medidas, mediante la creación de nuevos tipos penales y procedimientos de investigación, para hacer frente a estas nuevas y sofisticadas formas de actividad criminal.

Los países miembros de la Unión Europea tienen una regulación muy completa en el campo cibernético, que incluye seguridad de datos, creaciones intelectuales relacionadas con la informática, defraudación cibernética, contratos realizados a través de los medios binarios, cloneo electrónico y robo de información.

Francia y otros países europeos establecen como condición para proporcionar informes de los archivos de sus cuerpos policiacos, que el país que la solicite cuente con legislación protectora de la privacidad informática.

Países como Alemania. Austria y Francia han optado por crear una ley específica para combatir a los delitos informáticos, en tanto que otros países como Argentina. España y Estados Unidos de América, han optado por incluirlos en sus códigos penales.

El Estado mexicano esta obligado a proteger los bienes jurídicos de los sectores que utilizan la informática como instrumento de desarrollo, por ello, requiere de un marco jurídico acorde al avance tecnológico.

Algunos estados de la República, conscientes de la necesidad de legislar en esta materia han adoptado en sus ordenamientos penales normas tendientes a la protección de la información; tal es el caso de Sinaloa, que tipifica al delito informático, o Morelos y Tabasco, que protegen la información mediante la tipificación de la violación a la intimidad personal.

La inexistencia a nivel federal de tipos penales exactamente aplicables a esas conductas ha dado lugar a que sus autores queden impunes, por lo que es imperativo prever en la ley estas nuevas formas de delincuencia.

La magnitud de los daños ocasionados por estas conductas depende de la información que se vulnere, al grado que pueden tener un fuerte impacto en el desarrollo de la economía, en la seguridad nacional o en las relaciones comerciales.

Es necesario proteger la privacidad e integridad de la información contenida en sistemas y equipos de cómputo, de almacenamiento o procesamiento de información, por ello debe sancionarse a las personas que sin derecho, acceden a los equipos y sistemas de terceras personas para vulnerar la privacidad de la información, o dañarla, alterarla o provocar su pérdida.

La iniciativa que presentó a esa Soberanía, propone adicionar un capítulo al Código Penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer copiar, modificar o provocar la pérdida de información que contengan.

En virtud de que el bien jurídico que se pretende tutelar es la privacidad y la integridad de la información, se incluyen los tipos propuestos en el Título Noveno del citado ordenamiento, que ahora sólo ocupa el delito de revelación de secretos.

Asimismo se propone establecer una pena mayor cuando las conductas son cometidas en agravio del Estado. pues la utilización de sistemas de cómputo, computadoras, bases de datos y programas Informáticos es cada vez mayor, como lo es su regulación por las leyes federales; tal es el caso de la Ley de Información Estadística y Geográfica, Ley del Mercado de Valores, Ley que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública y Ley Federal para el Control de Precursores Químicos, Productos Químicos Esenciales y Máquinas para Elaborar Cápsulas, Tabletas o Comprimidos, entre otras.

En virtud de que las instituciones que integran el sistema financiero han sido con mayor frecuencia las víctimas por la comisión de estas conductas, se propone la creación de un nuevo artículo que proteja la información de su propiedad, aumentándose la pena hasta en una mitad, cuando las conductas previstas sean cometidas por miembros de las instituciones.

Finalmente, se propone agravar las sanciones previstas para los tipos penales antes descritos, cuando con la comisión de dichos ilícitos se obtenga un provecho propio o ajeno.

Código Penal Federal, Libro Segundo, Título Noveno.

Revelación De Secretos y Acceso Ilícito a Sistemas y Equipos de Informática
Capitulo II Acceso Ilícito a Sistemas y Equipos de Informática

Artículo 211 Bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 Bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 Bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.
ARTICULO 211 Bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 Bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 Bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 Bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En el siguiente cuadro, se especifican que en México los delitos informáticos se dividen en tres categorías: acceso ilícito a sistemas y equipos informáticos de particulares, de gobierno y del sistema financiero mexicano. La única variante son las sanciones y algunas agravantes especiales (Libro Segundo, Título Noveno.- Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, Código Penal Federal).

Sist. o Equipo Informático:	**Privado**		**Del Estado**		**Sistema Financiero**		
Agravantes:	Sin agravante	Provecho propio o ajeno	Sin agravante	Provecho propio o ajeno	Sin agravante	Empleado o Funcionario	Provecho propio o ajeno*
Sin autorización, modifique, destruya o provoque pérdida	Prisión: 6 m - 2 a Multa: 100 a 300 d	Prisión: 9 m - 3 a Multa: 150 a 450 d	Prisión: 1 a - 4 a Multa: 200 a 600 d	Prisión: 1.5 a - 6 a Multa: 300 a 900 d	Prisión: 6 m - 4 a Multa: 100 a 600 d	Prisión: 9 m - 6 a Multa: 150 a 900 d	Prisión: 13.5m - 9a Multa: 225 a 1350 d
Sin autorización, conozca o copie información	Prisión: 3 m - 1 a Multa: 50 a 150 d	Prisión: 4.5m-1.5a Multa: 75 a 225 d	Prisión: 6 m - 2 a Multa: 100 a 300 d	Prisión: 9 m - 3 a Multa: 150 a 450 d	Prisión: 3 m - 2 a Multa: 50 a 300 d	Prisión: 4.5 m - 3 a Multa: 75 a 450 d	Prisión: 6.75m-4.5a Multa: 112 a 675 d
Con autorización, modifique, destruya o provoque pérdida	N/A	N/A	Prisión: 2 a - 8 a Multa: 300 a 900 d	Prisión: 3 a - 12 a Multa: 450 a 1350 d	Prisión: 6 m - 4 a Multa: 100 a 600 d	Prisión: 9 m - 6 a Multa: 150 a 900 d	Prisión: 13.5m - 9a Multa: 225 a 1350 d
Con autorización, conozca o copie información	N/A	N/A	Prisión: 1 a - 4 a Multa: 150 a 400 d	Prisión: 1.5a - 6 a Multa: 225 a 600 d	Prisión: 3 m - 2 a Multa: 50 a 300 d	Prisión: 4.5 m - 3 a Multa: 75 a 450 d	Prisión: 6.75m-4.5a Multa: 112 a 450 d

*Penas de esta columna, suponiendo se den las dos agravantes (empleado o funcionario Y en provecho propio o ajeno). Si sólo se da el agravante de "en provecho propio o ajeno", las penas serían iguales a la columna de "empleado o funcionario".
m = meses, a = años, d = días multa, N/A = No Aplica

Anexo II. Aspectos relevantes que la Seguridad Lógica que contempla:

Confidencialidad
Conjunto de elementos que permitan garantizar razonablemente que la información magnética o documentos fuente son accesados o procesados por personal debidamente autorizado, de acuerdo a su posición jerárquica, responsabilidad y autoridad en la estructura de la organización.

Confiabilidad (disponibilidad)
Conjunto de elementos de control tanto automatizados como manuales, que permiten garantizar razonablemente la disponibilidad del producto. Relacionado directamente con premisa básica de informática:

- Continuidad del servicio
- Custodia de los datos
- La propiedad y uso de los datos pertenece a los usuarios

Intrusión
Es aquel acto que consiste en penetrar en sistemas administrativos o computacionales sin la autorización debida, con en fin de extraer información de manera visual o en forma virtual, sin implicar a ello necesariamente la extracción de información magnética o impresa.

Autenticación
Acción de verificación que consiste en validar que, quien dice ser sea efectivamente él, es decir, que al momento de identificarse en un sistema computacional o de telecomunicaciones, de acuerdo a los procesos de identificación efectivamente compruebe que es él. Ejemplo: Identificación de acceso, password. Debe existir un mecanismo que asegure la autenticación.

Encriptación
Es una técnica basada en algoritmos y modelos matemáticos que permite transformar un conjunto de caracteres o una secuencia de caracteres tal, que sólo puede ser entendida por el receptor que utilice el mismo algoritmo o modelo matemático desencriptador.

Sustracción
Acción deliberada y maliciosa de apropiarse de información magnética ya sea mediante un down loading (baja de archivo) o la sustracción de material impreso, respaldos, o cualquier otro medio de dispositivo de almacenamiento magnético.

Integridad
Concepto asociado a que la información magnética, mediante controles apropiados, se mantenga en forma modular sin perder su coherencia ni su consistencia.

Consistencia
Relacionado con la integridad de los datos, se refiere a que estos no pierdan su forma inicial y la relación coherente con otros datos, campos o tablas a través del tiempo.

Soporte
Es un concepto vinculado a las acciones o procesos que se encargan de mantener la integridad y consistencia de una determinada información.

Resguardo

Acciones manuales o automatizadas, para la custodia de la información magnética.

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no esta permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica, definiendo que los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento corrector
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Anexo III. Elementos de probabilidad.

No es nuestro objetivo dar un curso completo de probabilidad pero si exponer algunas definiciones para entender mejor los conceptos necesarios que se utilizan en el análisis de riesgo y que podrían ser de gran utilidad.

Espacio muestral

Si echamos un dado sobre una mesa, ignoramos qué cara quedará arriba, el resultado depende del azar, es una experiencia aleatoria.

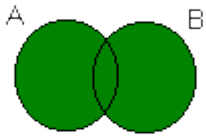
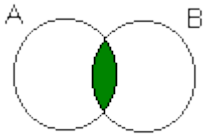
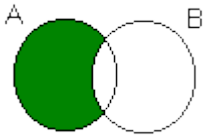
La vida cotidiana está plagada de sucesos aleatorios. Muchos de ellos, de tipo sociológico (viajes, accidentes, número de personas que acudirán a una tienda. etc.) aunque son suma de muchas decisiones individuales, pueden ser estudiados, muy ventajosamente, como aleatorios. A la colección de resultados que se obtiene en los experimentos aleatorios se le llama espacio muestral.
Ejemplo: si yo tiro un dado al aire el espacio muestral esta compuesto por: E = 1, 2, 3, 4, 5, 6

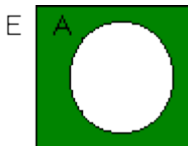
Suceso

Suceso de un fenómeno o experimento aleatorio es cada uno de los subconjuntos del espacio muestral E.

Operaciones con sucesos

Dados dos sucesos, A y B, se llaman:

Unión		$A \cup B$ es el suceso formado por todos los elementos de A y todos los elementos de B.
Intersección		$A \cap B$ es el suceso formado por todos los elementos que son, a la vez, de A y de B.
Diferencia		$A - B$ es el suceso formado por todos los elementos de A que no son de B.

Suceso contrario		El suceso $\overline{A}$ =E - A se llama suceso contrario de A.

Definición de Probabilidad

Probabilidad de un suceso es el número que tiende la frecuencia relativa asociada al suceso a medida que el número de veces que se realiza el experimento crece.

Frecuencia relativa:

La frecuencia relativa del suceso A:

$$f_r(A) = \frac{\textit{número de veces que aparece } A}{\textit{número de veces que se realiza el experimento}}$$

Definición de Laplace

En el caso de que todos los sucesos elementales del espacio muestral E sean equiprobables, Laplace define la probabilidad del suceso A como el cociente entre el número de resultados favorables a que ocurra el suceso A en el experimento y el número de resultados posibles del experimento.

Si $E = \{x_1, x_2, ..., x_k\}$ y $P(x_1) = P(x_2) = ... = P(x_k)$, entonces :

$$P(A) = \frac{\text{número de casos favorables al suceso } A}{\text{número de casos posibles}}$$

Teorema de la probabilidad total

Sea A1, A2, ...,An, un sistema completo de sucesos tales que la probabilidad de cada uno de ellos es distinta de cero y sea B un suceso cualquier del que se conocen las probabilidades condicionales P(B/Ai), entonces la probabilidad del suceso B viene dada por la expresión:

$$P(B) = P(A_1) \cdot P(B / A_1) + P(A_2) \cdot P(B / A_2) + ... + P(A_n) \cdot P(B / A_n)$$

Anexo IV. Manuales de Prevención Directv

a) Sismo o temblor, que hacer.

1. - Accionar la alarma de pánico.
2. - Conservar la calma.
3. - Desconectar los equipos de trabajo.
4. - Buscar las salidas de emergencia de acuerdo a los señalamientos existentes.
5. - No acercarse a las ventanas.
6. - No utilizar los elevadores.
7. - Salir ordenadamente sin correr.
8. - Tranquiliza a quien este cerca de ti.
9. - No situarse debajo de objetos colgantes que puedan caer.
10. - No tocar o quedarte cerca de cables sueltos.
11. - No situarse bajo postes, líneas telefónicas, árboles, anuncios u objetos que puedan caer fácilmente.
12. - Concentrarse en el Jardín frente al edificio en un área libre de árboles.
13. - No regresar a tu lugar de trabajo hasta que la Comisión revise si no hay Riesgos y se den las indicaciones necesarias para que puedes regresar a tu lugar de trabajo.
14. - Se tiene una relación de todo el personal con Teléfono y Dirección.

Nota: Es importante que todo el personal identifique las salidas de emergencia y No bloquee las mismas.

b) Amenaza terrorista o sabotaje.

Las amenazas terroristas o sabotaje pueden llegar de dos formas:

1. - Mediante una nota.
2. - Mediante una llamada telefónica.

Las notas suelen dejarse en un escritorio o un mostrador. Al encontrar una nota amenazante, mantén la calma, entrégala al funcionario de mayor jerarquía dentro de la oficina. El funcionario se encargará de avisar al personal experto y notificar al personal, no lo comentes con nadie para no provocar pánico.
Si recibes una llamada telefónica, mantén la calma trata de mantener al amenazante en la línea el mayor tiempo posible, eso mejora las posibilidades de identificación.

Trata de averiguar donde esta colocado el explosivo y a que hora va a explotar. Apenas cuelgues el teléfono anota la información siguiente:

- Hora de la llamada.
- Qué fue lo que te dijeron.
- Sexo de quién llamó.
- Tono y peculiaridad de la voz, acento regional, nivel social que denota el vocabulario, ruidos, sonido de fondo.
- Notifica de inmediato al funcionario de mayor jerarquía en ese momento, él se encargará de notificar al personal experto o autoridades competentes.

-En caso de emergencia por bomba o terrorismo espera con calma las instrucciones de los expertos nunca tomes decisiones precipitadas, un error puede ser fatal para ti o tus compañeros.
-El personal de oficinas puede colaborar tratando de localizarla observando si existe algún objeto extraño.
-Si localizas un paquete extraño no lo toques, ni permitas que nadie se acerque o lo toque.
-No fumar, el calor puede activarlo.
-No encender aparatos de radio, una radio frecuencia puede activarlo.
-No acercarse con ropa de nylon, la electricidad estática puede hacerla explotar.
-No levantes ninguna tapa.
-No abras ningún broche o cerradura.
-No cargues o inclines el paquete.
-No cambies de posición o pongas de costado el objeto sospechoso.

Cuida tu vida y la de tus compañeros no trates de ser héroe, en caso de encontrar objetos extraños, comunícalo a los expertos, ellos se encargarán de darte las instrucciones adecuadas.

c) Incendio.

La Torre Inverlat cuenta con sistemas modernos para la detección de incendios, tales como:

- Efectivo sistema de alarmas manuales para dar aviso inmediato en caso de emergencia.
- Consola de control que recibe la señal de alarma y localiza el lugar del incendio.
- Alarmas audiovisuales que permiten localizar el sitio de la emergencia.
- Detectores de ionización de alta sensibilidad al humo y al fuego.
- Sistemas de sonido ambiental para comunicación de instrucciones.
- Escaleras de emergencia que conducen a zonas seguras en caso de evacuación.
- Extintores de fuego colocados cerca de todas las áreas de trabajo.
- Hidrantes ubicados en puntos estratégicos y sólo se utilizan en caso de presentarse un incendio.

d) Medidas de prevención de fuego

- Al terminar las labores desconecte computadoras, cafeteras, ventiladores y en general todo equipo eléctrico que no sea ocupado.
- Evite tirar cerillos prendidos o semi-apagados a los botes de basura.
- No conectar más de un aparato por contacto.
- Evitar el uso de extensiones eléctricas si su uso es continuo solicite la instalación de más contactos.
- Reporte tomas de corriente, apagadores, balastros y en general todo equipo o instalación eléctrica en mal estado.

Aprende a distinguir el fuego:
Aprende a distinguir un conato de incendio y un incendio.

<u>Conato de incendio:</u>
Es cuando el fuego no se ha expandido demasiado y puedo combatirse con un extintor.

Incendio:
Es cuando el fuego se ha extendido y se vuelve incontrolable y requiere la presencia de especialistas que apliquen grandes cantidades de agua para apagarlo.

Como actuar en caso de un conato de fuego

- Conserva la calma.
- Localiza el extintor más cercano.
- Toma el extintor por la parte superior con la otra mano tómalo de la base, levántalo un poco y sepáralo de su sujeción.
- Trasládalo tomándolo del maneral con una mano.
- Oriéntate del lado contrario de las llamas del humo.
- Aproxímate al sitio del fuego y bájalo sin soltarlo ubicándolo lejos de tu cuerpo y piernas.
- Quita el seguro.
- Apunta el chiflón o la manguera hacia la base del fuego.
- Acciona el extintor y "barre" la base del fuego de izquierda a derecha y de derecha a izquierda varias veces.
- Una vez extinguido el fuego, mueve los rescoldos para verificar que ya existen brasas o llamas.
- Si persisten las llamas o brasas opera nuevamente el extintor.

Como actuar en caso de incendio declarado

- Un fuego detectado a tiempo y bien combatido nunca llegará a ser un incendio peligroso.
- Pero debemos estar prevenidos para actuar en caso de que el fuego no pueda controlarse en su inicio y se declare un incendio.
- En tal caso avisar inmediatamente al personal de seguridad del edificio.
- El personal de seguridad se encargará de utilizar los hidratantes y llamar a los bomberos.
- El personal de seguridad del edificio, dirigirá el plan de evacuación indicando mediante el sonido ambiental las zonas dañadas y las zonas de seguridad, así como los caminos y procedimientos para evacuar el piso y ponerse a salvo en una zona segura.
- Debes conservar la calma y seguir al pie de la letra sus instrucciones.
- Nunca contravengas sus instrucciones.
- Si es posible antes de abandonar tu lugar de trabajo desconecta el equipo eléctrico y cierra con llave tu escritorio.
- Al evacuar el área camina en fila pegado a la pared.
- Nunca utilices los elevadores.
- Al utilizar la escalera ocupa el costado, deja el centro libre para el paso de los encargados de combatir el incendio.
- Sigue los caminos establecidos no intentes nunca descubrir tu propia ruta de evacuación.
- No trates de ser el primero en salir. Toma tu lugar y camina al mismo ritmo de los demás.
- Si hay mucho humo agáchate, cerca del piso hay más oxígeno.
- No intentes regresar por algo que se te olvido.
- Al llegar al área de seguridad permanece cerca del encargado de seguridad quien pasará lista del personal de tu piso.
- Si notas la ausencia del algún compañero repórtala de inmediato.
- En el área de seguridad se te informará si puedes volver a tu lugar de trabajo y ahí mismo te proporcionarán cualquier otra información pertinente.

Cualquiera que sea el tipo de fuego (conato o incendio declarado), tu actuación debe ser rápida y efectiva.

El modo de operar del sistema de detección contra incendio FM-200 se describe a continuación:
¿Qué hacer en caso de alarma?

1.- Luz estroboscópica y tonos intermitentes.
El sistema ha detectado una condición de alarma, el sistema contra incendio no disparará el gas FM-200, deberá localizarse la posible existencia de fuego, generación de humo o gas volátil.

Si el punto anterior es controlable, podrá silenciarse la alarma sonora y visual y se logra desplazando y oprimiendo por dos (2) segundos el botón silenciar alarma que se encuentra en el interior del tablero. Hasta haber controlado el conato, podrá restablecerse la condición normal en el equipo, lo anterior se logra con el botón reset que se encuentra en el interior del tablero.

2.- Luz estroboscópica y tono constante.
El sistema ha detectado y confirmado la posible existencia de fuego, generación de humo o gas volátil, a partir de ese momento un (1) minuto se disparará el gas FM-200.
Durante el lapso de un (1) minuto, usted podrá decidir las siguientes opciones:

- Localizar la fuente que ha activado la alarma
- Disparar manualmente el sistema contra incendio

Si localiza la fuente que ha activado la alarma podrá decidir:

-Abortar la operación automática del sistema contra incendio, esto solo si fue una falsa alarma o el conato puede ser controlable.
-Dejar que el sistema contra incendio dispare automáticamente el gas FM-200
-Disparar manualmente el accionamiento que libera el gas FM-200.

¿Cómo abortar el sistema contra incendio?
Esto lo podrá realizar antes de que transcurra un (1) minuto a partir de la detección y confirmación (luz estroboscópica y sonido de alarma constante) para esto, deberá oprimir y mantener hacia adentro el botón amarillo cuya leyenda dice abortar. De requerirse la ayuda de otra(s) persona(s) para controlar el conato, usted no deberá soltar el botón de aborto.

Hasta tener controlada la situación y sin soltar el botón de aborto, usted u otra persona deberá restablecer (botón reset) en el tablero, con esto el tablero volverá a su condición normal y podrá de esta manera soltar a su posición normal el botón de aborto.

Disparo manual del sistema contra incendio. Esto lo podrá realizar de 2 maneras:
1.- En la situación manual (color rojo) deberá empujar y jalar la palanca de accionamiento. Inmediatamente liberará el gas FM-200.
En la parte superior del tanque contenedor del gas FM-200 existe un gatillo tipo granada para su accionamiento deberá retirarse el seguro (alambre) y tirar del gatillo.
2.- Una vez accionada la liberación del gas FM-200, nada lo detiene hasta vaciar el contenido de su depósito.

Cualquier anomalía o reporte se realizarla a esta empresa:
Tel. Celular: 044 5000-0000. Ing. Responsable
Vip. 50000000. Pin. 5000-. Derzu
Oficina: 50000000
Razón social del proveedor: "Derzu S.A. de C.V." Bufete de ingeniería eléctrica.

e) Que hacer en caso de falla del aire acondicionado.

En caso de falla del aire acondicionado, se cuenta con varias unidades de ventana o mini split, repartidas estratégicamente en todo el piso y en especial en el site ya que el aire acondicionado es confort para el personal.

Se tiene 4 unidades de ventana para el site.

f) Que hacer en caso de erupción del volcán

En horas y días hábiles

El Comité ejecutivo de desastres en base a las informaciones del CENAPRED procederá a informar a todos los empleados las acciones que procedan.
Dependiendo de la magnitud de este evento, se aplicaran las fases que contempla el manual de Recuperación de desastres determinando. El Comité Ejecutivo el inicio de las acciones de emergencia que procedan incluso defiriendo los lugares alternos de operación. En el caso de Telepuerto, se definirán las acciones alternas que procedan en coordinación con DTLA.

En horas y días inhábiles

La Dirección de Recursos Humanos establecerá comunicación con el Director General y los demás miembros del Comité Ejecutivo para definir las acciones más urgentes que procedan en base a las comunicaciones que se reciban a través de los medios de comunicación emitidos por el CENAPRED.

Se determinará en ese momento el plan a seguir debiendo el Director de Recursos Humanos implementar el plan de comunicación aprobado el cual se involucrará a todos los empleados de Directv, para lo cual se cuenta con registro de los teléfonos particulares de cada uno de los empleados para que en caso de que se requiera se les llame para informarles del plan de acción a seguir en las siguientes 48 horas del desastre y en todo caso de las siguientes 2 semanas.

Bibliografía

1.- Newton I. Bowers, Jr. ... [Et Al.], "Actuarial mathematics", Itasca, illinois : Society of actuaries, 624 p, 1986.

2. Baruch fischhoff... [et al.], "Acceptable risk" , Cambridge : Cambridge university, 320p, 1981.

3.- Charles P. Pfleeger , "Security in Computing", Edit. Prentice Hall, Englewood Cliffs, New Jersey, 352 p, 1989.

4.- Janet Butler, "Contingency planing and disaster recovery strategies", Edit. Computer technology research Corp., 1987.

5.- Rodríguez Prieto Amador, "Protección de la Información", Edit. Paraninfo, España, 420 p, 1985.

6.- Caballero Pino, Seguridad Informática, Edit. Ra-ma, Madrid, España, 195 p, 1997.

7.- Alcira Kreimer and Margaret Arnold, "Managing Disaster Risk in Emerging", Edit. The World Bank, 360 p, 2000.

8.- D.I. Cleland W.R. King, "Manual para la Administración de Proyectos", Ed. CECSA, México, 1999.

9.- Sonabend, "Total Recovery Planning System", Manual de metodología versión 7.0, Edit. Sonabend & asociados, S.C, 430 p, 1996.

10.- Gabriel Baca Urbina, "Evaluación de proyectos", Ed. Mc Graw Hill, México, 1999.

11.- Lawrance, W. William, "El Riesgo Aceptable", Ed. Nuevomar, México, 1978.

12.- Leonard H. Fine, "Seguridad en Centros de Cómputo": Políticas y Procedimientos, Edit. Trillas.

13.- Pierre Gratton, "Protección Informática", Edit. Trillas, 390 p, 1998.

14.- Richard B. Levin, "Virus Informáticos", Edit. Mc Graw Hill, España, 1991.

15.- Francoise Perroux, "La empresa y la Economía del siglo XX", Edit. Deusto, 370 p, 1970.

16.- Peter Bishop, "Conceptos de Informática", Ed. Anaya multimedia, Madrid, 1989.

17.- Jesús Manuel Macías, "Desastre en Guadalajara", SEP, México, 1994.

18.- Bill Gates, "Camino al Futuro", Edit. Mc Graw Hill, 1996.

19.- Thomas R. Peltier, "Information Security Policies", Procedures and Standards: Guidelines for Effective Information Security Management, CRC Press, 1 st Edition, 486 p, 2001.

20.- Thomas R. Peltier, "Information Security Risk Analysis", Auerbach Publications, 1 st Edition, 2001.

21.- Micki Krause, Harold F. Tipton, "Information Security Management Handbook", Fourth Edition, Volume I, Auerbach Publications, 1999.

22.- Jack Killmeyer Tudor, "Information Security Architecture": An Integrated Approach to Security in the Organization. CRC Press, 2000.

23.- Christopher King, Ertem Osmanaglu, Curtis Dalton, "Security Architecture": Design, Deployment and Operations, McGraw Hill Osborne Media, 1 st Ed. 2001.

24.- Scott Barman, "Writing Information Security Policies", QUE, 1 st Edition, 195 p,2001.

25.- Jay Ramachandran, "Designing Security Architecture Solutions", John Wiley & Sons, 1 st edition, 296 p, 2002.

26.- Jon William Toigo, "Disaster Recovery Planning: Strategies for Protecting Critical Information Assets", Prentice Hall, 3 rd ed, 2002.

27.- Eric Maiwald, William Seiglen, "Security Planning and Disaster Recovery", Mc Graw-Hill Osborne Media, 2002.

28.- Floyd Piedad, Michael Hawkins, "High Availability: Design, Techniques and Processes", Prentice Hall, 1 st edition,412 p, 2000.

29.- Evan Marcus, Hal Stern, "Blueprints for High Availability: Designing Resilient Distributed Systems", John Wiley & Sons, 1 st edition,386 p, 2000.

30.- Rodríguez Morilla Carmen, "Análisis de Series de Tiempo", La Muralla S.A., 1ra Edición, España, 2002

31.- Chris Chatfield, "Time-Series Forecasting", Chapman & Hall/crc, 1ra Edición, USA, 2000.

Sitios Internet

www.cenapred.unam.mx, UNAM, julio 2004.
www.dgpc.gob.mx, Dirección de protección civil del Gob. del D. F.,Agosto 2004
www.cpci.org.ar, Consejo profesional de ciencias en informática, Septiembre 2004
www.desenredando.org, Juan Manuel Macias, marzo 2004
www.compulinux.com/diego, Diego Bravo estrada, marzo 2004
www.cicese.mx, Centro de Investigación Científica y de Estudios Superiores de Ensenada, junio 2004
www.riskmexico.com/magazines/magazine21/asp/editorial.asp, mayo 2004
www.cismid-uni.org/modules.php?name=News&file=article&sid=3, noviembre 2003
www.ipqa.org.ar/eventos/presentaciones/2TPAmbien-17-10-01/Rambla.pdf, enero 2004
www.disaster-recovery-guide.com/, diciembre 2003
www.disasterrecoveryworld.com/, diciembre 2003
www.disaster-recovery-plan.com/, diciembre 2003
www.drj.com/new2dr/samples.htm, julio 2003
www.drj.com/new2dr/w2_002.htm, julio 2003
www.binomial.com/, marzo 2004
www.drplanning.org/ , febrero 2003
www.infosyssec.net/infosyssec/buscon1.htm, diciembre 2003
www.disasterrecoveryforum.com, junio 2003
www.rothstein.com, mayo 2004
www.espaciopyme.com/monograficos/, enero 2004
www.afina.com.mx/, julio 2003
www.noticiasdot.com/publicaciones/ 2004/1004/2110/noticias211004/noticias211004-1.htm
www.greenpeace.org/espana_es/features/ details?item_id=448860&campaign_id
www.ilustrados.com/publicaciones, julio 2003

Proveedores y Servicios

Recuperación del Desastre
Oficina en el Reino Unido
CTS Group Ltd. 14 Thames View Business Park, Abingdon, Oxon. OX14 3UJ
Tel: +44 (0)1235 559944 Fax: +44 (0)1235 550025 E-mail:info@cts-group.co.uk

DRP Consultores
Asesoría Integral, Orientado a las aplicaciones criticas
http;//www.drp.consultores.com

Preservation Servis leaflet
Recuperación de Desastres, Servicios y Artículos
1438 west peachstree street, suite 200
Atlanta, Georgia 30309
Phone: 404.892.0943
Website, www.solinet.net

Asistencia para Recuperación Ante Desastres
Departamento de Vivienda y Desarrollo Urbano de EE.UU. 451 7th Street S.W., Washington, DC 20410Teléfono: (202) 708-1112 TTY: (202) 708-1455

PRESERVATION SERVICESLEAFLET
1438 W. Peachtree St. NW / Suite 200 / Atlanta, G30309-
29551.800.999.8558 / 404.892.0943 / FAX 404.892.7879

Recuperación de Desastres: Servicios y Artículos
Belfor USA2425 Blue Smoke CourtSouth Fort Worth,
TX 76105817-536-1167, 800-856-3333

Strohl Systems
631 Park AvenueKing of Prussia, PA 19406610-768-4120, 800-634-2016 www.strohlsystems.com
asesoría, continuidad de negocios, programas para la planeación de recuperación de desastres

VidiPax
450 West 31st Street4th Floor
New York, NY 10001
212-563-1999, 800-653-8434
www.vidipax.com
Restauración y reformateo de cintas magnéticas y asesoría

Excalibur Data Recovery, Inc.
101 Billerica Avenue
Building 5
North Billerica, MA 01862
978-663-1700, 800-466-0893
Recuperación de información electrónica (anteriormente Randomex, Inc)

Belfor USA
2425 Blue Smoke Court
South Fort Worth, TX 76105
817-536-1167, 800-856-3333
www.belforusa.com
Recuperación de desastres, deshumidificación, limpieza de moho, recuperación de información en cintas magnéticas, secado por congelación

INTERGDATA
Soluciones de Integridad de Datos para Recuperación
México
Avenida México No. 803
Santa Teresa - Magdalena Contreras,
México, D.F. 10710 - MEXICO
Tel: (+52 55) 5449-4871
Fax: (+52 55) 5449-4810
Soluciones & Servicios
Flor E. Hernández
Teléfono: (+52 55) 5449-4874

INTERGDATA(E.U.A.)
12707 High Bluff Drive
Suite 200
San Diego, CA 92009 - U.S.A.
Tel: (858) 350-4232
Fax: (760) 942-1016

EMC (where information lives)
EMC es el líder mundial en sistemas, software, redes y servicios de almacenamiento de información
Contactos de Ventas y Servicios al Cliente
EMC Corporation
35 Parkwood Drive
Hopkinton, Massachusetts
01748
(508) 435-1000

KTL S.A. (Ingenieria en Seguridad Informática)
Centro: Piedras 264 piso 7 "D" (C1070AAF) Buenos Aires - Tel. (011) 4331 8878
Pompeya: Famatina 3985 (C1437OS) Buenos Aires - Tel. (011) 4911 0818
Tortuguitas: Av. Pte. Illia 4191 (km 40,4 de Ruta 8 vieja) - (B1613DSE) Tortuguitas - Pcia. de Bs. As.
e mail: info@ktl.com.ar

Soluciones Informáticas y Aplicaciones Crediticias S.A. de C.V.
Socio Director: I.S.C. Agustín Z. Zambrano Brambila
Direccion: José Guadalupe Zuno 48 (lateral Periférico Norte), Zapopan, Jalisco.
Teléfono: (33) 3364-1794